CHAPTER 1
INTRODUCTION

1.1 Background

The Internet of Things (IoT) is a network of interconnected physical devices that communicate over the internet, enabling users to monitor, interact with, and control them remotely. In recent years, IoT has experienced rapid growth, expanding its presence into various domains such as health, smart homes, transportation, and industrial automation. This widespread adoption positions IoT as a foundational technology for the future. IoT devices are typically equipped with sensors that continuously collect data and transmit it via the internet for purposes such as real-time monitoring, automation, and decision-making [1], As a result, IoT has driven the emergence of smart city innovations and Industry 4.0 applications, particularly in health. The health sector leverages IoT to enhance remote patient monitoring, automated medication dispensing, early disease detection, and dynamic treatment strategies. This evolution has given rise to Medicine 4.0 and health 4.0, both of which aim to revolutionize medical services by integrating real-time data analytics and automation [2]. One of the key technologies underpinning health 4.0 is the Internet of Health Things (IoHT), which connects medical devices, sensors, and hospital information systems to facilitate seamless health operations. Secure information sharing among medical professionals is critical to enhancing diagnostic accuracy, treatment efficiency, and patient outcomes [2] [3].

IoHT architectures typically rely on lightweight application-layer protocols such as MQTT and CoAP, which are chosen for their efficiency in constrained environments. Among these, MQTT is publish-subscribe model and TCP based reliability has emerged as the most widely adopted in health IoT systems [4]. MQTT is widely recognized as the most suitable protocol for transmitting patient health data in IoT-based healthcare systems. It is publish-subscribe architecture ensures efficient communication in multi-subscriber environments, and its support for multiple Quality of Service (QoS) levels guarantees reliable message delivery. This is a critical requirement in medical applications. Moreover, MQTT's lightweight nature and broad adoption across healthcare platforms make it the preferred choice for robust and scalable health data communication. While CoAP offers benefits such as lower latency and reduced energy consumption, particularly advantageous for ultra-low-

power devices, it lacks the delivery guarantees and flexibility provided by MQTT. Therefore, in scenarios where data reliability, real-time monitoring, and scalability are essential, MQTT stands out as the superior protocol [4].

In addition to MQTT and CoAP, another relevant protocol in IoT environments is AMQP (Advanced Message Queuing Protocol), which supports robust queuing mechanisms and reliable message delivery with built-in security and interoperability features. However, AMQP is significantly more resource-intensive than MQTT or CoAP, making it less suitable for low-power and embedded medical devices [4].

Table 1.1. Comparison of IoT Protocols in *IoHT* Communication Scenarios

Protocol	**Communication Model**	**Transport Layer**	**Strengths**	**Limitations**
MQTT	Publish-Subscribe	TCP	Lightweight, reliable, and scalable for real-time multi-subscriber communication.	No built-in encryption or metadata protection (requires external security layers).
CoAP	Request-Response	UDP	Extremely lightweight. Low latency and energy efficient. Good for short-lived sensor data.	No native support for publish-subscribe. Limited reliability and sequencing. Less robust for continuous streaming.
AMQP	Queuing / Publish-Subscribe	TCP	Built-in security and reliable message delivery. Suitable for enterprise-level integration.	Complex protocol stack. High computational and memory overhead. Not optimized for constrained devices.

CoAP, which follows a request-response model over UDP, is excellent for simple, short-lived communications in constrained environments. However, it lacks native support for asynchronous messaging, which is often required in health scenarios that involve continuous sensor data streaming or alerts. Furthermore, many IoHT applications require real-time responsiveness and low-latency communication. These attributes are difficult to achieve when traditional security layers such as TLS are applied, due to the associated computational overhead [5]. This makes the need for lightweight, embedded-friendly security approaches even more urgent, especially for remote or wearable medical devices.

In contrast, MQTT provides a persistent, bidirectional, publish-subscribe communication model, enabling real-time updates with minimal overhead. Furthermore, MQTT's support for Quality of Service (QoS) levels allows flexible trade-offs between delivery assurance and network resource consumption. This is critical for balancing reliability and efficiency in health settings. Given these characteristics, MQTT is considered the most appropriate protocol for IoHT systems, where continuous patient monitoring, scalability, and reliability under bandwidth constraints are top priorities. Its ability to operate efficiently on limited hardware resources and

across unstable network conditions makes it ideal for both in-hospital and remote health monitoring applications.

