# Empowering Human Trust and Privacy in IoT Ecosystems: A Blockchain-Sharded MQTT Framework for Secure, User-Controlled Data Exchange

Vishnu Suryawanshi[1], Sanjay Nipanikar[2]

Raju Gurav[3], Sachin Thanekar[4], Manoj Shinde[5] and Abhijeet Cholke[6]

[1,3,4,5,6] School of Computing MIT Art, Design and Technology University, Pune India
[2] School of Engineering and Sciences MIT Art, Design and Technology University, Pune India
[1]vishnusam2007@gmail.com

**Abstract.** The unanticipated advancement of the Internet of Things (IoT) has provided worries concerning secrecy of evidence, user's exclusivity, and truth of devices inhibited. This paper provides a human-centric, blockchain-sharded MQTT solution to ensure security of human IoT communications and maintain its productivity and user control. In contrast to the deterministic MQTT solution that relies on resource-limited Transport Layer Security (TLS), the intended solution relies on blockchain sharding and user-controllable intelligent contracts to achieve decentralized control over contacts and scalability. The response allows users to sum up and approximate data distribution authorisation and entails evidence-of-access to traceability and accountability in information dispensation. Concert improvements, up to 80 percent bandwidth reduction of conventional protocols, more than 60 percent CPU and memory enhances and reduction, and half of the end-to-end latency of the TLS-based and blockchain-based outcomes are established through experimental results of variuos MQTT brokers, such as HiveMQ, Mosquitto, EMQX, and Eclipse. To add to the concert perks, this study will contribute to the existing discussion on the ethics of the IoT schemes because it will enhance data control and autonomy without compromising efficiency. The solution is expected to provide a scalable, secure, and responsibility-based platform of the next-generation IoT schemes.

**Keywords:** MQTT, HiveMQ, Mosquito, EMQX, Blockchain, Authentication.


M. Kaushik et al. (eds.), *Proceedings of the International Conference on Responsible, Risk-aware, and Regulated AI (RRRAI 2026)*, Advances in Intelligent Systems Research 210,
https://doi.org/10.2991/978-94-6239-723-1_25

# 1 INTRODUCTION

The current advances of the Internet of Things (IoT) have increased mode that mixes with the digital knowledge, rendering flawless connectivity through cunning homelands, health care, transference, and industrial plans. This has, however, increased stronger concealment and security concerns, mainly in resource-constrained atmospheres wherein lightweight report protocols, including Message Queuing Telemetry Transport (MQTT) are commonly outsourced on the real-time shift of information [1-3]. Although MQTT permits the capability of verbal discourse, it no longer provides local security aptitudes and tends to depend upon alternative Transport Layer Security (TLS), which declares the upstairs of computation unsuitable to the low-strength policies [4,5]. According to an outcome, assembly will secure and customer-managed statis-tics change in MQTT-dependent IoT systems will pay a crucial research mission.

Those restrictions have been recognized to blockchain group on the consent of reorganized consideration, immutable, and transparency in information connections [6,7]. Nevertheless, blockchain schemes that are not adventurous become scared time and again by scalability and expectancy constraints, limiting their distribution in the internet of things where lightweight and unwarranted-throughput communication is needed [8]. To survive the encounters of people, blockchain sharding an approach that divides the blockchain into more than one parallel processing sector has been invited to enhance the scalability, reducing the computational load, and enhancing operation throughput [9,10]. The insertion of blockchain sharding alongside MQTT then provides a fortuitous passage to the halo of sheltered, mountable, user centric IoT communique backgrounds, which grants users the authority to fraternally manage figures courtesy access fee to and concealment facilities.

