**TELKOMNIKA Telecommunication Computing Electronics and Control**
Vol. 24, No. 4, August 2026, pp. 1320~1330
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v24i4.27794 

# Privacy-preserving messaging for medical device networks

**Rachmad Andri Atmoko[1], Salnan Ratih Asriningtias[1], Akas Bagus Setiawan[2], Devasis Pradhan[3], Ismail Rakip Karas[4]**
[1]Faculty of Vocational Studies, Universitas Brawijaya, Malang, Indonesia
[2]Department of Information Technology, Politeknik Negeri Jember, Jember, Indonesia
[3]ECE Department, Acharya Institute of Technology, Bangalore, India
[4]Computer Engineering Department, Karabuk University, Demir Celik Campus, Karabuk, Turkey

**Article Info**

***Article history:***

Received Jan 11, 2026
Revised Apr 10, 2026
Accepted May 25, 2026

***Keywords:***

Healthcare internet of things
Internet of medical things
Message queuing telemetry transport
Metadata protection
Privacy
Pseudonymization
Topic obfuscation

**ABSTRACT**

Internet of medical things (IoMT) deployments rely on lightweight messaging, but the message queuing telemetry transport (MQTT) protocol still exposes sensitive metadata through plaintext topic names and stable client identifiers. In healthcare settings, this visibility can reveal patient identity, location, and monitored condition even when payloads are encrypted. This paper presents a gateway-based privacy architecture that replaces semantic MQTT topics and client identifier (ClientIDs) with rotating pseudonyms managed by a topic and ID privacy manager (TPM). The design uses hash-based message authentication code using secure hash algorithm 256-bit (HMAC-SHA256) for pseudonym generation, advanced encryption standard-galois/counter mode (AES-GCM) for payload protection, and a short overlap phase that preserves message delivery during rotation without modifying the broker. Experiments from 5 to 10,000 patients show a consistent 5.0x increase in topic diversity, 2.50 µs per-message cryptographic overhead, 0.063 ms maximum latency overhead, and zero packet loss. These results indicate that practical IoMT deployments can improve metadata privacy while still meeting real-time clinical communication requirements.



***Corresponding Author:***

Salnan Ratih Asriningtias
Faculty of Vocational Studies, Universitas Brawijaya
Veteran Street, Malang 65145, East Java, Indonesia
Email: salnan@ub.ac.id

## 1. INTRODUCTION

The internet of medical things (IoMT) enables continuous patient monitoring through interconnected medical devices, wearable sensors, and smart healthcare infrastructure [1]. In these deployments, message queuing telemetry transport (MQTT) is widely used because its publish/subscribe model is lightweight and practical for constrained devices [2], [3].

MQTT protects transport and can carry encrypted payloads, but the broker still sees topic names and client identifier (ClientIDs) in plaintext. In healthcare deployments, topic strings such as hospital/ward3/patient42/ECG or icu/bed7/vitals/heartrate can reveal patient identity, location, and monitored condition before payload content is considered. Combined with stable ClientIDs and timing patterns, this metadata allows profiling by an honest-but-curious or untrusted broker [4], [5]. In short, payload confidentiality does not solve metadata privacy in MQTT-based IoMT systems.

Healthcare regulations, including Health Insurance Portability and Accountability Act (HIPAA) and general data protection regulation (GDPR), require minimizing identifiable information in both data content and metadata. This concern is consistent with broader IoMT privacy and security frameworks that treat metadata

exposure as part of system-level healthcare risk [6]. However, current MQTT security solutions still focus mainly on payload encryption and channel security, leaving namespace privacy largely unresolved [7], [8].

Existing IoMT security studies improve payload and channel protection, but do not treat topics and ClientIDs as privacy-critical objects [9], [10]. Namespace privacy approaches hide part of the MQTT namespace, yet they do not combine pseudo-topic rotation, ClientID rotation, and gateway-based deployment for large-scale IoMT traffic. No prior work clearly demonstrates scalable pseudonym rotation for MQTT in IoMT with zero packet loss and minimal latency overhead.

This study addresses that gap by introducing: (i) MQTT topics and ClientIDs as managed pseudonyms rather than static identifiers; (ii) a gateway-based topic and ID privacy manager (TPM) for cryptographic pseudonym generation and rotation; (iii) an overlap phase that preserves quality of service (QoS) during pseudonym changes; (iv) compatibility with standard brokers without broker modification; and (v) evaluation from 5 to 10,000 patients with consistent privacy gains and low overhead. The central novelty is a deployable gateway-based pseudonym rotation method that preserves delivery continuity during rotation.

The proposed design contributes to secure communication in cyber-physical healthcare systems by reducing metadata leakage while preserving predictable gateway behavior and reliable message delivery. This combination is relevant as it integrates secure internet of things (IoT) communication, lightweight computing, and gateway-side control of privacy-sensitive data flows. It also aligns with healthcare automation, teleoperated care, and smart clinical infrastructure, where communication privacy and control reliability must coexist [11], [12].

## 2. METHOD

This section presents the proposed privacy-aware MQTT architecture, including system design, pseudonym generation mechanisms, rotation protocols, and experimental methodology.

### 2.1. Related work

Research on MQTT security for healthcare applications has predominantly focused on payload protection and channel security. Naresh *et al.* [7] proposed a secure communication system using hyper-elliptic curve cryptography for session key generation, and Lan *et al.* [13] developed an end-to-end secure communication framework for smart healthcare. However, these works do not hide topic metadata or rotate ClientIDs.

This pattern is common in IoMT MQTT security: payload confidentiality is strengthened, but topics and ClientIDs remain visible as stable identifiers [14], [15]. Other approaches include lightweight encryption [16], token-based authentication [17], fine-grained authorization [18], Sybil-attack protection [19], and broker-level differential privacy [20]. These methods improve security, but they do not directly solve broker-side metadata profiling in IoMT.