Health-specific IoT systems are often built on architectures that include layers such as perception (sensor), network (connectivity), and application (service delivery). Middleware and service-oriented layers are also integrated to manage quality of service (QoS), security, and interoperability [6]. Within these architectures, IoHT devices are categorized based on capabilities, ranging from low-power embedded nodes like ESP8266 and Arduino, to gateway-level processors like Raspberry Pi. These devices must operate with minimal power, compute, and memory, requiring efficient software stacks and real-time protocols to ensure responsiveness and reliability in clinical settings [6].

Indonesia has begun to explore the implementation of IoHT, particularly in response to the growing demand for digital health solutions. Government initiatives, such as the development of Smart Hospitals and the integration of telemedicine platforms, demonstrate Indonesia's commitment to digital health transformation. Several hospitals and health providers have adopted IoT-based patient monitoring systems, enabling real-time tracking of vital signs and remote consultations. Indonesia's Ministry of Health has also promoted the use of electronic medical records (EMR) and IoT-driven diagnostics to improve health accessibility, especially in rural areas. Examples of IoHT Implementation in several hospitals in Indonesia have started implementing IoHT technologies:

1. **Rumah Sakit Universitas Indonesia (RSUI), Depok**
   RSUI has introduced *RSUI Telmon AI*, a telemedicine platform that integrates Artificial Intelligence (AI) and IoHT (Internet of Health Things). This system enables remote health monitoring, allowing doctors to track patients' vital signs in real time, enhancing diagnostic accuracy and patient care.

Fig. 1.1. Info Implementation IoHT in MMC Hospital.

2. **Rumah Sakit MMC (Metropolitan Medical Centre), Jakarta**
   RS MMC collaborates with XL Axiata Business Solutions to deploy *Smart Health* solutions. These include IoT-based medical devices for patient wellness monitoring, aiming to improve preventive care and chronic disease management.

3. **Waron Hospital, Surabaya**
   Waron Hospital has implemented *Smart Hospital* solutions, integrating robotic automation, IoT-driven patient monitoring, and electronic health records (EHR) to improve hospital operations and medical services.

Fig. 1.2. Info Implementation IoHT in Warron Hospital.

Among the various communication protocols adopted on the Internet of Things (IoT), the Message Queuing Telemetry Transport (MQTT) protocol is widely utilized due to its lightweight, publish-subscribe architecture that supports efficient communication in bandwidth-constrained and resource-limited environments [7] [8] [9] [10]. To secure data transmission in MQTT-based systems, the ASCON cipher suite is used as a lightweight cryptographic solution offering efficient authenticated encryption. ASCON, a finalist in the NIST standardization for lightweight cryptography, offers Authenticated Encryption with Associated Data (AEAD) and cryptographic hashing capabilities. It includes ASCON-128 and ASCON-128a [11], both of which provide 128-bit security while maintaining a low hardware footprint, making them well-suited for resource-constrained scenarios, including Internet of Health Things (IoHT) applications [12].

Recent studies have confirmed the practical effectiveness of ASCON in real-world MQTT-based Health systems, demonstrating significantly lower encryption overhead and latency compared to conventional solutions like AES-GCM and TLS. In particular, ASCON outperforms TLS by up to 11 times in terms of efficiency when applied to small to medium-sized health data packets. These findings are supported by experimental implementations using realistic edge computing environ-

ments involving Raspberry Pi, NVIDIA Jetson, and 5G test networks [7], affirming ASCON's suitability for performance-sensitive applications such as Remote Patient Monitoring (RPM).

Table 1.2. Comparison of Cryptographic Schemes for MQTT-Based Health Systems

Criteria	**AES-GCM**	**TLS 1.2**	**ASCON-128 (Proposed)**
Encryption Latency (small data)	Medium	High	Lowest
Encryption Latency (2KB data)	High	High	Moderate
Computational Overhead	High	Very High	Low
Suitability for Constrained Devices	Low	Very Low	High
Ease of Implementation	Moderate	Complex (certs, handshake)	Simple (in-place AEAD)
Protocol Compatibility	Full	Requires TLS support	Full (TLS-free)
Efficiency in Real Deployment	Acceptable	Poor	Excellent

