International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Strengthening IoT Device Security: A Cybersecurity Framework for Securing Over-the-Air Firmware Updates

Gayatri Khade[1], Shreya Raut[2]

Department of Computer Science

Dr. D. Y. Patil Arts, Commerce & Science College, Pimpri

Pune, Maharashtra, India

Abstract: - Safety concerns at the firmware updates, where vulnerabilities could affect total device concession, have increased due to the growing dependence on the Internet of Things (IoT) bias in consumer and critical surroundings. For always situate patches and point advancements, over-the-air (OTA) firmware updates are constantly used. Still, deficiently secured update mechanisms appear critical cybersecurity risks, such as force-chain attacks, vicious firmware injection, man-in-the-middle interception, and rollback to vulnerable firmware performances. Particularly for bias with resources, the present IoT update systems constantly warrant thorough trust evidence, interpretation performance, and post-update integrity verification. By establishing a secure and empirical OTA firmware update fashion, this study offers a cybersecurity approach intended to enhance the security of IoT bias. For securing the authenticity, integrity, and continuity of firmware execution, the recommended architecture involves secure charge enforcement, restated update channels, firmware digital signing, cryptographic integrity verification, and anti-rollback protection. The frame's capability to help common firmware-position attacks while still being practical for low-power IoT surrounds is demonstrated via a trouble-driven security study. The recommended approach for futuristic IoT ecosystems propagates secure-by-design OTA update approaches, strengthens firmware rigidity, and safeguards concerning attack shells.

Keywords: Internet of Things (IoT), Over-the-Air (OTA), Firmware Updates, Cybersecurity Approach, Anti-rollback Protection, Firmware Rigidity, Attack Shells.

1. Introduction

The rapid growth of Internet of Things (IoT) devices provides growth to new cyberspaces that allow for continuous networking between smart town infrastructure, networks of transport, industrial control locations, healthcare facilities, and smart consumers. The use of IoT devices, used to connect a lot of gadgets to the internet through sensors, has increased overall because of technological advances in cloud computing, wireless communication, and embedded technologies. Though it also leads to more cybersecurity concerns, the current state of internet connectivity provides emerging opportunities for technological advancements, industrial reliability, and taking decisions based on data. Because they work in restricted resource's locations, IoT devices require physical access, generating them especially vulnerable for hackers. The gadgets control sensitive data and manage critical infrastructure systems, thus analysts, stakeholders from the industry, and government agencies have started to focus on their security.

IoT gadgets firmware, or operating system, which handles all hardware features, routes of communication, and security features, provides the base software layer. Considering cybersecurity threats change on a regular basis, organizations require updating their firmware systems regularly that include security modifications, improvement of performance, and new features. The ability to distribute security patches over multiple locations and reduce expenses for operation while applying safety upgrades without requiring physical gadget communication are some of the benefits of OTA updates. OTA updates provide operational positive

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

advantages, but they also generate serious cybersecurity vulnerabilities requiring the implementation of suitable security measures to safeguard their systems.

OTA updates require exchanging firmware images over networks lacking in encrypted access, opening up new possibilities for technically sophisticated security breaches. Man-in-the-middle (MITE) attacks allow adversaries to monitor and modify firmware payloads that they target at devices by taking the advantage of communication channel vulnerabilities.

For Over-The-Air (OTA) firmware updates, the present security frameworks and standards for Internet of Things (IoT) systems are unsustainable. Present day versions do not offer end-to-end firmware validation and device reliability formation, instead concentrating their defence on networking layer security. The limited processing capacity, stored memories, and energy availability of IoT devices make it practically challenging to get them to maintain the demands for processing of the standard secure cryptographic networks. A system's insecure authentication techniques, unreliable device identity management system, and weak trust establishment points all contribute to its lack of ability to provide suitable safety protection. Secure authentication processes that verify firmware integrity previous system activity, hardware authentication gadgets, and secure booting techniques are not available in the majority of the present frameworks. The requirement for specific protection technologies that must safeguard their OTA updates with extensible and easily portable security systems makes the research necessary.

