



SecurIoT-ELACA: Lightweight Security Framework for Privacy-Enhanced Publish/Subscribe Communication in IoT Healthcare Systems

Rashmi H Chamarajappa¹✉, Guruprakash C Dyamanna²

¹Department of Information Science & Engineering, Asst. Professor, Sri Siddhartha Institute of Technology, SSAHE, Tumkur, India

²Department of Computer Science and Engineering, Professor, Sri Siddhartha Institute of Technology, SSAHE, Tumkur, India

Abstract

In the realm of IoT healthcare systems, the Publish/Subscribe (Pub/Sub) communication paradigm plays a pivotal role in ensuring the efficient and real-time dissemination of critical patient data. This, in turn, empowers timely medical interventions and seamless remote monitoring. However, the inherent characteristic of loose coupling within the Pub/Sub model raises concerns about security and privacy. This research paper introduces a comprehensive security framework named SecurIoT-ELACA (Security for IoT with Enhanced Lightweight Access Control and Anonymity-based Authentication). SecurIoT-ELACA is designed to integrate lightweight principles, including Lightweight Authentication based on Anonymity (LAA) and Lightweight Access Control (LAC), built upon an Asymmetric Encryption (AE) based model. The primary objective is to bolster access control and data privacy within IoT healthcare systems. SecurIoT-ELACA enhances security through various mechanisms, including anonymous authentication, user registration, and more. It places a strong emphasis on safeguarding the content, securing subscriber identities, and verifying publication authenticity, thereby ensuring lightweight, secure communication. One notable feature of SecurIoT-ELACA is its focus on reducing overhead in terms of storage and communication, aligning with the lightweight approach essential for IoT applications.

Keywords: SecurIoT-ELACA, IoT, Lightweight Access Control, Lightweight Authentication based on Anonymity (LAA)

1. INTRODUCTION

The widespread deployment of the Internet of Things (IoT) has resulted in a significant shift in the healthcare business. Internet of Things (IoT) technology can be applied in several ways in the healthcare sector, such as automating complex medical operations and providing real-time patient monitoring. The improvements outlined above possess the capacity to usher in a novel era

characterized by improved patient care and operational efficiency. In this context, the successful deployment of Internet of Things (IoT) devices requires the use of the publisher/subscriber (pub/sub) paradigm. The approach that is being given exemplifies a paradigm for communication that is dynamic and scalable [1].

Since the publish-subscribe model uses a centralized message broker to enable effective client-to-client communication, it is commonly accepted as an appropriate architectural solution for the Internet of Things (IoT) [2]. IoT-powered publish-subscribe systems frequently make use of the MQTT protocol [3]. Most people agree that the MQTT protocol is the best way to communicate when sending data across the Internet of Things (IoT) network. The main factor influencing this phenomenon is its suitability for low-cost, low-energy devices with limited storage capacity. Clients can post data on any topic that is currently available and subscribe to a particular topic from the available topics pool thanks to the MQTT broker.

Security considerations are not given enough weight in the present MQTT implementations. The efficiency of publish-subscribe paradigms as well as protocols in IoT systems is considerably improved by the inclusion of security considerations. The user/passcode approach, which involves exchanging a passcode between the communicating entities, is used by the MQTT authentication mechanism. It is important to understand that the passcode is transmitted in clear text. Including external authentication techniques like Kerberos and SCRAM in MQTT connection messages is one potential fix. When implementing the protocol, the server is advised to use Transport Layer Security (TLS), following the MQTT standard specification [4-5]. Given the current situation, using these strategies is inappropriate for Internet of Things (IoT) systems that make use of nodes with constrained resources [6]. Numerous studies demonstrated that integration offers numerous advantages. However, this technological innovation raises fundamental concerns about data security and patient privacy. The comparison of important opportunities and looming challenges emphasizes the importance of doing extensive research to establish a secure and resilient healthcare ecosystem powered by the Internet of Things (IoT) [7-8].