While ASCON effectively secures the message payload by ensuring confidentiality, integrity, and authentication, it does not encrypt the Associated Data (AD), such as device ID, client identifiers, Quality of Service (QoS) levels, data type or sensor type, location ID or room number, and timestamp fields. These elements remain exposed during transmission. This unprotected metadata can potentially be intercepted or manipulated by unauthorized parties, leading to privacy breaches or tampering with message routing. As depicted in Figure 1.3, the timeline of cybersecurity incidents in the health sector highlights a consistent growth in both the frequency and severity of attacks. These range from early denial-of-service (DoS) attacks and identity theft to modern ransomware threats such as WannaCry. Such breaches have affected millions of patient records globally and emphasize the critical need for robust data protection mechanisms, particularly in IoHT deployments where sensitive medical data is continuously transmitted.

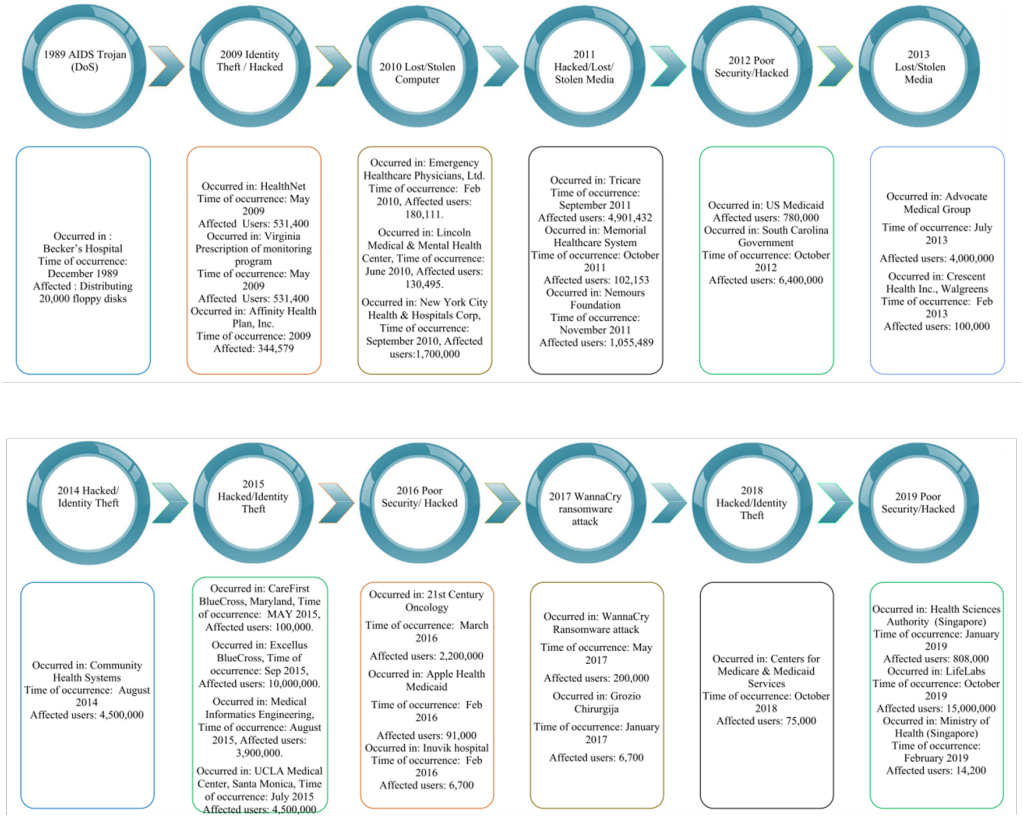

Fig. 1.3. Timeline of security attacks on health data.

To address the exposure of metadata in MQTT-based IoHT communication, this study introduces an approach by collaborating ASCON with a covert channel technique based on ZWC. While ASCON ensures protection of the message payload, the proposed method extends this security to include metadata confidentiality without altering the MQTT protocol structure. By invisibly embedding sensitive metadata, such as device ID, client identifiers, Quality of Service (QoS) levels, data type or sensor type, location ID or room number, and timestamp fields into textual fields using ZWC, the system provides an additional layer of privacy. This approach helps protect against traffic analysis and metadata inference attacks.

The proposed method is evaluated through simulation based on indicators, including latency, avalanche effect, and computational overhead. The results confirm that this approach strengthens end-to-end security in health data exchange scenarios and privacy-preserving protection for real-time medical communication over MQTT.

