International Journal on Science and Technology (IJSAT)

E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

End-to-End Encryption Strategies for Enterprise Healthcare WLANs: Beyond WPA3

Srinivas Maganti

magantisrinivas4@gmail.com

Abstract:
The recent rapid digitization of healthcare settings, driven by the advancement of the Internet of Medical Things (IoMT) and full Electronic Health Records (EHRs), has increased the wireless attack surface in clinical environments exponentially. Although the Wi-Fi Protected Access 3 (WPA3) protocol has solved the most critical cryptographic flaws of its predecessor, the WPA2, the WPA3 protocol essentially is a link-layer security solution. The paper is a systematic research study investigating the structural constraints of utilizing only link-layer encryption in healthcare Wireless Local Area Networks (WLANs) and examines the urgent need to shift to application-layer End-to-End Encryption (E2EE). This report applies a multifaceted approach to literature and framework analysis to assess the performance trade-offs of using advanced application-layer encryption protocols, namely Transport Layer Security (TLS) 1.3 and Datagram TLS (DTLS) 1.3, in WPA3-Enterprise infrastructure. Moreover, the review also considers how the IEEE 2933 standard (TIPPSS framework) and the NIST SP 800-207 Zero Trust Architecture (ZTA) can be merged to create an uninterrupted cryptographic verification throughout the clinical ecosystem. Due to the extremely low computational and energy efficiency of extreme-edge IoMT devices, the study compares lightweight cryptography (LWC) that is the NIST-standardized ASCON to traditional Advanced Encryption Standard (AES) suites. The main results indicate that a defense-in-depth architecture, a synthesis of WPA3-Enterprise 192-bit mode with ASCON-based E2EE and Zero Trust micro-segmentation, is the best balance between military-grade cryptographic security and the strict latency, throughput, and battery life needs of life-critical medical telemetry systems. [1]

Keywords: Wi-Fi Protected Access 3 (WPA3), End-to-End Encryption (E2EE), Zero Trust Architecture (ZTA), Healthcare WLAN, Internet of Medical Things (IoMT), Lightweight Cryptography, IEEE 2933.

1. Introduction

High capacity wireless networks are a mission-critical backbone of the modern healthcare ecosystem of the Internet of Medical Things (IoMT). Whether it is an infusion pump or ECG monitor, a smart bed or an autonomous robot, all devices that are connected to Wi-Fi relay sensitive ePHI, which requires strong security in the conditions of HIPAA and HITECH [4].

KRACK attacks defeated WPA2, the long-standing standard in 2017. WPA3 (2018) counters with SAE (Dragonfly) to enhance stronger authentication, PMF to protect management frames, and optional 192-bit CNSA-grade encryption. WPA3 is a link-layer protocol, however: it only secures the wireless hop. After arriving at the access point, data travels the wired network in plaintext unless safeguarded by higher-layer protocols- leaving ePHI vulnerable to insider threats, VLAN hopping, and misconfigurations [5].

To overcome this healthcare has to implement End to End Encryption (E2EE) in accordance with the NIST Zero Trust Architecture (ZTA) which presupposes no implicit trust, even
inside the network. E2EE secures the encryption of the

data at the IoMT device level and seals it until it is decrypted at its end point (e.g., EHR or clinician dashboard) [6].

But E2EE on resource-constrained edge devices is challenging. TLS 1.2 using AES-256 is resource-intensive in terms of CPU, memory, and power-consumption - threatening latency in life-critical telemetry and decreasing the battery life of devices. The solutions demand TLS 1.3, Lightweight Cryptography (LWC) on embedded systems, and implementation with IEEE 2933 TIPPSS interoperability, trade offs between security, performance, and clinical reliability [9][10].