The study presents an advanced cybersecurity framework that, for the reason its safety features, safeguards over-the-air firmware updates in Internet of Things gadgets. The framework includes a variety of protection levels such as two-factor authentication, end-to-end encryption, digital signature verification, and cryptographic hash code integrity validation. The system generates secure boot strategies that utilize hardware authentication to prevent firmware from being executed by unauthorized users. The framework establishes a reliable public key infrastructure framework, which includes certificate execution, encrypted key distribution, and privacy protection with the lifecycle management procedures. Blockchain-based verification methods and asymmetric reliability frameworks supply providers a technique to improve both the safety and transparency for their firmware distribution procedures. Because the recommended design has been specifically developed for devices with a few resources, it ensures effortless cryptography processes without dedicating cybersecurity protection.

The study is significant because it signifies devices to maintain operating regardless of Internet of Things (IoT) structures while protecting against new cyberthreats. For to reduce the possibility of botnet growth, with them firmware security breaches, and total system unsuccessful individuals, the framework safeguards firmware authenticity, confidentiality, and integrity everywhere the update process. The paper provides both theoretical as well as practical contributions by establishing an IoT security strategy that can be applied regarding healthcare and industries with the Internet of Things and smart infrastructure conditions, as well as an OTA security framework that takes advantage of relevant cybersecurity safeguards.

The analysis reveals that since over-the-air (OTA) firmware upgrades provide the legal foundation for developing trustworthy and safe Internet of Things (IoT) ecosystems, they must be safeguarded. With its integrated cryptographic protections, secure boot verification, secure authentication techniques, and sophisticated reliability management system, the solution provides a cybersecurity framework with many safeguards and lightweight components that can be strengthened to defence against security threats. The proposed framework protects the continuing explosion of all interconnected digital networks while strengthening the security of IoT devices through its systematic improvements of the OTA update process.

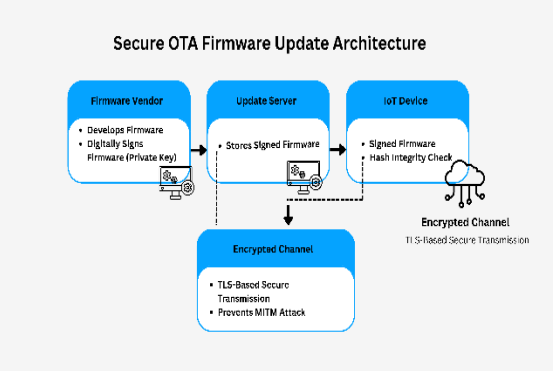

Figure 1: secure OTA firmware update architecture

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

2. Literature Review

With the rapid expansion of IoT networks into critical infrastructure, securing the firmware update process has become a top priority for researchers. While Over-the-Air (OTA) updates are essential for pushing security patches and keeping devices functional, the process is often riddled with risks like interception or malicious tampering. Because these wireless updates are a prime target for hackers, there is a growing body of work dedicated to fixing vulnerabilities through better encryption, cryptographic signatures, and more resilient system architectures. Essentially, as our world gets more connected, making sure a device can update itself without being hijacked has shifted from a technical convenience to a fundamental safety requirement.

2.1. Security Challenges in OTA Firmware Updates

The core of current exploration into IoT security focuses on the massive threats ignited into Over-the-Air(OTA) firmware distribution. Experts like Sicari et al.(2015) point out that as IoT partiality get more connected, their" attack shell" or the number of tricks a attackers can get in — expands significantly. This is primarily due to weakened authentication and insecure communication channels that quit updates wide open to being interdicted or switched with vicious law. Weber(2010) adds to this by noting that a lack of assiduity-wide security ethics means numerous bias hit the request with nearly no protection, turning OTA updates into a systemic adventure.

Further investigation by Mosenia and Jha(2017) highlights how well assaulters can use Man- in-the- Middle(MitM) or renewal attacks to trick a device into accepting" poisoned" firmware through relaxed channels. Structure on this, Alrawais et al. (2017) argue that numerous OTA services simply don’t use strong enough encryption or "cipher suites", leaving the door open for unauthorized access. Together these researches make it clear that we can’t just hope updates are safe; we need severe, multi-stage integrity checks and authentication assembled into the very DNA of the update process to help total system concession.