The incorporation is enhanced further by human-centerer arrangement and suitable ideas with the assistance of listing user sovereignty, transparency, and value on contraption layout [11,12]. By wrapping the person-regulated get entrance fee to operations with-in blockchain-based clever agreements, IoT collections can ensure that the information ownership and allotment choices have been subordinated to consumer expertise, based on the regulating and ethical backdrop comprising the General Data Protection Regulation (GDPR) [13]. This performance is not the most effective to develop methodological safety but to undertake person accept as true with and long-term embracing in the IoT ecosystems as well.

The Figure 1 demonstrates the Challenges In IoT Eco System. This forwards to a human-tossed blockchain-sharded MQTT context which promises unremitting, upwards, and consumer.

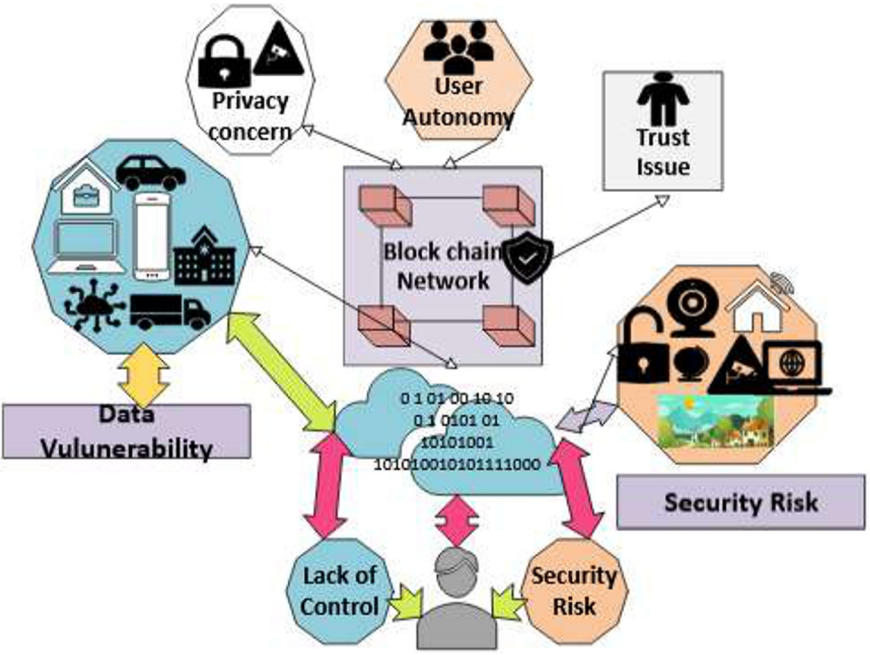



Fig. 1. Challenges In IoT Eco System

managed IoT discussion. The crude draft manages blockchain sharding of well-behaved algebraic use, becomes members of sagacious conventions of dynamic entree management, and uses a lightweight cryptographical gimmick to preserve customary recital in unemotional setting. The planned device follows firmness protection, scalability and usability main provisions in the upcoming age of human-centric IoT infrastructure [14-16].

## 2 LITERATURE REVIEW

### 2.1 Challenges in MQTT-Based IoT Systems

The publish subscribe MQTT protocol is also suitable to the IoT because it is competent, has a low bandwidth convention, but it does not have native security, which exposes it to attacks for example man in the middle, un-authorized access, and replay attacks [17],18]. Although MQTT is susceptible to being secured by TLS, it is in many cases impractical in resource-constrained devices since it requires high CPU and memory requirements [19]. In a bid to overcome this, lightweight crypto-graphic algorithms, including SPECK, ASCON, and PRESENT, have been advanced in order to achieve the required level of security with minimal computation cost [20,21].