A middleware solution known as EMMA [9] has been specifically designed to enhance the efficiency of migrating clients to brokers through the utilization of edge gateways. The migration process involves several key factors, including the calculation of average latency and the implementation of load-balancing techniques to effectively manage connections. EMMA primarily focuses on prioritizing dynamic MQTT bridging functionality, with a relatively lower emphasis on security features. An alternative approach to broker bridging, as suggested by [10], involves employing a combination of brokers and bridging

management servers within an overlay network. This technique offers significant advantages in terms of reducing control message overhead. An analysis conducted by [11] explored various broker distributions and provided a concise summary of their findings.

This paper outlines the XML schema used to build the XPath-based filter and demonstrates the technical feasibility of employing this filter for crafting intricate queries on both the content and structure of XDS documents. Integrating the Healthcare Enterprise (IHE) introduces a comprehensive framework for defining publish/subscribe interactions and offers a subscription mechanism within this framework. This mechanism depends on straightforward document metadata matching [12]. This paper focuses on a model for Publish/Subscribe M2M communication. The objective is to establish a formal methodology for designing and validating M2M systems, taking into account elements such as M2M mobile sensors and time-related criteria. To achieve this, we introduce a graph-based model to describe Publish/Subscribe M2M systems and employ model-checking mechanisms to facilitate verification procedures [13].

This paper introduces a Publish/Subscribe architecture facilitated by a web service, offering the potential for the early sharing of healthcare data among various stakeholders, including doctors, researchers, and policymakers. Our architecture effectively manages privacy and security requirements while also ensuring interoperability for seamless data exchange [14]. In this study, we explore the application of parametric subscriptions within the realm of public safety scenarios. We provide practical examples to illustrate the utilization of these subscriptions. Additionally, we put forth a cloud-based Publish/Subscribe framework and offer detailed insights into its operational mechanisms [15].

In this paper, we present an application layer gateway designed to transform Message Queuing Telemetry Transport Protocol (MQTT) messages into HTTP. This innovative solution can be implemented on a computer or Raspberry Pi, enabling devices to effortlessly transmit data to any REST endpoint. Rather than transmitting data directly to a middleware, IoT devices can transmit a compact message to this bridge, which reconstructs and relays it to a middleware, thereby alleviating the burden on the IoT device [16]. This research explores how intelligence gathered through a simple physical reconnaissance attack can be incorporated into a rapid kill-chain process to enable resource depletion and water torture attacks, ultimately leading to the disruption of three distinct MQTT broker implementations [17].

In this study, we utilize four LoRa modules as nodes/transmitters and one LoRa module as an access point/receiver. Data transmission is achieved using a

star topology, with four nodes transmitting data to access points at varying distances. The primary goal of this investigation is to transmit data through the LoRa SX1278 module using a star topology, assess the effectiveness of data transmission at different distances, and monitor the outcomes of data transmission optimization in IoT applications using MQTT (Message Queuing Telemetry Transport). This research can serve as an educational resource for understanding data transmission [18].

The motivation and contribution of this research are mentioned here. The integration of Internet of Things (IoT) technology into healthcare systems has opened new doors for hospitals, offering the promise of unprecedented advancements in patient care and operational efficiency. The publisher/subscriber model establishes a dependable infrastructure for facilitating seamless communication among IoT devices. Amid this ongoing transformative shift, the significance of prioritizing data security is growing steadily. Safeguarding patient confidentiality and trust necessitates a comprehensive approach that addresses both technical challenges and ethical responsibilities. As researchers, we have to diligently tackle these security concerns, striking a delicate balance between enhancing patient safety and driving innovation. The subsequent section underscores our contributions to this research.

- Develop a SecurIoT-ELACA (Security for IoT with Enhanced Lightweight Access Control and Anonymity-based Authentication) tailored for IoT-based healthcare systems.
- It combines a variety of mechanisms within the architecture, unifying lightweight design principles with an asymmetric encryption-based model. This integration extends to elements such as anonymous authentication, streamlined user enrollment, and other features aimed at fortifying access control and safeguarding data privacy.
- Enable publishers to authenticate their publications through Lightweight Authentication based on Anonymity (LAA), offering a robust means to validate the authenticity and integrity of the content being published.
- During the initial system setup, delegate the responsibility of generating cryptographic keys for Enhanced Asymmetric Encryption, lightweight access control within the Pub/Sub model, and Lightweight Authentication based on anonymity to a Trusted Authority (TA).
- Optimize system performance by reducing overhead, specifically in terms of storage and communication, ensuring the framework's practicality and efficiency.