2. Literature Review

The nexus of wireless network security, healthcare telemetry optimization, and applied cryptography has produced a solid academic research and industry standardization activity. The systematic review of the modern literature indicates that there are four main thematic clusters: the assessment of the cryptographic capabilities of WPA3 and transition vulnerability, the paradigm shift to the Zero Trust Architecture and the IEEE standard 2933 TIPPSS, the performance of application layer encryption under resource-constrained conditions, and the emergence of Lightweight Cryptography (LWC) as an extreme-edge medical device. The first implementation of WPA3 prompted a lot of scholarly criticism on its capacity to address the systemic flaws of WPA2. WPA3 studies on Simultaneous Authentication of Equals (SAE) handshake have established that the Dragonfly key exchange effectively addresses the passive eavesdropping and offline dictionary attacks that had devastating effects on the WPA2 Pre-Shared Key (PSK) architecture. Nevertheless, in the literature, it is also emphasized that WPA3 is not a fault-tolerant protocol6].

In 2019, the identification of the so-called Dragonblood vulnerabilities proved that the timing-based side-channel attacks were still capable of retrieving password data during the SAE handshake, and, as a result, led the IEEE 802.11 working group to adopt the Hash-to-Element (H2E) technique to recover the cryptographic integrity. Moreover, sources that discuss the implementation of enterprises highlight the difficulties of deploying the WPA3-Enterprise 192-bit mode. This is the highest level of security that requires 256-bit Galois/Counter Mode Protocol (GCMP-256) to encrypt the data and Elliptic Curve Digital Signature Algorithm (ECDSA) that involves the use of a 384-bit curve to derive the key. Although this suite provides military-level security that meets the requirements of the Commercial National Security Algorithm[9].

(CNSA) guidelines, research has shown that the computational requirements of GCMP-256 are prohibitive to a huge proportion of legacy medical devices and low-power internet of things sensors, which can be a significant bottleneck to widespread implementation in clinical environments. There is universal agreement among academics that WPA3 Transition Mode should never be used in healthcare settings, where it facilitates attackers to perform Basic Service Set Identifier (BSSID) spoofing, pitting the modern clients against the WPA2 networks without Protected Management Frames (PMF), and opening the attack surface to deauthentication and key reinstallation attacks once more. In acknowledgment of the innate weaknesses of perimeter-based protection, including firewalls and link-layer WLAN encryption, recent scholarly and regulatory discussion has vociferously shifted to Zero Trust Architecture (ZTA). The literature of this shift is NIST Special Publication 800-207, which officially identifies ZTA as an enterprise cybersecurity architecture that gets rid of implicit trust, using only network location, affiliation, or ownership. [9][3]

In systematic literature reviews assessing ZTA in the healthcare setting, scholars have reported that a combination of continuous authentication, dynamic policy enforcement, and identity-based micro-segmentation effectively mitigates the blast radius of compromised IoMT devices and blocks the subsequent spread of ransomware within the subnets in the clinical environment. The IEEE 2933-2024 standard, called the TIPPSS framework, is an explicit codification of this zero-trust philosophy into the medical field.

The works that investigate IEEE 2933 highlight that in order to establish real clinical interoperability, a concerted effort is needed to realize Trust (device attestation), Identity (cryptographic identities not spoofable MAC addresses), Privacy, Protection, Safety, and Security. Importantly, researchers emphasize that IEEE 2933 standard explicitly stipulates that clinical devices must either communicate using end-to-end encryption instead of using the security offered by the transport layer, which in effect formalizes the concept of E2EE as a regulatory and design requirement of the contemporary IoMT implementation. The literature on the assessment of implementing E2EE on IoMT devices demonstrates that there exists a large technical conflict between cryptographic strength and the physical resource limitations of medical devices. Transport Layer Security (TLS) 1.2 is an important part of traditional application-layer security. Nonetheless, comparative research indicates that TLS 1.2 is not the best in wireless healthcare as it uses a complex handshake procedure where two full round-trips (2-RTT) are needed before secure data transmission can occur, leading to unacceptable latency in real-time telemetry. The scholarly community heavily recommends deploying TLS 1.3 that minimizes the cryptographic handshake to a single round-trip (1-RTT) and removes outdated and insecure cipher suites in Favor of Authenticated Encryption with Associated Data (AEAD) algorithms [8][3].