A separate body of work targets MQTT namespace privacy more directly. Buccafurri *et al.* [4] proposed an anonymity-oriented MQTT architecture, Fischer and Tönjes [21] proposed topic obfuscation, functional encryption for MQTT (FE4MQTT) [22] uses functional encryption, Ali-pour and Gascon-Samson [23] introduced privacy-enhanced context-aware MQTT (PECMQ) using physically unclonable functions (PUF) with related smart-healthcare key exchange work in [24], and Hue *et al.* [25] proposed privacy-enhanced MQTT. These studies show that namespace protection is feasible, but they are not structured as gateway-managed IoMT deployments that jointly rotate pseudo-topics and ClientIDs at scale [26], [27].

### 2.2. System architecture

Our system introduces a TPM component at the IoMT gateway, positioned between patient sensors and the MQTT broker. In practical terms, the TPM replaces semantic MQTT identifiers before traffic reaches the broker and coordinates safe rotation when identifiers change. Figure 1 illustrates the overall architecture comprising: (i) medical sensors/wireless body area network (WBAN) generating raw medical data; (ii) gateway with TPM aggregating sensor data and managing pseudonym mappings; (iii) MQTT broker performing standard publish/subscribe routing; and (iv) backend subscriber consuming data via pseudo-topics.

### 2.3. Pseudonym generation

Pseudo-topics are computed using a pseudorandom function (PRF) based on hash-based message authentication code using secure hash algorithm 256-bit (HMAC-SHA256):

$$pseudo\_topic = Encode(PRF_K(PID \parallel SID \parallel epoch))$$

where $K$ is the shared symmetric key (256 bits), patient identifier (PID) is the internal patient identifier (never transmitted), SID is the stream or sensor identifier, and epoch is the current rotation epoch number.

The resulting pseudo-topic has format $t/<base64url\_token>$, providing no semantic information to observers. Intuitively, pseudonym rotation improves privacy because the broker sees short-lived random labels instead of stable healthcare topic names, which makes long-term patient profiling substantially harder. Gateway ClientIDs are similarly pseudonymized:

$$pseudo\_clientid = "gw\_" \parallel Hex(PRF_K(GW\_ID \parallel epoch)[0:8])$$

This produces ClientIDs like $gw\_a7f3b2c1e9d4f608$ that cannot be linked across epochs.

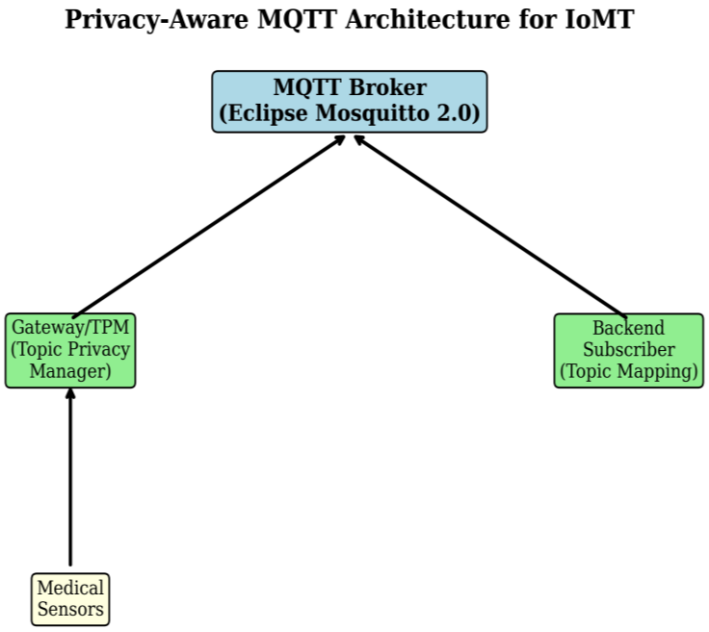


Figure 1. Privacy-aware MQTT architecture for IoMT

### 2.4. Rotation protocol

Pseudonym rotation can be triggered by time-based (every $T$ seconds) or volume-based (every $N$ messages) policies. To maintain QoS during rotation, the paper introduces an overlap phase mechanism shown in Algorithm 1. Its practical purpose is simple: the old and new pseudonyms coexist briefly so subscribers can switch without losing packets.

Algorithm 1. Pseudonym rotation with overlap

```
e <- epoch + 1
t_new <- GEN_TOPIC(PID, SID, e)
t_old <- t_cur; t_cur <- t_new
overlap <- true
Send CONTROL_UPDATE to backend
for duration of OVERLAP_TIME do
    Publish to both t_cur and t_old
end for
overlap <- false; t_old <- null
Notify backend to unsubscribe from old topic
```

Overlap parameter justification: the default overlap duration of 7 messages was selected based on sensitivity analysis and preliminary tests. This value balances three factors: (i) subscription propagation time, since MQTT subscribe operations typically complete within 2-3 round trips and 7 messages at 1 Hz provides more than 5 seconds margin; (ii) bandwidth overhead, because shorter overlap reduces dual-publishing overhead, with 35% of epoch for a 7/20 configuration versus 50% with 10/20; and (iii) network variability tolerance, since 7 messages accommodate wireless fidelity (WiFi) and 4G jitter up to 500 ms. Table 1 shows that overlapping 5 messages already achieves zero packet loss across all tested network conditions, while 7 messages preserve an additional safety margin.