The following is how the research is organized in this paper: The integration of IoT in healthcare is briefly discussed in the first section, with an emphasis on security issues, MQTT protocol improvements, middleware solutions, and blockchain-based Pub/sub-models [19-21]. The proposed methodology is then presented in the second section, and the performance evaluation is presented in the third section, with the result shown as a graph.

2 PROPOSED METHODOLOGY

This paper describes SecurIoT-ELACA (Security for IoT with Enhanced Lightweight Access Control and Anonymity-based Authentication) architecture, emphasizing its lightweight design concepts for the pub/sub model, asymmetric-based security model, and User_Access_Termination methods. Our study focuses on its use in IoT networks, providing a comprehensive solution for data and privacy protection.

2.1 Publish/Subscriber Architecture

This section describes the main components of a topic-based publish/subscribe (pub/sub) system. These elements include the Broker, Publisher, and Subscriber entities, which communicate with one another through the broker. Topics and payloads comprise publications, whereas subscribers establish subscriptions based on their interests. There are several essential steps in the communication process. To begin, subscribers perform the act of subscribing to specific topics of interest. Following this, publishers begin the transmission of publications. A broker then plays an important role in matching the themes to which the subscribers have subscribed with the accessible publications [22]. The broker then sends the pertinent publications to the appropriate subscribers. Our system's secure framework successfully satisfies key security requirements. The ability of the broker to match publications and subscriptions without revealing content or interests, the prevention of revoked subscribers from accessing subsequent publications, and the facilitation of publication authentication by publishers are some of these requirements [23-24].

The security framework used in pub/sub systems has several functions. First, it makes it easier for publishers to secure publication payloads using enhanced asymmetric encryption, protecting

content of their publications. Using LAC (Lightweight Access Control) for pub/sub also guarantees the confidentiality of publication and the privacy of subscribers to subscriptions. Finally, the framework enables publishers to use LAA (Lightweight Authentication based on Anonymity) to authenticate their publications, offering a way to confirm the veracity and integrity of the

published content [25]. The Trusted Authority (TA) is in charge of producing the cryptographic keys needed for Enhanced Asymmetric Encryption, Lightweight Access Control for the Pub/Sub Model, and Lightweight Authentication based on Anonymity during the initial setup of the system.

2.2 SecurIoT-ELACA (Security for IoT with Enhanced Lightweight Access Control and Anonymity-based Authentication)

2.2.1 Asymmetric encryption

The presented algorithm encompasses eight key steps, each contributing to a robust and secure communication framework within a distributed environment. It begins with Initialization, where security parameters are computed and critical structures are set up for Asymmetric Encryption (AE), Lightweight Access Control (LAC), and Lightweight Authentication based on Anonymity (LAA). The subsequent phases facilitate user registration, data encryption, client key generation, and user access termination, ensuring comprehensive control over user access and data security. The Retrieval of Data step enables efficient data access. Furthermore, the inclusion of Message Authentication and Signature Authentication strengthens the overall security posture, ensuring data integrity and the verification of message authenticity. This algorithm showcases a holistic approach to managing communication and data security in distributed systems, with a focus on user control and privacy. We can see the steps in the below table. An asymmetric encryption scheme enables users to encrypt data based on their attributes, offering fine-grained access control. Enhanced Asymmetric Encryption is designed below in

Table 1.