2.2. Cryptographic Solutions and Lightweight Protocols

Given the resource constraints of many IoT devices, scholars have explored optimized cryptographic methods tailored for low-power and low-memory environments. Humen et al. (2013) introduce lightweight key management structures that balance security with computational efficiency, proposing lightweight authentication protocols for IoT messaging. Similarly, Santos et al. (2018) investigate Elliptic Curve Cryptography (ECC) as a suitable alternative to traditional RSA schemes, emphasizing its reduced overhead for secure firmware signing and verification.

Jha and Raman (2019) examine the role of secure cryptographic channels in OTA updates, proposing secure key establishment mechanisms that ensure confidentiality and integrity without imposing excessive resource demands. In contrast, Lee et al. (2020) focus on hashing and message authentication codes (MACs) as efficient tools for integrity validation, demonstrating how firmware images can be reliably verified before installation.

2.3. Trust Management and Secure Boot

In current research, the idea of building an environment for reliable execution generates a lot of curiosity. Secure boot techniques are well known for their ability to stop unauthorised programming by confirming firmware integrity during device booting. A thorough review of hardware root-of-trust approaches that validate firmware early in the boot phase and significantly lower the risk of persisting malicious programs is given by Utting et al.(2016).

Hardware security components and Trusted Platform Modules (TPMs) are presented by Sadeghi et al. (2015) as trust anchors. Devices can confirm the firmware's origin prior to deployment thanks to these modules' support for secure key storage and cryptographic functions. These strategies aid in reducing external attack vectors by integrating trust into device hardware and separating it from network environments.

2.4. Certificate Management and PKI Approaches

Public Key Infrastructure (PKI) and certificate-based authentication have become essential approaches for securing Over-the-Air (OTA) updates. By ensuring that hardware only permits software from certified sources, Mayer et al. (2019) claim that using certificates to issue and authenticate identities offers a scalable method of building confidence between patch servers and IoT devices that require updates. The standard PKI methodology does have some limitations though; centrally handling these certificates can become a major technical challenge when IoT networks improve to involve millions of systems.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Researchers are now turning towards trusted decentralization models like blockchain to fix these growing challenges. According to Dorri et al. (2017), handling identity and certificate records through distributed ledgers reduces the need for a central authority and greatly increases the system's tolerance to manipulation or centralized failures. Hussein et al. (2020) caution that although this method is logically sound, it is not a "plug-and-play" solution. Blockchain technologies must be specially designed to avoid bugs that might slow down the very update process they are meant to secure, as a lot of IoT devices possess limited processing bandwidth.

2.5. Frameworks and Standardization Efforts

The introduction of numerous industry frameworks and standards aims to standardize the technique of preventing Over-the-Air (OTA) firmware updates. The Internet Engineering Task Force (IETF) and the Open Connectivity Foundation (OCF) are two organizations that issued guidelines to manage a device's whole lifecycle, including how it gets upgrades. The Software Update for the Internet of Things (SUIT) specification provided by the Internet Engineering Task Force (IETF) is a well-known example. By using "manifests"—basically, digital descriptions of an update—SUIT enables a device to verify the signatures and monitor compatibility with the hardware before the updating process ever begins.

Recent research, however, indicates that these frameworks are frequently less like a whole image and more like separate puzzle pieces. They rarely offer a complete, end-to-end security solution, even though they offer great technological specifications for specific operations. For example, SUIT does an excellent job of specifying what a secure manifest seems like, but it does not really clarify how that data should be transmitted or how device IDs should be handled. This fragmented technique illustrates the need for an integrated method by introducing weaknesses in security that professional attackers can still exploit.

2.6. Limitations and Gaps in Current Research

A major issue in the literature looks at how security conditions conflict with limited coffers. Despite the suggested cryptographic and trust mechanisms provide reliable protection, their high processing power constraints make them difficult for use on devices that consume less power. Integrated frameworks that include trust management, secure booting, and encryption authentication into a single system designed for OTA firmware updates are not yet available in the literature. There are two primary challenges to the current research. Actual real-world usage is required to validate the results of the research. Many theoretical and simulation-based studies are available in the current body of research, but there is a dearth of experimental research that verifies conclusions in real-world settings by testing various device types and network topologies.