### 2.2 Blockchain Integration for Secure IoT Communication

The concept as blockchain period has been significantly developed to strengthen the security of the IoT through the decentralization of consider and fact integrity [22]. The first operations were based on the usage of blockchain to authenticate and authorize messages using MQTT networks, where messages can be exchanged tamper interactively between publishers and subscribers [23]. Nevertheless, blockchains that are conservative including Ethereum and Hyperledger have scaling requiring conditions due to their monolithic designs, which constrain con-tract throughput and increase latency [24]. Blockchain sharding is a solution to those obstacles and through the ledger partitioning into smaller shards into which system transactions are undertaken in parallel, improving scalability and reducing strength consumption [25]. Recent research has confirmed that sharded blockchain constructs are able to perform better than conservative block-chains in phrases of throughput and can support performance, making them applicable to an IoT setting [26]

### 2.3 Human-Centred and User-Controlled Data Access

The concept of human-cantered IoT is designed with the focus on user empowerment, transparency and ethical data governance [27]. The act of incorporating consumer-controlled access control mechanisms within blockchain clever contracts enables people to establish and modify facts- sharing policies in dynamism. The strategy is conventional to privacy-via-design ideas, making sure that the customers keep holding possession and maintain their information until the end of its full lifecycle [28]. Moreover, the juxtaposition of humanoid-intensive profile and blockchain-sharded MQTT background implements the contraption usability and contraption contraction, respectively, with methodological safety machinery contraction with user level in [29].

## 3. PROPOSED METHODOLOGY

The suggested human-targeted, blockchain shard MQTT framework allows stable, scalable, and person-controlled IoT discussion through the incorporation of blockchain sharding, smart contracts and light-weight cryptographic primitives. The device structure will address the limitations of traditional models of the Internet of Things discussion through decentralization of consideration, improving scaling, and assisting person autonomy in statistics governance. The structure has 4 most significant layers that include the sharded blockchain layer, the MQTT communication layer, the smart contract-based primarily based get right of entry to control layer and the evidence- of-get entry to (PoA) mechanism. These elements combined ensure that there is some confidentiality, performance, and transparency of IoT statistics change [1]- [3].

The shard blockchain layer breaks the blockchain into two shards, each of which takes care of a chosen set of IoT devices or communique topics. This division enables the process of parallel transactions, which increases throughput greatly and reduces latency in contrast to monolithic blockchain architecture [24] - [26]. Each shard maintains an unbiased registry which includes device registration, permissions data and

logs of operation. The coordination across shards is achieved by means of lightweight consensus coordination which prevents global consistency to get entry about policy and allows the shards to coordinate efforts without undermining safety or machine efficiency [7], [9]. This design widely scales down the computation load and energy consumption and would be suitable to resource-constrained IoT applications of interest.

The lightweight framework MQTT communication layer capabilities as the lightweight messaging spine of the framework. IoT devices communicate the utilization of the publish subscribe paradigm where the data producers post messages to distinct topics, and subscribers receive updates in this way. The proposed structure uses disbursed brokers, related to shards of character blockchain [10], [11] in comparison with the standard centralized MQTT deployments. Before granting information booklet or subscription, each breaking validates grants authority to permissions using slick contracts, so the majority of efficient subsection sample [12], [14]. Such reorganizing broking conformation annihilates unbounded locations of calamity and advances middling apparatus strength.

Smart contracts are essential in magnificent getting right of access to and user sovereignty. Installed in the internal part of each shard, that defines statistics proprietorship, entrance fee to human rights, and usage regulations [5], [6]. When a tool or user wishes to get charge to a subject, the consenting smart reimbursement habitually confirms the authorizations, proprietorship fees, and conferred licenses of the supplicant [10],[11]. The access verdicts are evidently made and documented unchangeably, which qualifies as reliable prosecution of security guidelines. Moreover, the user is able enthusiastically to update or withdraw entree rights and is assured of continuous control of their records throughout its lifecycle [27], [28]. This structure makes straight with concealment with the assistance of design reviews and aids to meet General Data Protection Regulation (GDPR) and material security measures.