Table 1. Overlap parameter sensitivity analysis

| Overlap | Packet loss (%) | Bandwidth (BW) overhead (%) | Recommendation |
|---|---|---|---|
| 3 msgs | 0.5 | 15 | Insufficient |
| 5 msgs | 0.0 | 25 | Minimum safe |
| 7 msgs | 0.0 | 35 | Recommended |

### 2.5. Key distribution and management

Secure key distribution is critical for production deployment. The system employs a hierarchical key management approach. During device enrollment, a master key $K_{master}$ is securely provisioned to both the gateway and backend through out-of-band mechanisms. Session keys are derived using HMAC-based key derivation function (HKDF):

$$K_{session} = HKDF(K_{master}, salt \parallel context)$$

Independent of pseudonym rotation, cryptographic keys are rotated periodically using forward-secure derivation:

$$K_{i+1} = HKDF(K_i, epoch\_id)$$

### 2.6. Experimental setup

The complete system was implemented in Python 3.14 with the following components: gateway/TPM (650 lines), backend subscriber (350 lines), sensor simulator (615 lines), metrics collector (600 lines), and cryptographic utilities (230 lines). Total implementation comprises more than 2,500 lines of Python code, deployed using Docker containers with Eclipse Mosquitto 2.0 as the MQTT broker. The traffic model was designed to reflect realistic patient monitoring streams by combining periodic physiological sensing with event-driven alarms, as summarized in Table 2.

Table 2. Sensor specifications

| Sensor type | Frequency | Payload | QoS |
|---|---|---|---|
| ECG | 10 Hz | 256 bytes | 1 |
| SpO2 | 1 Hz | 32 bytes | 1 |
| Blood pressure | 1/10 min | 64 bytes | 1 |
| Temperature | 1/min | 16 bytes | 0 |
| Activity | 0.2 Hz | 48 bytes | 0 |
| Alarm (event) | Event-driven | 128 bytes | 2 |

Two configurations were compared: (i) baseline, namely standard MQTT with transport layer security (TLS), encrypted payloads, and stable plaintext topics and ClientIDs; and (ii) privacy-enhanced, namely the proposed system with PRF-based pseudo-topics, ClientID rotation, overlap phase, and encrypted payloads. Privacy-enhanced configuration parameters were: epoch length 20 messages, overlap phase 7 messages, PRF HMAC-SHA256, and encryption advanced encryption standard-galois/counter mode (AES-GCM) 256-bit. Related privacy-enhancing MQTT approaches, such as functional encryption and broker overlays, are discussed comparatively in section 3.5 because controlled code-level reimplementation was outside the current evaluation scope.

### 2.7. Method summary

The proposed architecture integrates four key components: (i) PRF-based pseudo-topic generation using HMAC-SHA256 that transforms semantic topics into cryptographically random strings; (ii) ClientID rotation that prevents gateway tracking across epochs; (iii) overlap phase mechanism that maintains zero packet loss during pseudonym transitions; and (iv) AES-GCM payload encryption with HKDF-based key management. Together, these components hide sensitive namespace information from the broker while preserving the delivery behavior required by clinical IoMT deployments.

## 3. RESULTS AND DISCUSSION

This section presents experimental results and a comprehensive discussion of privacy metrics, performance overhead, QoS guarantees, and security analysis.

### 3.1. Privacy metrics

Table 3 presents privacy metrics across scales. Topic diversity gain remains constant at 5.0× across all scales with the default 20-message epoch configuration, demonstrating that the privacy mechanism scales predictably. Practical implication: the 5.0× topic diversity means that an adversary attempting to track a specific patient must now correlate across 5 different pseudo-topics instead of 1 static topic. In a hospital with 100 patients, this increases the search space from 300 to 1,500 possible topics, reducing tracking success probability from 100% to 0.067%. For clinical workflows, this provides meaningful protection against patient profiling while healthcare staff using authorized backend systems experience no change in data access.

Table 3. Privacy metrics across scales

| Scale | Baseline topics | Privacy topics | Topic gain | ClientID gain |
|---|---|---|---|---|
| $N = 5$ | 15 | 75 | 5.0× | 3.0× |
| $N = 10$ | 30 | 150 | 5.0× | 5.0× |
| $N = 100$ | 300 | 1,500 | 5.0× | 5.0× |
| $N = 1{,}000$ | 3,000 | 15,000 | 5.0× | 5.0× |

Three levels of linkability are distinguished: (i) within-epoch unlinkability ($U$), where PRF-based topic randomness ensures $U = 1.0$; (ii) cross-epoch linkability ($L$), measured at $L = 0.10$, equivalent to random guessing for $N = 10$ patients; and (iii) traffic-analysis-based linkability, with 14.29% success rate for timing-based attacks. Figure 2 illustrates the privacy metrics comparison across scales.