In the case of UDP-based telemetry protocols (typically found in IoT), including the Constrained Application Protocol (CoAP), Datagram TLS (DTLS) 1.3 can offer the same efficiencies, and research has demonstrated that the implemented symmetric encryption ciphers (e.g., AES-128 or AES-256) consume significant processing power that cannot be matched by extreme edge devices. In an attempt to tackle this very critical gap, emphasis has been put on Lightweight Cryptography (LWC) by researchers.

In 2023, NIST completed standardization of the ASCON family of algorithms which were specifically developed to operate in constrained settings. Although the vulnerabilities of WPA3 are carefully investigated in separate scholarly articles, the notion of the Zero Trust and lightweight cryptographic performance can be followed, the literature on the organization of a complete, holistic architecture integrating all these aspects in a live enterprise healthcare WLAN setting is significantly underrepresented. Recent studies tend to lack practical engineering methods of smoothly overlaying ASCON-based application-layer E2EE over a WPA3-Enterprise network segmented with an 802.1X Policy Decision Point (PDP). The report brings together these divergent areas of research to fill that particular architectural gap.

3.Methodology

To satisfy the specifications of this analysis, this report uses a research and survey methodology, which involves a thorough literature and framework analysis technique without the use of primary experimental laboratory testing but the synthesis of empirical information based on the already developed cryptographic benchmarks and architectural standards. This paradigmatic approach is quite suitable to research in cybersecurity architecture because it enables the holistic assessment of multi-layered protocol interactions in a diverse array of enterprise environments that would be prohibitively costly and challenging to model holistically in a single controlled laboratory environment.

The study plan is implemented in form of three analytical steps. In the initial step, the systematic literature review and data extraction protocol was used on major academic and industry repositories, mostly focusing on peer-reviewed articles of the IEEE Xplore Digital Library, Google Scholar, the ACM Digital Library, as well as the National Institute of Standards and Technology (NIST) publication database. The search terms were limited to the scope of literature published since 2018 (the year of WPA3 ratification) and up to 2026, which would make the analysis consider the latest cryptographic standards and threat platforms. The Boolean search strings were based on the following keywords: WPA3-Enterprise, End-to-End Encryption, Healthcare WLAN, IoMT Security, Zero Trust Architecture, TLS 1.3, ASCON Lightweight Cryptography, and IEEE 2933 TIPPSS.

The second phase involved a comparative framework analysis that aimed to assess the technical effectiveness and trade-offs in operation of the various cryptographic protocols. This comprised of retrieving the secondary empirical data in the chosen literature namely benchmark data on the encryption/decryption execution time, central processing unit (CPU) memory usage, network latency (in milliseconds of round-trip time), and power consumption (in milliwatts/microamps). They used this quantitative data to develop comparative models to compare link-layer encryption (WPA2 vs. WPA3-Enterprise 192-bit mode) with application-layer encryption protocols (TLS 1.2 vs. TLS 1.3 and DTLS 1.3). Moreover, dedicated benchmarking measurements were obtained to conduct a stringent comparison between conventional Advanced Encryption Standard (AES) implementations (namely, AES-128-GCM and AES-256-GCM) and the new NIST-standardized ASCON lightweight cryptography suite when implemented on resource-constrained microcontroller units characteristic of extreme-edge IoMT devices.

An architectural synthesis was done in the last stage. This entailed aligning the optimized cryptography protocols in phase two with the stringent regulatory and architectural requirements of the NIST SP 800-207 Zero Trust Architecture guidance and the IEEE 2933-2024 Clinical IoT Data and Device Interoperability standard (TIPPSS framework). This architecture was intended to create a unified, defense-in-depth architectural design, which combines network access control (802.1X/EAP-TLS), dynamic micro-segmentation, wireless air-interface protection (WPA3 PMF), and application-layer data confidentiality (E2EE) to meet the requirements of the complex interplay of the clinical workflows and patient safety of an enterprise healthcare setting.