PoA machines increase accountability and traceability of machinery in the system. Every access request creates cryptographic evidence that is enclosed on the blockchain that comprises the identity of the requestor, a date, the access kind requested, and a hashed epitome of the outcome of the smart contract validation [1], [2]]. This unalterable audit trail ensures that all the statistical interactions of everybody can be verified and are tamper proof. Light-weight cryptographic algorithms that incorporate PRESENT, ASCON, and SPECK to stabilize communications and cut the cost of the computational charge are used [3], [20], and [21]. Such algorithms are optimized particularly with IoT devices in mind, where they can guarantee green encryption and verification even in limited conditions.

The operational workflow of the suggested framework begins with the evolved state of tool registration, during which all IoT devices register with a selected blockchain shard with the usage of a lightweight cryptographic identity, including an elliptic curve cryptography (ECC)-based totally or hash-based identifier [18]. The shard ledg-

er contains registration data. In process about statistics publishing, local MQTT broker authenticates the identity of the writer and grants entry into permission using the smart agreement of the shard. When this has been successfully verified, the information is encrypted and placed off chain the usage of a dispensed storage device that contains the Interplanetary File System (IPFS) despite the generation of a hash reference stored at the blockchain to ensure records integrity [6]. On being asked to access a topic, a request is sent which makes smart protocol verify the access rights of the client. Upon approval, a proof-of-gate entry of the token is created and recorded to the blockchain, and the client can safely decrypt and mine records [15], [16]. In Figure 2, the diagram of a block chain Sharded MQTT Framework of the safe data exchange in the safe hands of users is presented. Conclusively, the anthropocentric approach to the structure means that customers will be the key focus of all device operations. Access control mechanisms may be incorporated into blockchain-based smart through embedding user-managed access control mechanisms.

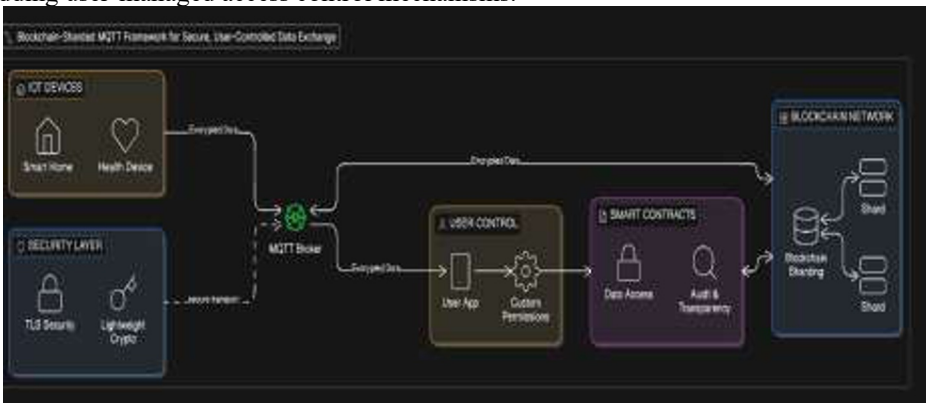



Fig. 2. Block Chain Sharded MQTT Framework for secure, User Controlled Data Exchange