MPK $\rightarrow \mathcal{H}$

MSK $\rightarrow \mathcal{F}$

Asymmetric Encryption $\rightarrow AS$

Lightweight Authentication based on Anonymity $\rightarrow LAA$

Lightweight Access Control $\rightarrow LAC$

Attributes $\rightarrow \omega$

Security Parameter $\rightarrow f$

<i>Step 1</i>	Initialization: Compute AE_Setup (f = security parameter) to generate $(\mathcal{H}, \mathcal{F})$ Compute $LAC_Setup(f, \mathcal{H})$, Lightweight Access Control with parameters $(\mathcal{H}, \mathcal{F})$. Compute $LAA_Setup(f, P)$ to set up Lightweight Authentication based on anonymity with $(pubkey, \mathcal{F})$.
<i>Step 2</i>	User registration: perform $Create(pubkey, ID)$ Update the user list ($listupdated$)
<i>Step 3</i>	Encrypt sensitive data: Encrypt sensitive data for publication perform $EncIndex(pubkey, AS, Y)$ create an encrypted index (F)
<i>Step 4</i>	Client Key Generation: perform $EAE_KeyGen(\mathcal{H}, C)$ use $KeyGen(pubkey, masterpubkey, C)$ generate a user's $seckey$
<i>Step 5</i>	User Access Termination: Perform $ReKeyGen(\mathcal{S}, \mathcal{F})$ to generate re-encryption keys updated keys ($MK0$ and $pubkey0$) Use $ReEncIndex(re-encrypt_key, F, 1)$ execute $ReKey(S, re-encrypt_key, partialseckey)$
<i>Step 6</i>	Retrieval of Data: Generate $specific_task_auth(pubkey, seckey, Y0)$ Search($listupdated, F, \mathcal{S}$)
<i>Step 7</i>	Message Authentication: Perform $LAA_Extract(pubkey, \omega)$ Execute $LAA_Sign(seckey, \omega, tm)$
<i>Step 8</i>	Signature Authentication: Verify a signed message Use $LAA_Verify(tm, \omega, pubkey, \delta)$ ensures the signer possesses the required attributes (ω)

3 PERFORMANCE ANALYSIS

In evaluating the effectiveness of the SecurIoT-ELACS framework, which is designed to provide both security and lightweight communication in a publish-subscribe environment, we take into consideration the impact on communication and storage overhead. To assess its performance, we compare this proposed model with two key benchmarks: the TLS protocol and the existing model. Through this comparative analysis, we aim to gain insights into how the SecurIoT-ELACA framework influences communication and storage overhead, as outlined in reference [25].

3.1.1 Storage Overhead

In a publish-subscribe system, the management of subscriber information and their preferences can lead to increased storage requirements. To address this, we entrust a Trusted Authority (TA) with the responsibility of generating cryptographic keys for Lightweight Access Control, Enhanced Asymmetric Encryption, and Lightweight Authentication based on Anonymity during the configuration of our pub/sub system. As depicted in Figure 1, when we consider

the storage capacity with the publish module in mind, we observe variations among three methodologies. TLS, with 321 storage units, provides the least storage capacity. The existing system offers a more moderate 80 units, while our proposed system, with a storage capacity of 60 units, presents the most storage among the three. The choice between these options should be influenced by the available storage resources and budget constraints.

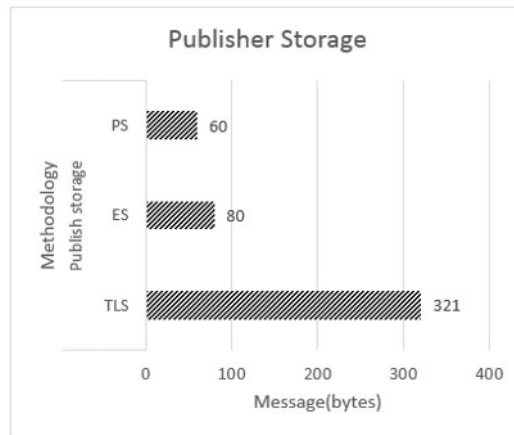


Figure -1 Storage publish comparison

In Figure 2, we observe the storage capacities of three different technologies: TLS, with 321 units, offers the highest storage capacity; the existing system provides a moderate capacity of 80 units, while the proposed system offers a more streamlined storage capacity of 60 units. This lower storage capacity makes the proposed system particularly suitable for smaller-scale applications.