3.1 Result and Discussion

The implementation of strong End-to-End Encryption in healthcare WLANs in the enterprise level needs a multi-layered, highly coordinated implementation. The literature review and empirical standards analysis demonstrate that the implementation of the protocols, which are not closely integrated with each other, cannot ensure the security of clinical data; on the contrary, the close coordination of the wireless perimeter defense, the maximum-efficient cryptography of the transport layer, and the network segmentation based on identity are required. These sections elaborate on the analytical results of the structural constraints of WPA3, the performance index of E2EE protocols, the architectural need of lightweight cryptography as well as the architectural assembly of these components into a Zero Trust architecture.

4. Proposed Architecture

Multi-Layer Security Model

1. **Access Control Layer**
   - 802.1X + EAP-TLS
   - Certificate-based authentication
2. **Network Layer**
   - WPA3-Enterprise
   - PMF protection
3. **Application Layer**
   - TLS 1.3 / DTLS 1.3
   - ASCON encryption
4. **Control Layer**
   - Zero Trust Policy Engine
   - NAC systems (ISE/ClearPass)

5.1 Limitations of WPA3

- High CPU overhead
- Compatibility issues

- No internal network protection

5.2 Performance Comparison

Protocol	Latency	CPU Usage	Efficiency
TLS 1.2	High	High	Low
TLS 1.3	Low	Medium	High
DTLS 1.3	Very Low	Medium	Very High

5.3 ASCON vs AES

Algorithm	Power Usage	Speed	Suitability
AES-256	High	Medium	High-End Devices
ASCON	Low	High	IoMT Devices

5.4 Zero Trust Integration

Benefits:

- Prevents lateral attacks
- Enforces identity verification
- Enables micro-segmentation

6.1 The Link-Layer Bottleneck: Limitations of WPA3-Enterprise in Clinical Settings

The implementation of WPA3-Enterprise protocol on healthcare WLANs goes a long way in strengthening the physical air interface, which is essential as the first line of defense against external cyber assaults. WPA3, by both enforcing 802.1X authentication and enforcing the use of Protected Management Frames (PMF), basically prevents the use of rogue access points that seek to spoof either the disassociation or deauthentication frame to hijack a clinical session or to interfere with important telemetry streams. Moreover, the optional WPA3-Enterprise 192-bit mode takes wireless security to new levels by applying Suite B cryptography, that is, using the 256-bit Galois/Counter Mode Protocol (GCMP-256) to encrypt the data and the Elliptic Curve Digital Signature Algorithm (ECDSA) to derive the key using a 384-bit curve. Nonetheless, the analytical information demonstrates that there are critical operations and architectural trade-offs when healthcare organizations want to rely on WPA3 as the sole means of securing data. WPA3-Enterprise 192-bit mode involves very complicated certificate generation mechanisms - it necessitates minimum 3072-bit RSA keys, but strongly recommended 4096-bit keys - and uses large CPU cycles to sustain the GCMP-256 state. Most legacy IoMT devices, and even many of the most recent wearable sensors, simply do not have the computational capacity to run these intensive mathematical computations. Efforts to make these devices use 192-bit mode cause unacceptable network latency, lost telemetry packets and fast and unsafe battery drainage. In turn, operational necessity frequently compels the IT administrators of the respective hospitals to activate WPA3 Transition Mode- a backward-compatibility scheme that permits both WPA2 and WPA3 devices to coexist on the same Service Set Identifier (SSID).The literature also warns unanimously that the use of WPA3 Transition Mode in a clinical scenario is a risky security tradeoff.[6]