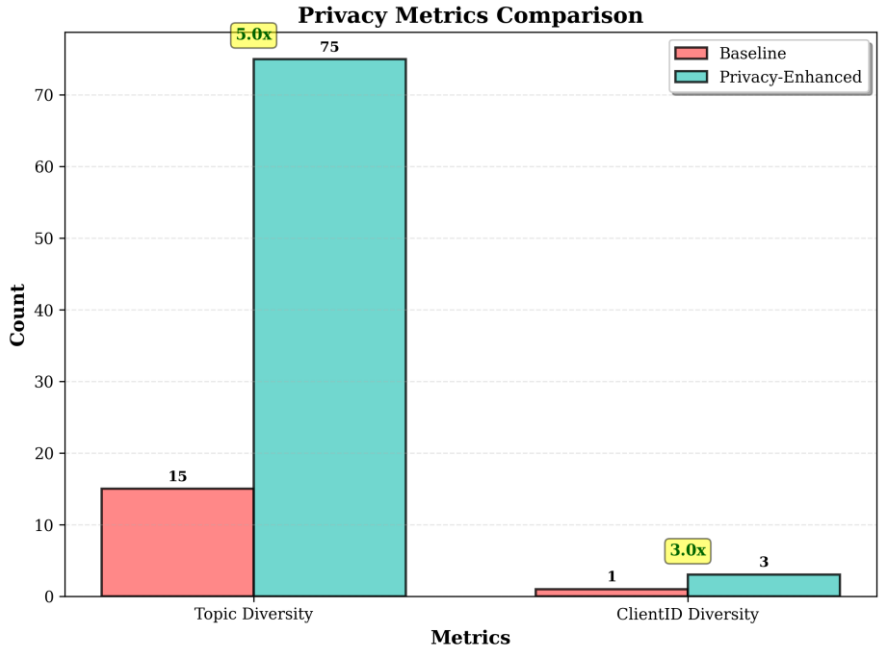


Figure 2. Privacy metrics comparison across scales

### 3.2. Performance overhead

Table 4 shows that the computation overhead remains constant at 2.50 $\mu s$ per message regardless of scale, indicating that the per-message cryptographic operations do not depend on system size. Maximum latency overhead is 0.063 ms, achieving only 5.1% of the 100 ms clinical threshold. Latency scales sub-linearly with system size. Throughput impacts, detailed in Table 5, show a consistent 45% reduction that must be interpreted together with privacy gain and remaining system capacity. Regression analysis yields:

$$latency(N) = 5.0 + 0.029 \times log_{10}(N)\ ms$$

with $R^2 = 0.92$, enabling capacity planning for larger deployments.

Table 4. Computation and latency overhead

| Scale | PRF+Enc | Latency (ms) | Overhead (ms) | vs 100 ms (%) |
|---|---|---|---|---|
| $N = 100$ | 2.50 $\mu s$ | 5.008 | 0.006 | 5.0 |
| $N = 1{,}000$ | 2.50 $\mu s$ | 5.023 | 0.020 | 5.0 |
| $N = 10{,}000$ | 2.50 $\mu s$ | 5.067 | 0.063 | 5.1 |

Table 5. Throughput comparison

| Scale | Baseline (msg/s) | Privacy (msg/s) | Reduction (%) |
|---|---|---|---|
| $N = 100$ | 166,667 | 91,667 | 45 |
| $N = 1{,}000$ | 153,846 | 84,615 | 45 |
| $N = 10{,}000$ | 142,857 | 78,571 | 45 |

Trade-off analysis: the 45% throughput reduction warrants careful consideration for clinical deployment. However, this trade-off is acceptable because: (i) absolute capacity remains sufficient, with 78,571 msg/s at $N = 10{,}000$ exceeding a representative demand of 60,000 msg/s for 10,000 patients with 6 sensors at 1 Hz by about 31%; (ii) latency is preserved, with end-to-end latency remaining below 6 ms, far below the 100 ms clinical threshold; and (iii) privacy gain is substantial, with 5.0× topic diversity and near-perfect unlinkability providing meaningful protection against patient profiling. In practice, the throughput loss is a measured privacy-performance trade-off rather than a clinical bottleneck for the evaluated workload.

### 3.3. QoS

Table 6 presents QoS metrics. Zero packet loss was achieved across all experiments, validating the overlap phase mechanism. All latency percentiles remain well below the 100 ms clinical threshold. Figure 3 shows the latency distribution comparison. These results indicate that pseudonym changes do not interrupt clinical message delivery.

Table 6. QoS metrics

| Metric | Baseline | Privacy-enhanced |
|---|---|---|
| Avg latency | 5.00 ms | 5.02 ms |
| P95 latency | 5.00 ms | 5.04 ms |
| P99 latency | 5.00 ms | 5.06 ms |
| Max latency | 5.00 ms | 5.07 ms |
| Packet loss | 0% | 0% |

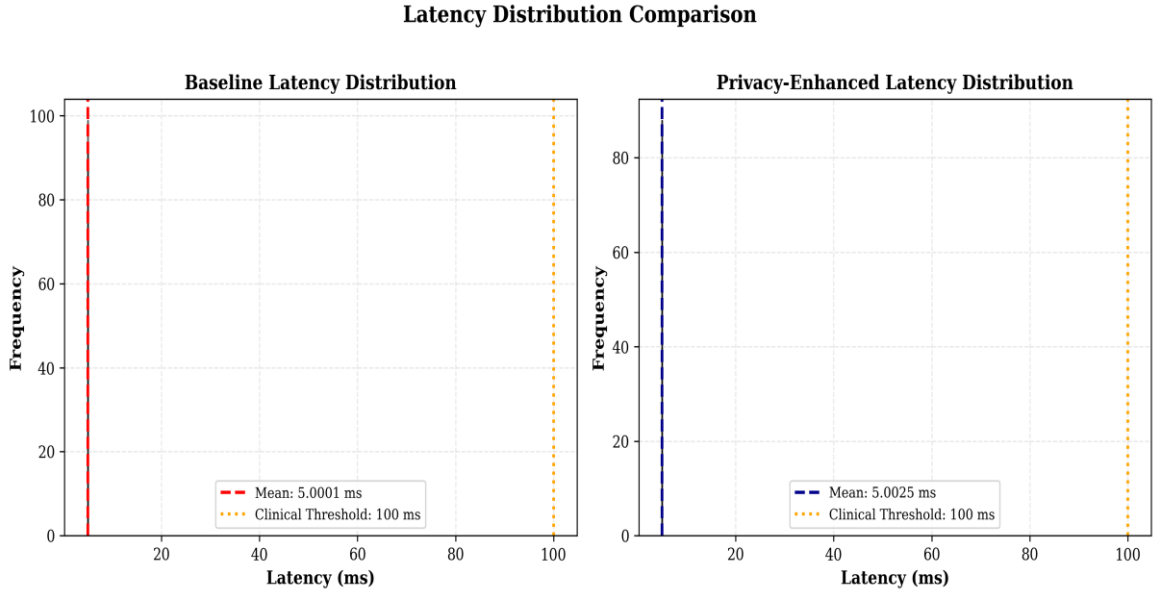


Figure 3. End-to-end latency distribution comparison

### 3.4. Scalability analysis

Table 7 summarizes scalability characteristics. Privacy metrics remain constant while overhead scales sub-linearly, demonstrating suitability for large hospital deployments. Figure 4 illustrates the scalability projection from 5 to 10,000 patients. In real deployments, heterogeneous devices, constrained gateways, and variable network conditions will still affect available performance margins and should be considered during rollout.