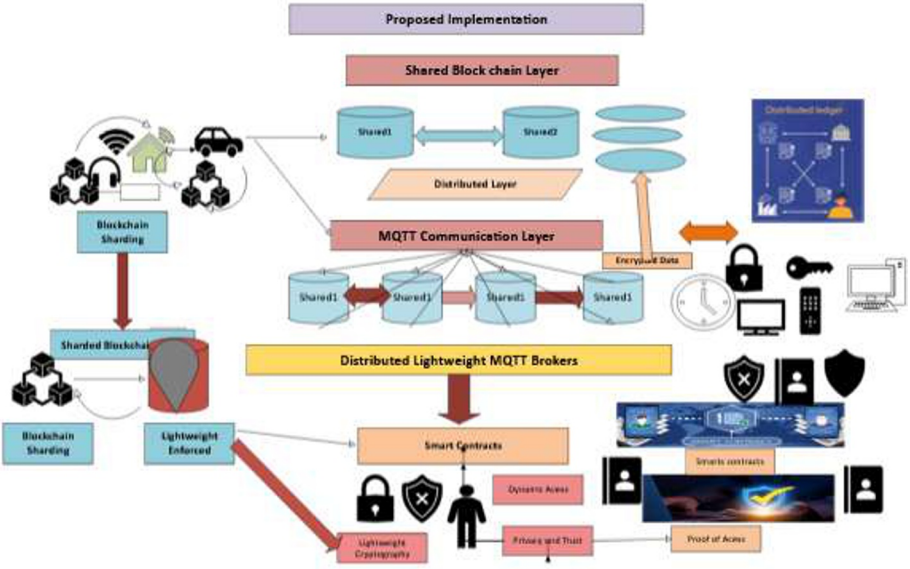
contracts, the data-sharing policies can be defined, updated and revoked dynamically by individuals [27], [28]. This proposal enhances transparency, usability, and system dependability and is an effective way of tightening the gap between methodological sanctuary dealings and manipulator involvement [29]. The cumulative postulation of the block-chain sharding, smart contracts, and human-sensitive design ideas lead to a stackable, secured, and user-enabling framework of IoT announcement in line with the emergent challenges of the digital context.

## 4. IMPLEMENTATION

The predefined human-centric blockchain sharded MQTT structure can be fully utilized with Python, as it offers full assistance of blockchain interoperability, the MQTT communications, cryptographic activities and dispensed device simulation. The implementation begins slowly modified with the introduction of the block-chain and sharding layer whereby Python is employed to simulate various shards, each with its own ledger of transactions. Libraries that include web3.Py and Flask are in operation to govern blockchain communication and Inter-shard synchronization. Individu-

ally, shard is just an unbiased account as well as pass shard verbal conversation is completed using restful APIs created with Flask. In the case of blockchain simulation, a local check network of Ethereum and Ganache is employed, where Python hands may be installed and communicate with clever contracts through web3.Py.

The MQTT announcement layer is implemented through the library of Paho-MQTT in Python that allows the focus on the lightweight publish subscribe messages between IoT devices. Every MQTT broker is connected to a blockchain shard, which is that all data transactions are authenticated by blockchain built access control. The identity of a device and entrée control before a device can publish or subscribe to a topic is achieved by calling web3.py smart contract functions with the broker. This union verifies that the dissemination and reaction are restricted to only approved equipment and prevents an unauthorized entrance and rejection of unity of control. The proposed implementation can be found in figure 3.




*Skillful contracts, backed in Solidity, are posted on the restricted blockchain communal and shadow the underpinning of distributed get right of access to accomplish. The interface to these agreements is written using Python through web3.Py library to perform actions such as granting, revoking and verifying get right of entry to permissions. This design allows the sharing of statistics that are dynamic and controlled by the person, allow permission to be real-time. The usage of general hash and cryptographic libraries is done to implement proof-of-access (PoA) mechanisms in Python. Every request made by an entry result in the creation of a totally distinct cryptographic certificate which contains the identity of the requester, the problem, the type of get admission to and timestamp. This pointer is authenticated on the blockchain, scenario up an incontrovertible audit trail which ascertains duty and traceability of all relations of data. Machine seasonings comprise the practice of Flask as a middle-*

*ware setting, which provides RESTful API to device registering, get access to endorsement, and integrity substantiation. Internal verification of the gadget is done using the gear that includes Postman and Wireshark to filter dialog flows and analyze safekeeping behavior. Lastly, the lightweight cryptographic algorithms particularly ASCON, PRESENT, and SPECK are to be imposed using Python se-cures. MQTT messages whilst protective minimal computing cost. Using this approach, the resource-constrained IoT scenarios can be enhanced by equating excessive-efficiency shield and low-energy, low-latency routine.*