Analytical data shows that Transition Mode actively opens the network to advanced downgrade attacks, where attackers silence WPA3 beacons and coerce dual-capable medical devices to use the weaker WPA2 protocol, to bypass the more robust WPA3 protective measures and reinstigate the long-known KRACK exploits. Moreover, WPA3, despite being used without Transition Mode, still has a critical architectural vulnerability: WPA3 is exclusively a link-layer protocol, which encrypts the payload only on the wireless air interface. When the data is put into the wired Local Area Network (LAN), it will pass through access switches, distribution layers, and core routers in full plaintext unless it is secured by upper-level

applications. In case a malicious actor manages to compromise a switch in a hospital or physically gain access to a LAN port in a patient room, the unencrypted ePHI can be easily intercepted and read with basic packet sniffing tools, thus although the implementation of WPA3-Enterprise 192-bit mode is a key requirement in realizing a secure wireless perimeter, it serves only as a secure transport pipe. [7][5].

6.2 Overcoming Extreme Edge Constraints with Lightweight Cryptography (LWC)

In order to attain genuine End-to-End Encryption (E2EE), health care architectures need to encrypt data on the application layer where the payload of the request is mathematically sealed between the source medical sensor and the cloud platform or EHR database., In the past, E2EE using Transport Layer Security (TLS) 1.2 added considerable performance overhead to clinical settings because the handshake process was unwieldy (2-round-. This delay was especially harmful to life-critical, time-sensitive telemetry, e.g., continuous cardiac surveillance. This critical bottleneck is decisively solved by the universal adoption of TLS 1.3. TLS 1.3 simplifies the cryptographic interaction to a single round-trip (1-RTT), and fully removes outdated, insecure cipher suites (including RC4, DES and CBC-mode ciphers), and uses only highly optimized Authenticated Encryption with Associated Data (AEAD) algorithms. Moreover, TLS 1.3 adds a 0-RTT mode to session-resumption, a feature that enables devices that have already connected to a clinical server to send encrypted data as soon as they connect to a TCP connection and this will reduce network overhead by a significant margin. To use datagram-based patient monitoring systems, which operate over constrained, lossy networks, Datagram TLS (DTLS) 1.3 in combination with the Constrained Application Protocol (CoAP) provides unrivaled efficiency and performance. Analytical evidence shows that DTLS 1.3 reduces bytes-over-the-air so dramatically in comparison with its predecessor. In intense benchmark measurements, the architectural design of Wi-Fi 6 (802.11ax) with Target Wake Time (TWT) and CoAP/DTLS demonstrated the lowest average Round-Trip Time (RTT) of 10.98 milliseconds, with predictable and low-latency time-sensitive clinical telemetry [3][6].

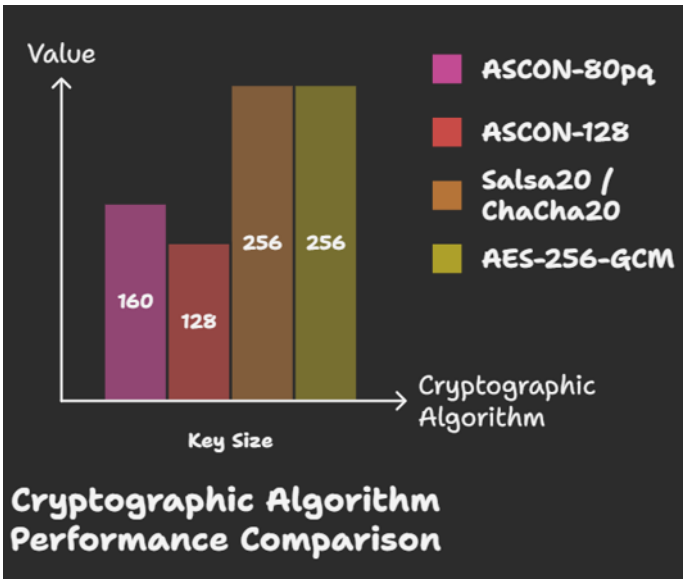

Figure 1: Crypto Algorithm Comparison

By implementing ASCON for application-layer E2EE, medical device manufacturers can drastically reduce both latency and code size. In dense mesh network simulations, replacing traditional AES + HMAC protocol stacks with ASCON resulted in significant power preservation, ensuring that continuous glucose monitors and similar life-critical devices do not have to sacrifice operational lifespan or patient safety to achieve mandatory data confidentiality [1].