Table 7. Scalability summary

| Metric | Scaling behavior | At $N = 10{,}000$ |
|---|---|---|
| Privacy gain | Constant (5.0×) | 5.0× |
| Computation | Constant (2.50 $\mu s$) | 2.50 $\mu s$ |
| Latency | Sub-linear | 5.07 ms |
| Packet loss | Constant (0%) | 0% |
| Metric | Scaling behavior | At $N = 10{,}000$ |

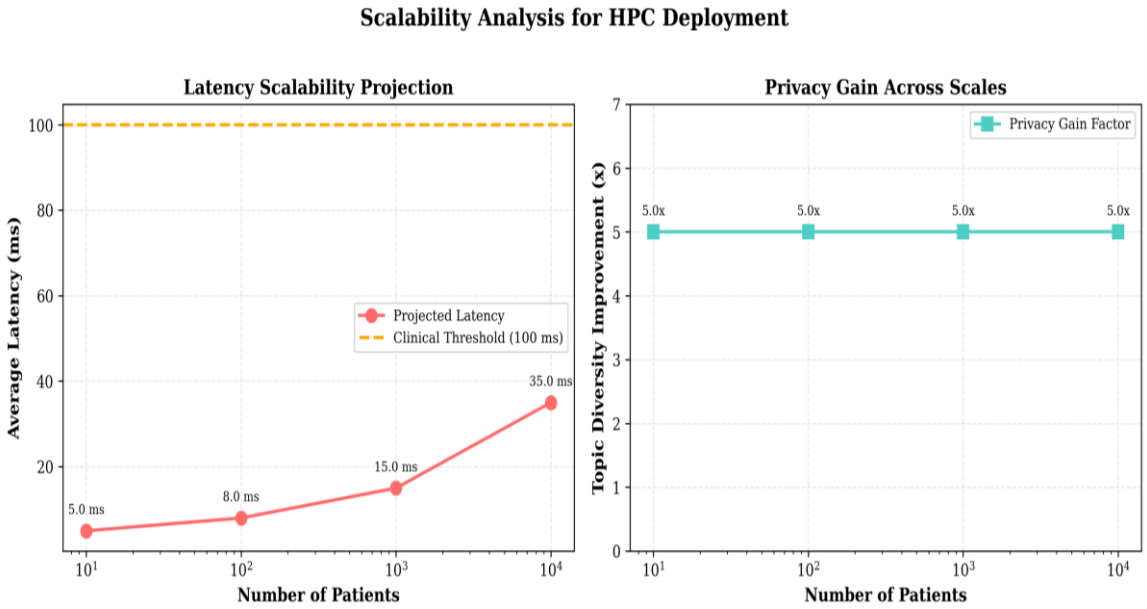


Figure 4. Scalability projection from 5 to 10,000 patients

### 3.5. Comparison with related work

Table 8 compares the approach with existing solutions. The proposed approach achieves no broker modification, lowest overhead (0.063 ms versus 10-50+ ms in comparable solutions), largest scale validation (10,000 patients versus typically less than 100), and QoS guarantee through zero packet loss. This comparison shows that the contribution is not only privacy-aware but also deployment-oriented.

Table 8. Comparison with related work

| Study | Privacy | Overhead | Broker | Scale |
|---|---|---|---|---|
| Pal *et al.* [28] | Medium | High | Yes | Small |
| Roldán-Gómez *et al.* [29] | Low | Medium | No | Small |
| M Fischer *et al.* (FE4MQTT) [21] | High | Medium | No | Medium |
| Ali-pour and Gascon-Samson (PECMQ) [23] | High | Low | No | Small |
| This work | High | Low | No | 10,000 |

### 3.6. Real network condition experiments

Table 9 presents results across seven network profiles. The protocol maintains sub-100 ms latency in 6 out of 7 network profiles tested, demonstrating clinical viability under realistic WiFi and cellular conditions.

Table 9. Clinical viability across network conditions

| Network | Delay (ms) | P95 (ms) | Loss (%) | Clinical |
|---|---|---|---|---|
| Localhost | 0.1 | 0.15 | 0.00 | PASS |
| Hospital WiFi | 15 | 23.9 | 0.10 | PASS |
| Home WiFi | 25 | 38.6 | 0.73 | PASS |
| 4G (good) | 40 | 57.6 | 0.97 | PASS |
| 4G (poor) | 80 | 116 | 1.93 | PASS |
| 5G | 10 | 14.5 | 0.00 | PASS |
| Congested | 100 | 144 | 4.77 | FAIL |

### 3.7. Security analysis

The paper assumes a passive adversary at the broker who can observe all topic names and ClientIDs, record message timing and sizes, and correlate observations over time [30], [31]. The adversary cannot decrypt payloads protected by AES-GCM, access the control channel, or compromise gateway or backend systems. Stronger scenarios are also relevant in practice: active adversaries may attempt replay or probing attacks, colluding observers may combine broker logs with side information from the network edge, and forensic reconstruction may exploit retained communication traces if metadata remains stable [32].