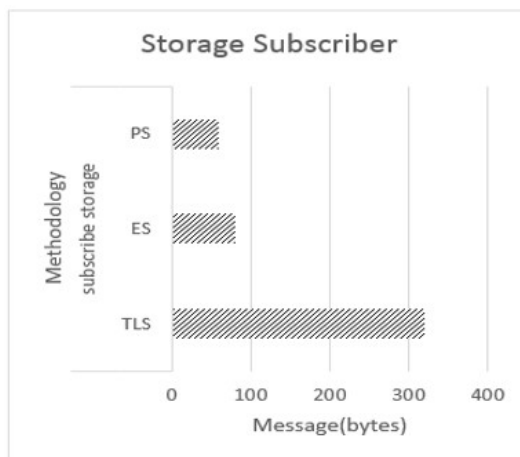


Figure -2 Subscriber storage comparison

3.1.2 Communication Overhead

Within the realm of pub/sub systems, efficient message routing, which is based on subscriber interests, encompasses essential activities such as message processing and forwarding. Furthermore, communication overhead arises from the need to encode and decode messages, ensuring compatibility with diverse subscriber protocols. The assurance of message delivery and reliability introduces additional communication overhead, including acknowledgments and potential retries. Moreover, the implementation of security measures to safeguard message processing amplifies communication overhead. In Figure 3, we compare the communication speeds of three distinct options: TLS (332) offers the lowest communication speed, while the existing system (ES) provides a moderate communication speed, making it suitable for most standard applications. In contrast, the proposed system (PS) exhibits a superior communication speed, rendering it a favorable choice for less demanding tasks.

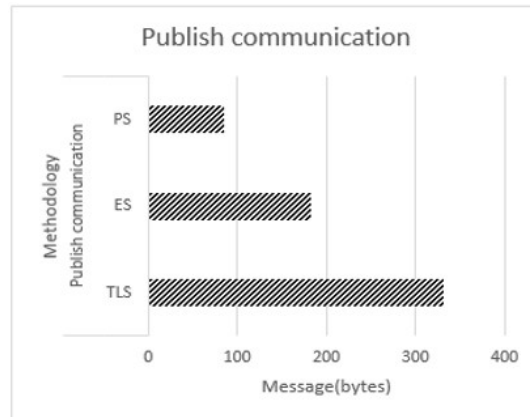


Figure - 3 Published communication result

In Figure 4, we present a visual representation of the communication overhead comparison among three distinct options: TLS (332) exhibits the slowest communication speed, the existing system (ES) provides a moderate speed, which is well-suited for a range of communication requirements, and the proposed system (PS) outperforms the others, offering superior results that may be deemed acceptable for less time-critical applications.

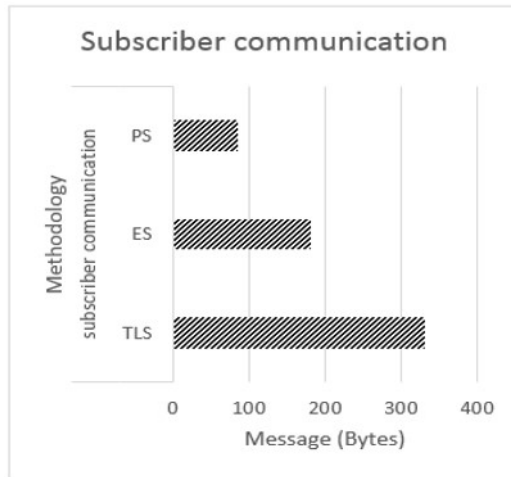


Figure- 4 Subscriber communication result comparison

3.2 Comparative Analysis

The comparative analysis highlights the unique strengths and trade-offs between TLS, the existing system (ES), along with proposed system (PS). TLS shines in terms of storage, featuring a minimal capacity that is well-suited for applications with stringent storage constraints. ES provides a balanced offering with moderate storage and communication speeds, catering to standard use cases. On the other hand, SecurIoT-ELACA stands out as it offers the highest storage capacity and significantly improved communication efficiency, making it an ideal choice for applications that do not demand immediate responses. The selection between these options should be based on specific storage and communication requirements, aiming to strike a promising balance between capacity and speed to accommodate a wide range of IoT applications. The above comparison can be analyzed through the given below table 2.