This research aims to enhance the security of medical data transmission by collaborating covert channels with AEAD encryption using ASCON to develop a highly secure health communication system. The main contributions of this research are as follows:

- Proposes the enhancement of ASCON by improving the security of the Associated Data (AD) component, such as device identifiers, sensor types, Quality of Service (QoS) levels, and timestamps. This is achieved using a covert channel mechanism based on ZWC, with the goal of strengthening metadata confidentiality in ASCON based IoHT communication.

This research contributes to the field of IoHT security by enhancing secure communication to ensure both payload protection and metadata confidentiality, thereby addressing a critical gap in MQTT-based IoT security.

1.2 Statement of Problem

The rapid adoption of the Internet of Things (IoT) in health applications has significantly improved medical services through real-time patient monitoring, remote diagnostics, and automated health data management. This transformation, often referred to as the Internet of Health Things (IoHT), relies on lightweight messaging protocols such as Message Queuing Telemetry Transport (MQTT) to facilitate communication between medical devices and health providers [13]. As sensitive medical data is continuously exchanged across these systems, ensuring data confidentiality, integrity, and authenticity becomes critical, especially in resource-constrained environments.

Traditional cryptographic protocols such as Transport Layer Security (TLS) offer encryption but are often unsuitable for IoHT due to their high energy consumption and computational requirements. In contrast, lightweight encryption schemes like ASCON Authenticated Encryption with Associated Data (AEAD) provide more practical solutions for IoT environments. Among them, ASCON has been standardized by NIST as a lightweight cipher due to its efficient performance and robust security [14]. ASCON effectively secures the payload by providing confidentiality, integrity, and authentication while operating efficiently on constrained devices.

However, ASCON does not encrypt metadata (Associated Data, AD), which means that certain fields remain exposed. This exposed metadata poses a security risk, as it can be intercepted, analyzed, or manipulated by unauthorized parties. Such exposure may potentially reveal patient identity, health conditions, or device interactions, even without accessing the encrypted payload. These metadata inference attacks represent a significant threat to privacy in real-world IoHT deployments. To mitigate this issue, ZWC as a covert channel technique have been explored as an additional security mechanism to hide metadata within seemingly

normal network communication [15]. ZWC techniques can be used to conceal sensitive metadata information within MQTT packets, messages without altering the protocol's structure, providing an additional layer of confidentiality to the associated data, making it difficult for attackers to detect and analyze communication patterns. This approach offers a solution for securing both payload and metadata in IoHT communication.

1.3 Research Objectives

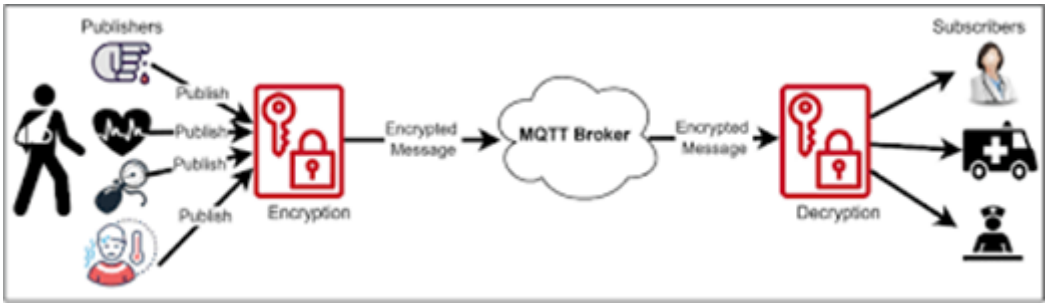

Fig. 1.4. IoHT with MQTT Protocol.

The objective of this research is to improve the security of communication in MQTT-based Internet of Health Things (IoHT) systems by proposing a dual-layer security approach for both payload and metadata. This approach collaborates the ASCON scheme with a covert channel technique based on ZWC, focusing on protecting Associated Data (AD) such as device identifiers, sensor types, Quality of Service (QoS) levels, and timestamps, without modifying the MQTT protocol structure, thereby enhancing both the confidentiality and integrity of the data.