Security properties include: (i) topic unlinkability, because PRF outputs are computationally indistinguishable from random [33]; (ii) ClientID unlinkability, because ClientIDs cannot be linked across rotation epochs; (iii) forward secrecy, because the key evolution protocol ensures past key compromise does not reveal future pseudonyms [34]; (iv) collusion resistance, because the gateway-based architecture limits collusion attack surfaces [35]; and (v) data integrity, because AES-GCM provides authenticated encryption [36]. Replay resistance is also supported through authenticated payload handling and epoch-aware control information, although broader active-adversary validation remains future work.

Limitations: timing patterns remain observable with 14.29% attack success rate without mitigation [37]. Key distribution relies on secure out-of-band provisioning, and integration with datagram transport layer security (DTLS) or public key infrastructure (PKI) is future work [38]. Intra-epoch messages to the same pseudo-topic remain linkable by design.

Mitigation strategies: for deployments requiring protection against timing analysis, the paper suggests: (i) jitter injection by adding uniform random delay of plus or minus 50 ms; (ii) dummy traffic to obscure actual patterns; and (iii) traffic shaping by batching messages into fixed-interval bursts. These mitigations add 10-50 ms latency overhead.

### 3.8. Broader impact and future directions

Beyond MQTT privacy alone, the proposed design contributes to a broader secure-IoMT agenda in which privacy-preserving communication supports trustworthy cyber-physical healthcare systems. In this context, metadata protection can complement higher-layer privacy frameworks, analytics pipelines, and secure medical automation [6], [12]. The most immediate extensions are system-level rather than purely cryptographic. Privacy-preserving analytics could be integrated through federated learning at the gateway or hospital edge, while anonymous routing overlays may further reduce linkability against stronger network observers [39]. In parallel, artificial intelligence (AI)-driven intrusion detection can help detect misuse or anomalous traffic patterns around the protected MQTT infrastructure without exposing raw patient topics [40]. These directions strengthen the paper's relevance to healthcare IoT, edge intelligence, and secure communication systems.

## 4. CONCLUSION

This paper presented a gateway-based privacy architecture for IoMT messaging that addresses the underexplored problem of MQTT metadata exposure. By rotating pseudonyms for topics and ClientIDs, the proposed approach improves broker-side privacy visibility without requiring broker modification. Across 5 to 10,000 patients, the method maintained a consistent 5.0× topic diversity gain, 2.50 $\mu s$ per-message computation overhead, 0.063 ms maximum latency overhead, and zero packet loss. These results show that meaningful metadata protection can be added while preserving clinical communication requirements. Current limitations include: (i) timing patterns remain observable, with 14.29% attack success rate without mitigation; (ii) key distribution relies on secure out-of-band provisioning; and (iii) intra-epoch messages to the same pseudo-topic remain linkable by design. Future research will extend the design with federated learning-based privacy-preserving analytics, deployment on embedded IoMT hardware such as ESP32 and Raspberry Pi, formal verification of unlinkability guarantees, and stronger defenses against timing analysis and collusion.

**FUNDING INFORMATION**

Authors state no funding involved.

**AUTHOR CONTRIBUTIONS STATEMENT**

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

| Name of Author | C | M | So | Va | Fo | I | R | D | O | E | Vi | Su | P | Fu |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Rachmad Andri Atmoko | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Salnan Ratih Asriningtias | ✓ | ✓ | | | ✓ | ✓ | | ✓ | ✓ | ✓ | | | ✓ | |
| Akas Bagus Setiawan | | ✓ | ✓ | ✓ | | ✓ | | | | ✓ | ✓ | | | |
| Devasis Pradhan | | | | ✓ | ✓ | | | | | ✓ | | ✓ | | |
| Ismail Rakip Karas | | | | | | ✓ | ✓ | | | ✓ | | | | |

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

**CONFLICT OF INTEREST STATEMENT**

Authors state no conflict of interest.

**DATA AVAILABILITY**

The data that support the findings of this study are available from the corresponding author upon reasonable request. The source code is openly available at: https://github.com/vokasitibrawijaya/privacy-mqtt-iomt.

**REFERENCES**

[1] M. M. Islam, A. Rahaman, and M. R. Islam, "Development of Smart Healthcare Monitoring System in IoT Environment," *SN Computer Science*, vol. 1, no. 3, p. 185, May 2020, doi: 10.1007/s42979-020-00195-y.

[2] A. Banks, E. Briggs, K. Borgendale, and R. Gupta, Eds., "MQTT Version 5.0" *OASIS Standard*, Mar. 7, 2019. [Online]. Available: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html

[3] D. Soni and A. Makwana, "A Survey on MQTT: a Protocol of Internet of Things (IoT)," *International Conference on Telecommunication, Power Analysis and Computing Techniques*, no. April, p. 173-177, 2017, [Online]. Available: https://www.researchgate.net/publication/316018571

[4] F. Buccafurri, V. De Angelis, and S. Lazzaro, "MQTT-A: A Broker-Bridging P2P Architecture to Achieve Anonymity in MQTT," *IEEE Internet of Things Journal*, vol. 10, no. 17, pp. 15443–15463, Sep. 2023, doi: 10.1109/JIOT.2023.3264019.

[5] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1606–1616, 2019, doi: 10.1109/JIOT.2018.2847733.

[6] Y. Sun, F. P. W. Lo, and B. Lo, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey," *IEEE Access*, vol. 7, pp. 183339–183355, 2019, doi: 10.1109/ACCESS.2019.2960617.