Table - 2 Comparative Analysis

	TLS (Message)	ES	PS
Storage Overhead	321	80	60
Communication Overhead	332	182	85

4 CONCLUSION

This study introduces the SecurIoT-ELACA framework. By allowing publishers to use LAA (Lightweight Authentication based on Anonymity) to confirm the legitimacy of their publications, the framework protects the accuracy of the published information. The initial configuration of the system requires the Trusted Authority (TA) to produce the cryptographic keys required for Enhanced Asymmetric Encryption, Lightweight Access Control for the Pub/Sub Model, and Lightweight Authentication based on Anonymity. In order to support a wide range of IoT applications, it not only increases storage capacities but also connection speeds. However, unique requirements, financial limitations, and the importance of communication all play a role in the decision between the proposed system and the existing system. This methodology is a valuable addition to the IoT technology landscape as it offers a substantial advancement in enhancing IoT connectivity and security.

REFERENCES

1. T. G. F. Barros, E. F. Da Silva Neto, J. A. D. S. Neto, A. G. M. De Souza, V. B. Aquino and E. S. Teixeira, "The Anatomy of IoT Platforms—A Systematic Multivocal Mapping Study," in *IEEE Access*, 2022, pp.72758-72772, doi: 10.1109/ACCESS.2022.3189660.
2. L.G.A.Rodriguez and D.M.Batista, "Resource-Intensive Fuzzing for MQTT Brokers: State of the Art, Performance Evaluation, and Open Issues," in *IEEE Networking Letters*, 2023 pp. 100-104, doi: 10.1109/LNET.2023.3263556.
3. T. Rausch, S. Nastic, and S. Dustdar, "EMMA: Distributed QoS-aware MQTT middleware for edge computing applications," in *Proc. IEEE Int. Conf. Cloud Eng.*, 2018, pp. 191–197.
4. V.N. Pham and E.N. Huh, "An efficient edge-cloud publish/subscribe model for large-scale IoT applications," in *Proc. 13th Int. Conf. Ubiquitous Inf. Manage. Commun.*, 2019, pp. 130–140.
5. A. E. C. Redondi, A. Arcia-Moret, and P. Manzoni, "Towards a scaled IoT Pub/Sub architecture for 5G networks: The case of multiaccess edge computing," in *Proc. IEEE 5th World Forum Internet of Things*, 2019, pp. 436–441
6. L. Bisne and M. Parmar, "Composite secure MQTT for Internet of Things using ABE and dynamic S-box AES," in *Proc. Innov. Power Adv. Comput. Technol. (i-PACT)*, 2017, pp. 1–5.
7. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, 2006, pp. 89–98.
8. B. S. Adiga, P. Balamuralidhar, M. A. Rajan, R. Shastri, and V. L. Shivraj,

“An identity based encryption using elliptic curve cryptography for secure M2M communication,” in *Proc. 1st Int. Conf. Secur. Internet Things*, 2012, pp. 68–74.

9. Y. Zhang, X. Wang, X. He, N. Zhang, Z. Zheng and K. Xu, "Galaxy: A Scalable BFT and Privacy-Preserving Pub/Sub IoT Data Sharing Framework Based on Blockchain," in *IEEE Internet of Things Journal*, 2023 doi: 10.1109/JIOT.2023.3307073.

10. M. Hamad, A. Finkenzeller, H. Liu, J. Lauinger, V. Prevelakis and S. Steinhorst, "SEEMQTT: Secure End-to-End MQTT-Based Communication for Mobile IoT Systems Using Secret Sharing and Trust Delegation," in *IEEE Internet of Things Journal*, 2023, pp.3384-3406, doi: 10.1109/JIOT.2022.3221857.

11. T. Zaarour, A. Bhattacharya and E. Curry, "OpenPubSub: Supporting Large Semantic Content Spaces in Peer-to-Peer Publish/Subscribe Systems for the Internet of Multimedia Things," in *IEEE Internet of Things Journal*, 2022, pp. 17640-17659, doi: 10.1109/JIOT.2022.3158088.

12. L. Liu and S. Yuan, "XPath-Based Filter for Publish/Subscribe in Healthcare Environments," *IEEE 12th International Conference on Computer and Information Technology*, Chengdu, China, 2012, pp. 1092-1096, doi: 10.1109/CIT.2012.222.