3. Methodology and Material

3.1 Research Methodology

The study proposes and evaluates a cybersecurity framework that safeguards Over-the-Air (OTA) firmware updates in Internet of Things (IoT) networks using the Design Science Research (DSR) methodology. Although the goal of the research is to generate and establish a structured security system that will defend against known vulnerabilities in updated OTA systems, choosing the option of DSR appears sensible.

(I) Problem identification and security requirement analysis.

(II) framework design and architectural modelling.

(III) cryptographic and trust mechanism implementation.

(IV) experimental validation .

(V) performance and security evaluation are all five sequential phases included in the research process.

The proposed structure is established in three different stages, beginning with the theoretical foundations and then transferring on to methodological establish and real-life scenarios in Internet of Things environments.

3.2 System Architecture

Through utilization of a layered architectural framework, the recommended cybersecurity framework safeguards every aspect of updating the firmware during the entire update procedure.

The five key parts of the system are now as follows:

1. IoT Device Layer: Embedded devices with a few resources that can boot securely.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

2. OTA Update Server: This centralized structure firmware transmission system is in the role to provide authorized firmware updates.
3. Public Key Infrastructure (PKI): These digital certificate authorities are in the role of maintaining the certificate lifecycle and providing identification.
4. Secure Firmware Development Environment: A totally separate system for the following one; hashing, and digital signature of firmware.
5.Communication Network: A wireless transmission network based on protocols like Bluetooth, Wi-Fi, and LTE for communication.

Device related identification and authentication, encrypted data communication, firmware production and authorization, and secured implementation with authorized validation are the four operational stages that protect the OTA process.

3.3 Security Mechanism Implementation

3.3.1 End-to-end encryption :
Transport Layer Security (TLS 1.3) and Datagram TLS (DTLS), functioning depends on each device's weaknesses, are utilized by the entire network to maintain the confidentiality of data. Because Elliptic Curve Cryptography, also known as ECC, is accessible on devices with less resources and is lacking technical expectations, it has developed into the most prevalent technique. The system's standard safety framework defends against man-in-the-middle attacks (MITM) and intercepting data.

3.3.2 Mutual authentication :
Mutual authentication was established between the OTA server and the IoT device via authentication certificates the PKI techniques. Every gadget was given a special cryptographic identity by the whole framework, as well as a private key that would be encrypted by secure hardware. Sensors authorize server the certificates before acquiring updates, and the OTA server analyses device certificates before firmware availability.

3.3.3 Secure Boot and Hardware Root of Trust :
The system's secure boot technique, which established a hardware Root of Trust (Rot) as its foundation, executes authorized firmware. For the purpose of verifying firmware identities regarding authorized authentication data preserved on secure hardware, the boot firmware executes its startup strategy. Attackers are prevented from maintaining control of the system when verification unsuccessfully fails and the electronic device automatically reverts to the previous verified firmware version.

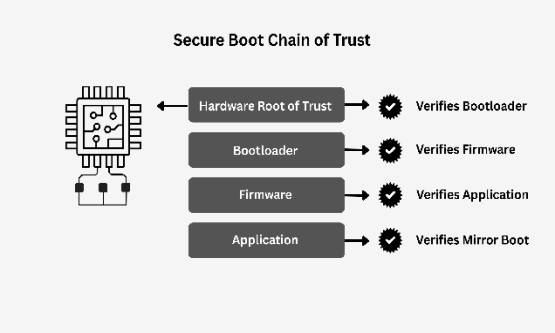

Figure 2: secure boot chain of trust

3.3.4 Key Management and Certificate Lifecycle :
Secure key enrolment for device establishment techniques, frequently happening key rotation, controlling of certificate termination, and secured key storage according to Trusted Platform Modules (TPM) for systems that were accessible were all aspects of the organization's secure key lifecycle management plan. Unauthorized users posing as authorized users and breached keys are the two key vulnerabilities that the technique safeguards to prevent.

3.3.5 Optional Distributed Ledger Validation
A blockchain-based firmware hash tracking system was employed in the currently experimental evaluation, providing an alternative approach to successfully get beyond the drawbacks of administrative authority. Firmware hash values were saved by the distributed blockchain system as a validation technique that prevented malicious modification. Prior to the installation process, the devices verified the firmware integrity using a tracking network.