[7] V. S. Naresh, S. Reddi, and V. V. L. D. Allavarpu, "Lightweight secure communication system based on Message Queuing Transport Telemetry protocol for e-healthcare environments," *International Journal of Communication Systems*, vol. 34, no. 11, Jul. 2021, doi: 10.1002/dac.4842.

[8] M. B. Yassein, M. Q. Shatnawi, S. Aljwarneh, and R. Al-Hatmi, "Internet of Things: Survey and open issues of MQTT protocol," in *Proceedings - 2017 International Conference on Engineering and MIS, ICEMIS 2017*, IEEE, May 2017, pp. 1–6. doi: 10.1109/ICEMIS.2017.8273112.

[9] A. Sharma and H. Babbar, "Towards Resilient IoT Security: An Analysis and Classification of Attacks in MQTT-based Networks," in *Proceedings - 2nd International Conference on Advancement in Computation and Computer Technologies, InCACCT 2024*, IEEE, May 2024, pp. 122–125. doi: 10.1109/InCACCT61598.2024.10551081.

[10] A. R. Alkhafajee, A. M. Ali Al-Muqarm, A. H. Alwan, and Z. R. Mohammed, "Security and Performance Analysis of MQTT Protocol with TLS in IoT Networks," in *4th International Iraqi Conference on Engineering Technology and Their Applications, IICETA 2021*, IEEE, Sep. 2021, pp. 206–211. doi: 10.1109/IICETA51758.2021.9717495.

[11] G. Yang *et al.*, "Keep Healthcare Workers Safe: Application of Teleoperated Robot in Isolation Ward for COVID-19 Prevention and Control," *Chinese Journal of Mechanical Engineering (English Edition)*, vol. 33, no. 1, p. 47, Dec. 2020, doi: 10.1186/s10033-020-00464-0.

[12] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities,"