While ASCON ensures confidentiality, integrity, and authentication of the message payload, metadata such as topic names, client identifiers, QoS levels, and timestamps remain exposed and vulnerable to traffic analysis or inference attacks. To address this, the proposed method embeds sensitive metadata invisibly within textual fields using ZWC, without changing the MQTT protocol format. Additionally, ASCON-HASH is incorporated as a lightweight cryptographic hash function, increasing unpredictability and enhancing security by randomizing or obscuring metadata patterns before embedding them. This reduces the risk of detection through statistical or pattern-based analysis. This system not only addresses conventional security threats but also anticipates post-quantum attacks by implementing dynamic key and nonce updates to enhance forward secrecy. The approach is tested in an MQTT-based IoHT environment, focusing on use cases like remote patient monitoring and hospital automation.

1.4 Scope of Work

This research focuses on enhancing the AEAD (Authenticated Encryption with Associated Data) functionality of ASCON within MQTT-based Internet of Health Things (IoHT) communication, specifically targeting the protection of Associated Data (AD) such as metadata. The enhancement is achieved by integrating a covert channel technique using ZWC to conceal sensitive metadata (e.g., device ID, client identifiers etc) without altering the MQTT protocol structure. The scope of this study includes:

1. Enhancing ASCON for Metadata Protection
   This research focuses on improving the handling capabilities of Associated Data (AD) in ASCON for MQTT-based IoHT communication. While ASCON securely encrypts the payload, metadata such as device ID, client identifiers, etc., remain exposed. This study aims to address this gap by collaborating ASCON with additional covert protection techniques.

2. Zero-Width Character (ZWC) Collaboration as Covert Channel
   A covert channel method using ZWC will be applied to conceal sensitive metadata within the textual fields of MQTT packets. This collaboration enables the hiding of metadata without modifying the MQTT protocol structure, ensuring compatibility and lightweight operation.

3. Design and Prototype Implementation
   The study will design a framework that collaborates ASCON encryption and ZWC-based metadata hiding within an MQTT-based communication setup for IoHT applications.

4. Security and Performance Evaluation
   Evaluations will focus on latency, avalanche effect, and computational overhead as key indicators.

5. Experimental Simulation Setup
   Testing will be conducted using devices such as three laptops and local MQTT brokers to emulate secure medical data transmission scenarios.

6. Scope Limitations
   This research focuses solely on the software-level implementation of ASCON and its collaboration with covert channel techniques in MQTT communication. It does not involve hardware-based security modules such as Hardware

Security Elements (HSE) or Secure Enclaves, and excludes other IoT protocols like CoAP, AMQP, or HTTP. Furthermore, advanced anti-detection methods designed to counter sophisticated traffic analysis tools are considered outside the scope of this study.

1.5 Hypothesis

This research hypothesizes that integrating ASCON for payload protection with ZWC for metadata concealment in MQTT-based IoHT communication will enhance data security. The expected outcomes include improved confidentiality and integrity of both payload and metadata, with a slight improvement in the avalanche effect, increasing resilience against metadata inference attacks. By encrypting the payload and invisibly embedding sensitive metadata, such as device IDs, client identifiers, QoS levels, and timestamps, this method aims to mitigate the risk of traffic analysis and maintain full compatibility with the MQTT protocol. Through experimental validation and performance evaluation, this study will demonstrate that the proposed enhancement offers a safer solution for securing sensitive health data communications in resource-constrained IoHT environments.

1.6 Research Methodology

The methodology used in conducting research is based on the division of work packages as follows:

1. **Literature Study**
   This research begins with a literature review and problem analysis to identify security vulnerabilities in MQTT-based IoHT communication, focusing on payload confidentiality and metadata exposure risks. It evaluates existing security mechanisms, such as ChaCha20-Poly1305, AES-based encryption, and ASCON implementations, highlighting their limitations in protecting metadata from traffic analysis and inference attacks.

2. **System Design**

   - Design a secure MQTT communication model by integrating ASCON with covert channels to enhance metadata protection.
   - Develop a covert channel mechanism to embed metadata within MQTT messages, ensuring invisibility while preserving message integrity.

- Implement ASCON-128 AEAD, optimized for optimal functionality in resource-constrained IoHT environments.

3. **Method Implementation** Use Python to integrate ASCON and covert channels into an MQTT-based communication platform.

4. **Simulation and Performance Analysis** Evaluate Avalanche Effect to ensure confidentiality and integrity, and latency also computational overhead to assess system availability and performance.