3.4 Materials and experimental setup

3.4.1 Hardware components :
The following component structure was created the experimental tested:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

· ARM Cortex-M and ESP32 microcontroller boards, which stand in for specific Internet of Things device.
· A Raspberry Pi 4 set up as the server's activities for OTA updates.
For encrypted key storage and take advantage of the Trusted Platform Module (TPM) hardware module.
· Secure embedded systems with boot functionalities.
The system's specified components are designed for simulating real-world IoT network the operating environment.

3.4.2 Software Environment :
The practical implementation utilized the properties of the following aspects:
· Analysing embedded C/C++ for developing firmware.
· The OpenSSL library for the technology of cryptography.
· Protocols encrypted by using TLS/DTLS including HTTPS and MQTT.
· Server arrangement dependent on Linux operating system.
· Wireshark for analysing communication across networks.
The Metasploit framework is used for simulating controlled malicious activity.
To establish security of the supply chain safeguards, the software development team used a secure environment for development for performing cryptography and firmware verification procedures.

3.5 Experimental Evaluation

3.5.1 Analysis via Experimentation :
The analysts chosen two techniques to analyse the system's operational strengths and safety technologies with the intention to establish the system's performance.

3.5.2 Measures of Performance
For the analysis to determine their device's performance assessment and evaluation, they require a specific to the device technical analysis.
1. The period necessary to perform the cryptographic evaluations.
2. How lengthy it generally takes to finalize the firmware verification procedures.
3. The amount of the data processed and memory required.
4. The network functionality range utilized to facilitate communication of data.
5. The overall amount of strength required during the updating procedures.
In order to identify the most beneficial protection proper balance between systems performance and security techniques, the analysts thoroughly analysed all of the security data points that were collected.

3.5.3 Verification of Security
The following attacks were among the remote threat simulation activities that the analysis team had successfully performed:
1. Man-in-the-middle (MITM) attacks
2. Attacks by replay
3. An effort to downgrade
4. Modifying to Firmware
5. Server impersonation scenarios.
Two criteria, the success rate of the attack and the system response behavior, were used to evaluate the performance of detection and prevention activities as well as recovery procedures.

3.6 Evaluation via Comparison

The suggested framework was evaluated against basic OTA models that essentially implemented TLS and standardized update systems and lacked digital signatures. The evaluation analysed five aspects, which involve system performance visualizations, scalability, authentication accuracy, integrity protection, and resilience to the advanced persistent breaches.

3.7 Data Analysis

The analysts used quantitative analysis of data while analysing what was discovered of their procedures. The analysts evaluated the framework's abilities to facilitate large-scale IoT installations using average performance values, effectiveness for security efficiency, and operating expenses analyses.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

4. Results and Discussion

4.1 Experimental Results

Through testing on ESP32 and ARM Cortex-M microcontroller systems as well as their Raspberry Pi-based OTA server, which performed in a controlled environment, the research team developed and examined their cybersecurity architecture that secures Over-the-Air (OTA) firmware updates. The analysis highlighted two main aspects:
(I) resilience against OTA-related cyberattacks and (ii) performance efficiency in resource-constrained scenarios.

4.1.1 Cryptographic Performance Analysis :
When the TLS 1.3 secure communication medium and Elliptic Curve Cryptography (ECC) were released for digital signatures, more computing power was claimed for upgrading the firmware. According to the assessment, ECDSA signature verification required very little time to process, remained within the operational range of the device, as well as acceptable integrated system delay constraints.

As its foundational model, the OTA model used in the study to test CPU loading declined signature verification. The system's CPU use only went up during the firmware authentication process. The RAM capacity of the specified microcontrollers was still exceeded by the memory resources necessary for establishing the TLS session and certificate validation. The study proves that ECC-based secure algorithms that are lightweight and limited in resources function effectively on Internet of Things devices.

4.1.2 Firmware Verification and Update Latency :
A controlled increase in the whole update time was the outcome of the SHA-256 hashing and digital signature verification process used to validate firmware integrity. As the firmware size increased, the system's processing latency also increased, however this delay had no effect on the functionality or availability of the device. There was a barely apparent delay in beginning due to the secure boot verification process that was performed during device reconfiguration. Through its verification procedure, the hardware Root of Trust verified the authenticity of the firmware and confirmed that runtime integrity assurances may operate without impacting a decline in system reliability.