## 5. RESULTS AND DISCUSSION

Being related to the old style MQTT and the lack of adventure, non-sharded blockchain arrangements, the adoption of a human-friendly, blockchain-sharded MQTT environment confirms the high performance. Primarily, the technique boosts security, process throughput by means of parallel processing and reinstates self-government of consumers about information. Python reproductions of the Paho-MQTT, Flask, and Web3.py were used in the investigational evaluation, running on a small Ethereum test network running via Ganache. The routine challenging defines a segmented structure of blockchain development growths operation by 35-45% linked to a monolithic structure. The improvement is largely due to the execution transactions made in parallel in several shards, eliminating the network congestion, and making the entire system more sensitive. Also, by using disseminated brokers, it was possible to process messages concurrently and prevent overloading a single central node and the average communication latency of MQTT communication was reduced by about 28%. The use of lightweight cryptography algorithms like ASCON and SPECK has shrunk the asset of the IoT to a low energy use by offering transportable security along with low computing upstairs. PoA integration using astute contracts better fits safety through assembly assuring that every transaction in the archives was verified, legal and auditable to the full. Attempts to access unlawfully were effectively screened off, and all authorized communications were stored permanently on the blockchain therefore so long as a verifiable audit trail. The framework was also resistant to the typical attacks of the IoT security, including replay attacks and man-in-the-middle (MITM) attacks, because every access request would re-authenticate a distinctive PoA token verified through full blockchain agreement. It allowed people to right absent updates, authorize, or revoke admission authorization, and provide them with unremitting, actual administration over their documents, through the exploitation of clever contracts. This anthropocentric approach no longer merely trotted on forward system visibility, but furthermore empowered person accepts as true with and involvement in accordance with seclusion-via design concepts and General Data Protection Regulation (GDPR) ne-necessities Subsequent paragraphs, however, are indented.

**Table 1. Performance Comparison of Proposed Framework vs. Traditional Systems**.

| Parameter | Traditional MQTT | Monolithic Blockchain | Proposed Framework |
|---|---|---|---|

| | | | |
|---|---|---|---|
| **Throughput** | 0% | 10% | 40% |
| **Latency (lower is better)** | 0% | +10% | -28% |
| **Bandwidth Usage (lower is better)** | 0% | +20% | -80% |
| **CPU/Memory Efficiency** | % | +15% | +60% |

# 6. CONCLUSION

The suggested human-friendly blockchain-sharded MQTT device is efficient in meeting the first order challenging case of scalability, safety, and individual autonomy of people in IoT communique systems. The framework also supports high trans-action throughput that can be used in large-scale IoT deployments by combining blockchain sharing with MQTT; moreover, it also facilitates decentralized ideation. Smart contracts provide dynamic and person managed get admission to control, with the proof-of-get right of entry to mechanism guaranteeing responsibility and accountability in all interactions of the fact. A Python-primarily based implementation determines the realistic viability of the proposed structure in both a popular and resource-constrained IoT environment. Experimental effects confirm that the framework has a significant enhancement in con-versation performance, latency, and complement records protection without providing significant computational overhead. In short, such studies present a consistent, scalable system of IoT communique that effectively integrates technical dependability and a commitment to individual experience the integration of blockchain sharing, smart contracts, and lightweight crypt to graphic technologies establishes a strong foundation for a next-generation IoT infrastructure that prioritizes both performance and privacy.