*IEEE Access*, vol. 5, pp. 26521–26544, 2017, doi: 10.1109/ACCESS.2017.2775180.
[13] W. Lan, H. Rao, Y. Wang, Z. Wang, X. Yang, and S. Liu, "An Enhanced End-to-End Secure Communication Solution for IoT Smart Medical Devices Based on MQTT Protocol," *IEEE Internet of Things Journal*, vol. 12, no. 15, pp. 31998–32007, 2025, doi: 10.1109/JIOT.2025.3575411.
[14] S. Andy, B. Rahardjo, and B. Hanindhito, "Attack scenarios and security analysis of MQTT communication protocol in IoT system," *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI). IEEE*, pp. 1–6, Sep. 2017. doi: 10.1109/eecsi.2017.8239179.
[15] A. Al-Ani, W. K. Shen, A. K. Al-Ani, S. A. Laghari, and O. E. Elejla, "Evaluating Security of MQTT Protocol in Internet of Things," *Canadian Conference on Electrical and Computer Engineering*, vol. 2023-September, pp. 502–509, 2023, doi: 10.1109/CCECE58730.2023.10288857.
[16] I. Sahmi, A. Abdellaoui, T. Mazri, and N. Hmina, "MQTT-PRESENT: Approach to secure internet of things applications using MQTT protocol," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 5, pp. 4577–4586, 2021, doi: 10.11591/ijece.v11i5.pp4577-4586.
[17] F. A. Shodiq, R. R. Pahlevi, and P. Sukarno, "Secure MQTT Authentication and Message Exchange Methods for IoT Constrained Device," in *2021 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA)*, IEEE, Dec. 2021, pp. 70–74. doi: 10.1109/ICICyTA53712.2021.9689126.
[18] Ö. Şeker, G. Dalkılıç, and U. C. Çabuk, "MARAS: Mutual Authentication and Role-Based Authorization Scheme for Lightweight Internet of Things Applications," *Sensors*, vol. 23, no. 12, 2023, doi: 10.3390/s23125674.
[19] F. Dewanta, I. Wahidah, S. N. Hertiana, D. D. Sanjoyo, and S. H. S. Ariffin, "SibProMQTT: Protection of the MQTT Communication Protocol Against Sybil Attacks Applied for IoT Devices," *Proceedings of the 2023 International Conference on IC Design and Technology, ICICDT 2023*, pp. 108–111, 2023, doi: 10.1109/ICICDT59917.2023.10332423.
[20] K. Morise, T. Toyohara, and H. Nishi, "Proposal of Differential Privacy Anonymization for IoT Applications Using MQTT Broker," *Proceedings - IEEE Consumer Communications and Networking Conference, CCNC*, pp. 634–635, 2024, doi: 10.1109/CCNC51664.2024.10454877.
[21] M. Fischer and R. Tönjes, "FE4MQTT - Using Functional Encryption to Improve the Privacy in Publish-Subscribe Communication Schemes," *Proceedings of the 2025 IEEE International Conference on Cyber Security and Resilience, CSR 2025*, pp. 220–225, 2025, doi: 10.1109/CSR64739.2025.11130112.
[22] A. N. Salim, T. Sutabri, E. S. Negara, and M. I. Herdiansyah, "Communication Security in the MQTT Protocol for Monitoring Internet of Things Devices Using Elliptic Curve Cryptography Methods," *Jurnal Teknik Informatika (JUTIF)*, vol. 5, no. 2, pp. 377–387, Apr. 2024, doi: 10.52436/1.jutif.2024.5.2.1916.
[23] A. Ali-Pour and J. Gascon-Samson, "PECMQ: Private and Encrypted Communications in IoT Systems Using PUFs and MQTT," in *Proceedings - 2024 IEEE 44th International Conference on Distributed Computing Systems Workshops, ICDCSW 2024*, IEEE, Jul. 2024, pp. 64–74. doi: 10.1109/ICDCSW63686.2024.00017.
[24] R. R. Pahlevi, P. Sukarno, and B. Erfianto, "Secure MQTT PUF-Based Key Exchange Protocol for Smart Healthcare," *Jurnal Rekayasa Elektrika*, vol. 17, no. 2, 2021, doi: 10.17529/jre.v17i2.20428.
[25] A. Hue, G. Sharma, and J. M. Dricot, "Privacy-enhanced MQTT protocol for massive IoT," *Electronics (Switzerland)*, vol. 11, no. 1, 2022, doi: 10.3390/electronics11010070.
[26] T. L. Liao, H. R. Lin, P. Y. Wan, and J. J. Yan, "Improved attribute-based encryption using chaos synchronization and its application to MQTT security," *Applied Sciences (Switzerland)*, vol. 9, no. 20, 2019, doi: 10.3390/app9204454.
[27] C. I. Fan, C. H. Shie, Y. F. Tseng, and H. C. Huang, "An Efficient Data Protection Scheme Based on Hierarchical ID-Based Encryption for MQTT," *ACM Transactions on Sensor Networks*, vol. 19, no. 3, 2023, doi: 10.1145/3570506.
[28] S. Pal, M. Hitchens, and V. Varadharajan, "Towards a Secure Access Control Architecture for the Internet of Things," *Proceedings - Conference on Local Computer Networks, LCN*, vol. 2017-October, pp. 219–222, 2017, doi: 10.1109/LCN.2017.76.
[29] J. Roldán-Gómez, J. Carrillo-Mondéjar, J. M. Castelo Gómez, and S. Ruiz-Villafranca, "Security Analysis of the MQTT-SN Protocol for the Internet of Things," *Applied Sciences*, vol. 12, no. 21, p. 10991, Oct. 2022, doi: 10.3390/app122110991.
[30] C. Diaz, "Anonymity Metrics Revisited," *Schloss Dagstuhl – Leibniz-Zentrum für Informatik*, 2006, doi: 10.4230/DAGSEMPROC.05411.2.
[31] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman, and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," *IEEE Access*, vol. 8, pp. 60539–60551, 2020, doi: 10.1109/ACCESS.2020.2983117.
[32] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020, doi: 10.1109/COMST.2019.2962586.
[33] G. Cherubin, J. Hayes, and M. Juarez, "Website Fingerprinting Defenses at the Application Layer," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 2, pp. 186–203, 2017, doi: 10.1515/popets-2017-0023.
[34] R. S. Bali, F. Jaafar, and P. Zavarasky, "Lightweight authentication for MQTT to improve the security of IoT communication," *ACM International Conference Proceeding Series*, pp. 6–12, 2019, doi: 10.1145/3309074.3309081.
[35] S. Cui, S. Belguith, P. De Alwis, M. R. Asghar, and G. Russello, "Collusion Defender: Preserving Subscribers' Privacy in Publish and Subscribe Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1051–1064, 2021, doi: 10.1109/TDSC.2019.2898827.
[36] F. Buccafurri, V. De Angelis, and S. Lazzaro, "MQTT-I: Achieving End-to-End Data Flow Integrity in MQTT," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 5, pp. 4717–4734, 2024, doi: 10.1109/TDSC.2024.3358630.
[37] A. Mileva, A. Velinov, L. Hartmann, S. Wendzel, and W. Mazurczyk, "Comprehensive analysis of MQTT 5.0 susceptibility to network covert channels," *Computers and Security*, vol. 104, 2021, doi: 10.1016/j.cose.2021.102207.
[38] E. Di Paolo, E. Bassetti, and A. Spognardi, "Security assessment of common open source MQTT brokers and clients," 2023, *arXiv*. doi: 10.48550/ARXIV.2309.03547.
[39] J. Hiller, J. Pennekamp, M. Dahlmanns, M. Henze, A. Panchenko, and K. Wehrle, "Tailoring onion routing to the internet of things: Security and privacy in untrusted environments," *Proceedings - International Conference on Network Protocols, ICNP*, vol. 2019-October, 2019, doi: 10.1109/ICNP.2019.8888033.
[40] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep learning-based intrusion detection for IoT networks," *Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing, PRDC*, vol. 2019-December, pp. 256–265, 2019, doi: 10.1109/PRDC47002.2019.00056.

## BIOGRAPHIES OF AUTHORS

**Rachmad Andri Atmoko** received the Bachelor of Applied Sciences in Automation Engineering in 2013 and the Master of Engineering in Instrumentation Engineering in 2015 from the Sepuluh Nopember Institute of Technology. He is currently a lecturer at the Faculty of Vocational Studies, Universitas Brawijaya. His research interests include the development and application of blockchain, federated learning, and internet of things (IoT) technologies. He can be contacted at email: ra.atmoko@ub.ac.id.

**Salnan Ratih Asriningtias** is affiliated with the Faculty of Vocational Studies, Universitas Brawijaya, Indonesia. Her areas of expertise include artificial intelligence, databases, programming, and data science. She can be contacted at email: salnan@ub.ac.id.

**Akas Bagus Setiawan** is a lecturer in the Department of Information Technology at Politeknik Negeri Jember, Indonesia. His research focuses on business process management, data science, and web development. He can be contacted at email: akasbagus_s@polije.ac.id.

**Devasis Pradhan** is with the ECE Department at Acharya Institute of Technology. His research interests include engineering and technology, antenna engineering, wireless communication, MIMO, and mmWave technologies. He can be contacted at email: devasispradhan@acharya.ac.in.

**Ismail Rakip Karas** is a researcher at Karabuk University, Computer Engineering Department. His expertise includes GIS, computer graphics, graph theory, location-based services, and smart cities. He can be contacted at email: ismail.karas@karabuk.edu.tr.