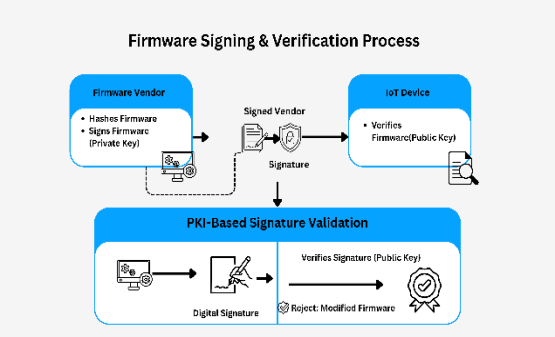

Figure 3: firmware signing and verification process

4.1.3 Network Overhead Evaluation :
Because certificates required to be exchanged and cryptographic data had to be sent over the internet, encrypted OTA transmission via the TLS and DTLS protocols led to increased packet sizes. The complete encryption of all firmware payloads is demonstrated by Wireshark traffic monitoring, thus preventing the visibility of binary data while it was being transmitted. IoT systems based on Wi-Fi and LTE maintained the available bandwidth, but the network overhead rises when compared to unencrypted connections.

4.1.4 Energy Consumption Assessment :
Power usage increased only moderately during the cryptographic handshake and signature verification procedures, according to energy profiling. Because OTA updates are sporadic, their effect on battery-operated devices is limited. The framework exhibits enough environmental sustainability to facilitate useful Internet of Things applications in actual-life scenarios.

4.2 Security Validation Results

4.2.1 Man-in-the-Middle (MITM) Attack :
Attackers tried to access and update firmware data streams during the simulated MITM attacks. Because the TLS encryption system used certificate-based mutual authorization to guard against unauthorized access to the host user identities, it was able to block payload access. Due to the failure for the attackers to successfully carry out their interception tries, the system protected every interaction session.

4.2.2 Firmware Tampering Detection :
Because researchers tested the system by introducing updated firmware samples into the OTA system, the system developers implemented that technique to test their code modifications. By detecting hash anomalies and signature discrepancies, the device discovered verification issues. Because digital signature and integrity

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

validation methods operated efficiently, the system was able to stop compromised firmware from being deployed.

4.2.3 Replay and Downgrade Attack Prevention :
The attackers used repeat attacks to test their capability to transfer firmware data that they had before acquired. To stop attempts at security access replay, the system uses session-based nonce algorithms with timestamp validation. Version control enforcement prevented initiatives to update bias using out- of- date firmware, assuring anti-rollback integrity.

4.2.4 Server Impersonation Attempts :
The malicious firmware was distributed via unauthorized OTA servers, which were made accessible autonomously of the current system. Because the devices used severe PKI certificate validation, which validated the efficiency of their mutual authentication process, they blocked firmware downloads from unauthorized sources.

4.2.5 Key Compromise Mitigation :
The simulated key theft cases revealed that users were successfully prevented by using their compromised credentials by certificate revocation systems. To demonstrate the need for safe key lifecycle management, the devices rejected authentication requests originating from revoked certificates.

4.3 Comparative Analysis

When compared to baseline OTA implementations lacking signature verification and secure boot enforcement, the proposed framework exhibited significantly stronger resistance to firmware manipulation and unauthorized update distribution. TLS-only implementations provided transmission confidentiality but did not ensure firmware authenticity or rollback prevention.

The integration of secure boot and hardware Root of Trust provided an additional security layer absent in conventional update models. This significantly reduced the risk of persistent firmware-level compromise, which is commonly exploited in IoT botnet formation and large-scale cyberattacks.

Although the framework introduced moderate computational and communication overhead, the trade-off between security enhancement and resource consumption was favourable. The additional overhead remained within acceptable limits for embedded devices while substantially improving resilience against advanced cyber threats.

4.4 Discussion

The framework protects against firmware changes by using hardware Root of Trust and secure boot, providing an essential security advancement over safe OTA updates that do not confirm signatures. While the TLS encryption method secures data during transfer, it cannot verify the firmware's authenticity, which forces attackers to upgrade to original, more vulnerable versions. The approach blocks any continuous minor attacks that hackers use to create IoT botnets, which turns out to be a good trade-off although it needs more processing from the device. It simply needs a small additional load, which integrated devices can manage, and provides reliable defence against emerging cyberthreats.