13. G. Gharbi, N. Guermouche and T. Monteil, "Temporal verification of mobile publish/subscribe machine-to-machine communications," *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks* 2014, Sydney, NSW, Australia, 2014, pp.1-3, doi: 10.1109/WoWMoM.2014.6919022.

14. R. Wadhwa, A. Mehra, P. Singh and M. Singh, "A pub/sub based architecture to support public healthcare data exchange," *7th International Conference on Communication Systems and Networks (COMSNETS)*, Bangalore, India, 2015, pp. 1-6, doi: 10.1109/COMSNETS.2015.7098706.

15. Al-Muaythir and M. A. Hossain, "Cloud-Based Parametrized Publish/Subscribe System for Public Safety Applications in Smarter Cities" *IEEE/ACM 9th International Conference on Utility and Cloud Computing (UCC)*, Shanghai, China, 2016, pp.208-213.

16. M. A. A. da Cruz, J. J. P. C. Rodrigues, E. S. Paradello, P. Lorenz, P. Solic and V. H. C. Albuquerque, "A Proposal for Bridging the Message Queuing Telemetry Transport Protocol to HTTP on IoT Solutions," *3rd International Conference on Smart and Sustainable Technologies (SpliTech)*, Split, Croatia, 2018, pp. 1-5.

17. R. D. Paz, A. Sehovic, D. M. Cook and L. Armstrong, "A Novel Approach to Resource Starvation Attacks on Message Queuing Telemetry Transport Brokers," *4th International Conference on Information Technology, Information*

Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 2019, pp. 150-154, doi: 10.1109/ICITISEE48480.2019.9003770.

18. K. Saputro, A. R. Anditya, M. Ulum, H. Sukri, R. Alfita and A. F. Ibadillah, "Application of LoRa (Long Range Access) in Optimizing Internet of Things Using MQTT (Message Queuing Telemetry Transport) For Fish Feed Monitoring," *6th Information Technology International Seminar (ITIS)*, Surabaya, Indonesia, 2020, pp. 224-228, doi: 10.1109/ITIS50118.2020.9321021.

19. K. Wolf, F. Pallas and S. Tai, "Messaging with Purpose Limitation – Privacy-Compliant Publish-Subscribe Systems," *IEEE 25th International Enterprise Distributed Object Computing Conference (EDOC)*, Gold Coast, Australia, 2021, pp. 162-172, doi: 10.1109/EDOC52215.2021.00027.

20. S. Kul and A. Sayar, "A Survey of Publish/Subscribe Middleware Systems for Microservice Communication," *5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, Ankara, Turkey, 2021, pp. 781-785, doi: 10.1109/ISMSIT52890.2021.9604746.

21. Y. Liu and X. Yu, "A Distributed Publish-Subscribe Algorithm Based on Spatial Text Information Flow," in *Journal of Web Engineering*, 2023, pp. 385-404, doi: 10.13052/jwe1540-9589.2231.

22. D. Hernandez, L. Gameiro, C. Senna, M. Luís and S. Sargento, "Handling Producer and Consumer Mobility in IoT Publish–Subscribe Named Data Networks," in *IEEE Internet of Things Journal*, 2022, pp. 868-884, doi: 10.1109/JIOT.2021.3069054.

23. N. Pavlopoulou and E. Curry, "IoTSAX: A Dynamic LAAtractive Entity Summarization Approach with Approximation and Embedding-Based Reasoning Rules in Publish/Subscribe Systems," in *IEEE Internet of Things Journal*, 2022, pp. 1830-1847, doi: 10.1109/JIOT.2021.3089931.

24. J. Vestin, A. Kassler, S. Laki and G. Pongrácz, "Toward In-Network Event Detection and Filtering for Publish/Subscribe Communication Using Programmable Data Planes," in *IEEE Transactions on Network and Service Management*, 2021, pp. 415-428, doi: 10.1109/TNSM.2020.3040011.

25. 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," 2020, in *IEEE Access*, pp. 60539-60551, doi: 10.1109/ACCESS.2020.2983117.