6.3 Architectural Orchestration: Integrating E2EE with IEEE 2933 and Zero Trust

The implementation of strong cryptographic protocols would be irrelevant in the end unless there is a strict and centralized identity and access control. WPA3 and application-layer E2EE integration has to be coordinated in the strict conditions of the NIST SP 800-207 Zero Trust Architecture (ZTA) and the IEEE 2933-2024 standard on Clinical IoT Data and Device Interoperability., The IEEE 2933 standard presents the overall TIPPSS framework: Trust, Identity, Privacy, Protection, Safety, In this model, the constant identity confirmation is crucial. In the past, MAC Authentication Bypass (MAB) was an important part of healthcare IT with headless medical devices. But MAC addresses can be easily spoofed in plaintext on the air interface and can be used to easily evade the perimeter access control by malicious actors. To address the TIPPSS requirement, IEEE 2933 specifically forbids the use of network-layer identifiers, but requires verifiable, cryptographically secure identities to be used. Enterprise healthcare WLANs need to universally use 802.1X with EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) to align with ZTA and TIPPSS, and it requires that the digital certificates installed on the central RADIUS server and connecting IoMT client are mutually authenticated, so password-guessing attacks are impossible. In this Zero Trust architecture, a sophisticated Network Access Control (NAC) platform—such as Aruba ClearPass or Cisco Identity Services Engine (ISE)—functions as the central Policy Decision Point (PDP)., When an IoMT device attempts to connect to the WLAN, the PDP verifies its cryptographic certificate, assesses its real-time security posture, and queries external databases (such as Mobile Device Management platforms) to confirm the device's health., Once identity is verified, the PDP enforces strict micro-segmentation by instructing the wireless LAN controller (acting as the Policy Enforcement Point, or PEP) to dynamically assign the device to a highly restricted Virtual Local Area Network (VLAN)., An infusion pump, for example, is segmented so it can only communicate with the specific pharmacy server managing drug libraries, strictly preventing any lateral access to other hospital subnets or patient databases[9][8][3]

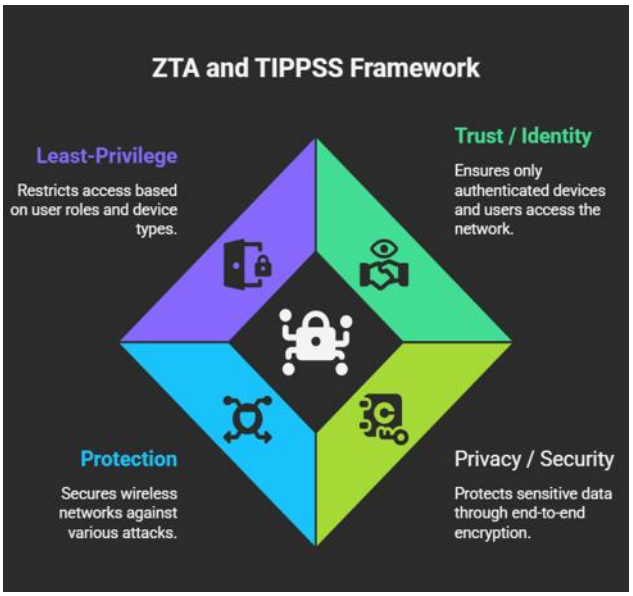

Figure 2: ZTA and TIPPSS

This EAP-TLS network admission control, WPA3-Enterprise link-layer defense, dynamic micro-segmentation breach isolation, and ASCON/TLS 1.3 application-layer E2EE synthesis builds a holistic, defense-in-depth architecture. In case a advanced persistent threat physically hacks the hospital premises, directly connects to an ethernet port, creates a rogue Wi-Fi network, the Zero Trust Architecture will not allow unauthorized network access, and the E2EE will make the data packet intercepted rendered semantically unintelligible via encryption.