5. Conclusion

Rapid growth in Internet of Things (IoT) environments resulted in a demand for secured device management systems that can manage firmware updates over the air (OTA). Because they allow attackers to do firmware modifications, man-in-the-middle attacks, replay and downgrade attacks, and unauthorized upgrades, OTA update methods that are not secure pose serious security concerns to devices. IoT networks as a whole as well as individual devices are at risk from these threats, which have a special impact on critical sectors such as healthcare, industrial automation, and smart city development.

The analysis makes an advanced technology cybersecurity framework that protects firmware updates for Internet of Things devices with limited processing ability Over the Air (OTA). To prevent illegal access to firmware updates, the framework applies fully encrypted theft prevention, PKI mutual authentication, digital signatures, hash integrity verification, secure boot, structured key management, and hardware Root of Trust.

Analysis and findings of the study shows that Elliptic Curve Cryptography (ECC) generates effective safeguarding with equivalent performance. Man-in-the-middle (MITM) attacks, modification, replay, downgrade, and server impersonation are among the six types of attacks that the framework protects against while handling effectively in scarce resources IoT scenarios. Additionally, it builds more trust.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

6. References

1..L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.
https://www.researchgate.net/publication/270107935_Security_privacy_and_trust_in_Internet_of_Things_The_road_ahead

2. M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications, vol. 38, pp. 8–27, 2018.
https://www.researchgate.net/publication/322864555_Internet_of_Things_A_survey_on_the_security_of_IoT_frameworks

3. M. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in Proc. 52nd ACM/EDAC/IEEE Design Automation Conf., 2015.
https://www.researchgate.net/publication/283593608_Security_and_privacy_challenges_in_industrial_Internet_of_Things

4. S. R. Choudhury, S. Das, and S. Bhatia, Secure over-the-air software updates in Internet of Things devices: A survey, IEEE Internet of Things Journal, vol. 7, no. 9, pp. 7831–7845, 2020.
https://www.researchgate.net/publication/339279259_Over-the-Air_Software_Updates_in_the_Internet_of_Things_An_Overview_of_Key_Principles

5. A. Costin and A. Francillon, Firmware security: A survey of embedded device vulnerabilities and secure update mechanisms, in Proceedings of the USENIX Security Symposium, 2014.
https://www.researchgate.net/publication/278763280_A_Large-Scale_Analysis_of_the_Security_of_Embedded_Firmwares

6. Internet Engineering Task Force (IETF), "A Firmware Update Architecture for Internet of Things," RFC 9019, 2021.
https://www.researchgate.net/publication/372946962_Design_and_Evaluation_of_a_Method_for_Over-The-Air_Firmware_Updates_for_IoT_Devices

7. A. Rahman and E. Dijk, "Security for constrained IoT devices in firmware update scenarios," IEEE Communications Magazine, vol. 58, no. 10, pp. 56–62,2020.
https://www.researchgate.net/publication/333472928_Secure_Firmware_Updates_for_Constrained_IoT_Devices_Using_Open_Standards_A_Reality_Check

8. H. Tschofenig and H. Birkholz, "A Firmware Update Architecture for Internet of Things," Internet Engineering Task Force (IETF), RFC 9019,2021.
https://www.researchgate.net/publication/363698590_Toward_Identification_and_Characterization_of_IoT_Software_Update_Practices

9. A. Ukil, S. Bandyopadhyay, and A. Pal, "IoT Security with Secure Firmware Update Mechanisms," in IEEE Conference on Advanced Networks and Telecommunications Systems, 2018.
https://www.researchgate.net/publication/348309426_Security_in_IoT_Threats_and_Vulnerabilities_Layered_Architecture_Encryption_Mechanisms_Challenges_and_Solutions

10. H. Birkholz, H. Tschofenig, and K. Thaler, "Security Considerations for Firmware Updates in IoT Devices," IETF Internet Draft, 2020.
https://www.researchgate.net/publication/358886946_Secure_firmware_Over-The-Air_updates_for_IoT_Survey_challenges_and_discussions