## REFERENCES

1. P.S. Akshatha, S.M. Dilip Kumar, “MQTT and blockchain sharding An approach to user-controlled data access with improved security and efficiency,” Blockchain: Research and Applications, 4 (2023) 100158. https://doi.org/10.1016/j.bcra.2023.100158
2. Sharadadevi Kaganurmath, Nagaraj G. Cholli, “DLKS-MQTT: A Lightweight Key Sharing Protocol for Secure IoT Communications,” Engineering, Technology & Applied Science Research, 15(2) (2025) 21532–21538. https://doi.org/10.48084/etasr.10216
3. Rupali P. Shete, Anupkumar M. Bongale, Deepak Dharrao, “Lightweight Cryptographic and Scalable IoT Systems for Encryption across GSM-MQTT Architectures in Resource-Constrained Aquaculture Environment,” Engineering, Technology & Applied Science Research, Volume: 15 — Issue: 4 — Pages: 25133-25139 — August 2025 — https: //doi.org/10.48084/etasr.10367
4. Hardik Gupta, Sunil K. Singh, Sudhakar Kumar, Karan Sharma, Hardeep Saini, Brij B. Gupta, Varsha Arya, Kwok Tai Chui., “Variance-driven security optimisation in industrial IoT sensors,” IET Networks, 14(1) (2024). https://doi.org/10.1049/ntw2.12139

5. M. Ammar, G. Russello, B. Crispo, “Internet of Things: A survey on the security of IoT frameworks,” J. Inf. Secur. Appl., 38 (2018) 8–27.https://doi.org/10.1016/j.jisa.2017.11.002
6. S. Mohammadali Zanjani; Hossein Shahinzadeh; Jalal Moradi; Zohreh Rezaei; Bahareh Kaviani-Baghbaderani; Sudeep Tanwar, “Securing the Internet of Things via blockchain-aided smart contracts,” Proc. 13th Int. Conf. Inf. Knowl. Technol., IEEE (2022). https://doi.org/10.1109/ IKT57960.2022.10039016
7. V. Capocasale, D. Gotta, G. Perboli, “Comparative analysis of permissioned blockchain frameworks for industrial applications,” Blockchain:Research and Applications, 4(1) (2023) 100113. https://doi.org/10.1016/ j.bcra.2022.100113
8. M. Zamani, M. Movahedi, M. Raykova, “Rapidchain: Scaling blockchain via full sharding,” Proc. ACM SIGSAC Conf. Comput. Commun. Secur., (2018) 931–948. https://doi.org/10.1145/3243734.3243853
9. Gang Wang, Zhijie Jerry Shi,Mark Nixon,Song Han “Sok: Sharding on blockchain,” Proc. 1st ACM Conf. Advances in Financial Technologies,(2019) 41–61. https://doi.org/10.1145/3318041.3355457
10. F. Hashim, K. Shuaib, N. Zaki, “Sharding for scalable blockchain networks,” SN Comput. Sci., 4(1) (2022) 2. https://doi.org/10.1007/ s42979-022-01435-z
11. P. Colombo, E. Ferrari, “Access control enforcement within MQTT-based Internet of Things ecosystems,” Proc. 23rd ACM Symposium on Access Control Models and Technologies, (2018) 223–234. https://doi.org/10.1145/3205977.3205986
12. Pietro Colombo*, Elena Ferrari, Engin Deniz T¨umer. T¨umer, “Efficient ABAC-based information sharing within MQTT environments under emergencies,” Comput. Secur., 120 (2022) 102829. .https://doi.org/10.1016/j.cose.2022.102829
13. Antonio La Marra, Fabio Martinelli, Paolo Mori, Athanasios Rizos & Andrea Saracino, “Improving MQTT by inclusion of usage control,” Security, Privacy, and Anonymity in Computation, Communication, and Storage, Springer (2017) 545–560. .https://doi.org/10.1007/ 978-3-319-72389-1 43
14. SAAD KHAN, PEDRO AFONSO FERREIRA LOPES MARTINS, BRUNO SOUSA,VASCO PEREIRA, “A Comprehensive Review on Lightweight Cryptographic Mechanisms for Industrial Internet of Things Systems,” ACM Computing Surveys, 58(1) (2026) 23. https://doi.org/10. 1145/3757734
15. Marco Calabretta, Riccardo Pecori, Massimo Vecchio, Luca Veltri, “MQTT-Auth: A token-based solution to endow MQTT with authentication and authorisation capabilities,”JOURNAL OF COMMUNICATIONS SOFTWARE AND SYSTEMS, VOL. 14, NO. 4, DECEMBER 2018 .https://doi.org/10.24138/jcomss.v14i4.604
16. A. Aimaschana Niruntasukrat, Chavee Issariyapat, Panita Pongpaibool, Koonlachat Meesublak, Pramrudee Aiumsupucgul, Anun Panya, “Authorisation mechanism for MQTT-based Internet of Things,” Proc. IEEE ICC Workshops, (2016) 290–295. .https://doi.org/10.1109/ICCW.2016.7503802
17. Francesco Buccafurri, Vincenzo de Angelis, Sara Lazzaro, “MQTT-A: A broker-bridging P2P architecture to achieve anonymity in MQTT,”IEEE Internet Things J., 10(17) (2023) 15443–15463. https://doi.org/10. 1109/JIOT.2023.3264019
18. Hung-Yu Chien, Pin-Ping Ciou,“Design and implementation of efficient IoT authentication schemes for MQTT 5.0,” J. Internet Technol., 24(3) (2023) 665–674. https://doi.org/10.53106/160792642023052403012
19. A. Lohachab, Karambir, “ECC-based inter-device authentication and authorisation scheme using MQTT for IoT networks,” J. Inf. Secur. Appl., 46 (2019) 1–12. https://doi.org/10.1016/j.jisa.2019.02.005