7. Conclusion

The legacy WPA2 to WPA3-Enterprise is a fundamental, critical step in securing the wireless air interface of dense healthcare settings, effectively addressing long-standing, critical vulnerabilities, including offline dictionary attacks and frame spoofing. Nevertheless, the use of link-layer encryption only is also a significant architectural weakness that leaves extremely sensitive patient telemetry to internal network breaches, rogue infrastructure, and horizontal mobility. End-to-End Encryption (E2EE) in the application layer is without question mandatory to meet strict regulatory requirements of HIPAA and technical interoperability specifications of IEEE 2933 TIPPSS framework.

Although cryptographic protocols were computationally intensive and thus limited the performance of battery-constrained IoMT devices, the introduction of TLS 1.3 and the NIST-standardized ASCON lightweight cryptography algorithm have made robust and military-grade E2EE possible without compromising network latency or the important device lifespan. One of the biggest obstacles to the widespread and fast implementation of this architecture is the sheer scale of out-of-date medical gear, which simply cannot execute EAP-TLS certificates or run modern encryption ciphers, and thus requires sophisticated transition modes and continued risk acceptance. Moreover, the introduction of actual E2EE effectively renders the visibility tools of the traditional network useless, so the ancient Intrusion Detection Systems (IDS) cannot scan the packet payloads to detect malware signature.

The development of healthcare cybersecurity architecture should be directed towards supporting edge-assisted federated learning models, which identify localized anomalies using metadata analysis and traffic flow analysis, avoiding deep packet inspection of encrypted payloads. Moreover, the industry should focus on widespread deployment of post-quantum cryptography (PQC) algorithms, including ASCON-80pq, in order to protect sensitive and long-lasting patient health records against the looming threat of quantum-enabled, so-called harvest now, decrypt later attacks. The further development of the IEEE 2933 standard will play a key role in making manufacturers adopt such important cryptographic protections.

REFERENCES:

1. IEC, "Application of Risk Management for IT-Networks Incorporating Medical Devices," *IEC 80001-1*, 2021.
2. IEEE, "IEEE/UL Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS—Trust, Identity, Privacy, Protection, Safety, and Security," *IEEE/UL 2933-2024*, 2024.
3. A. P. Singh and M. Singh, "Handshake Comparison Between TLS V 1.2 and TLS V 1.3 Protocol," *Cyber Security in Intelligent Computing and Communications*, 2022.
4. NIST, "Ascon-Based Lightweight Cryptography Standards for Constrained Devices," *NIST Special Publication 800-232*, 2023.
5. E. P. Obrik-Uloho et al., "Zero-Trust Architecture for Smart Hospitals: A Virtual Blueprint for Cyber-resilient Healthcare Infrastructure," *Archives of Current Research International*, 2025.
6. A. Alluhaidan and P. Prabu, "End-to-end encryption in resource-constrained IoT device," *IEEE Access*, 2023.
7. A. Halbouni et al., "Wireless Security Protocols WPA3: A Systematic Literature Review," *IEEE Access*, 2023.
8. R. R. K. Chaudhary and K. Chatterjee, "Safeguarding IoT Big Data: Lightweight End-to-End Encryption for Enhanced Security," *2024 First International Conference on Data, Computation and Communication (ICDCC)*, 2024
9. Obrik-Uloho, "Zero Trust in Healthcare," 2025
10. D. Eastlake, "Transport Layer Security (TLS) 1.3," RFC 8446, 2018
11. E. Rescorla, "DTLS 1.3," IETF RFC 9147, 2022.
12. Cisco, *Zero Trust for Healthcare Networks*, 2024.

13. Fortinet, *Secure Healthcare IoMT with Zero Trust*, 2025.
14. Gartner, *Future of Cloud Security and SASE*, 2025.