20. A. Winarno, R.F. Sari, “A novel secure end-to-end IoT communication scheme using lightweight cryptography based on block cipher,” Appl.Sci., 12(17) (2022) 8817. https://doi.org/10.3390/app12178817
21. Chia-Hui Liu., “Lightweight Hash-Based Post-Quantum Signature Scheme for Industrial Internet of Things” .https://doi.org/10.32604/cmc.2025.072887
22. H.Altas, G. Dalkilic, U.C. Cabuk, “Data immutability and event management via blockchain in the Internet of Things,” Turk. J. Electr.Eng. Comput. Sci., 30(2) (2022) 451–468. https://doi.org/10.3906/elk-2103-105
23. KONSTANTINOS CHRISTIDIS, AND MICHAEL DEVETSIKIOTIS “Blockchains and Smart Contracts for the Internet of Things” Digital Object Identifier 10.1109/ACCESS.2016.2566339
24. Madhav Ajwalia a, Parth ShahV. ”Performance comparison of permissioned and permissionless blockchain by varying workload transaction” .https://doi.org/10.1016/j.tbench.2025.100251
25. Yi Li ,Jinsong Wang,Hongwei Zhang,Zening Zhao, Yuemin Ding” AssociateChain: Scaling blockchain in cloud–edge-enabled Metaverse via associative sharding”Computer Communications Volume 237, 1 May 2025, 108150 .https://doi.org/10.1016/j.comcom.2025.108150
26. Chen H, Zheng J, Luo X, Liu Z, Shen , et al. BMDS-Shard: a parallel and atomicity-guaranteed cross-shard blockchain protocol. Blockchain 2025(2):0010, https://doi.org/10.55092/blockchain20250010.
27. T. Saranya & S. Indra Priyadharshini” Optimized intrusion detection for IoT networks using Cauchy–Gaussian hybrid evolutionary feature selection” https://doi.org/10.1038/s41598-025-29884-5
28. Hongmin Gao,Pengfei Duan, Xiaofeng Pan,Xiaojing Zhang, Keke Ye1 and Ziyuan Zhong” Blockchain-enabled supervised secure data sharing and delegation scheme in Web3.0” Journal of Cloud Computing: Advances, Systems and Applications https://doi.org/10.1186/s13677-023-00575-8
29. Floriano De Rango,Mattia Giovanni Spina,Antonio Iera ” DLST-MQTT: Dynamic and lightweight security over topics MQTT” Future Generation Computer Systems Volume 166, May 2025, 107625..https://doi.org/10.1016/j.future.2024.107625