Received: December 16, 2023. Revised: January 29, 2024.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

An Improved Congestion Handling in Blockchain Secured Cloud Based Healthcare System

Thakur Saikumari[1]* **George Victo Sudha[1]**

[1]*Department of Computer Science and Engineering, Dr. M.G.R. Educational and Research Institute, Chennai, Tamilnadu, India.*
* Corresponding author's Email: neelima0318phd@gmail.com

Abstract: Nowadays, blockchain-based healthcare systems have gained more attention for handling a huge amount of patient health data observed by Internet-of-Things (IoT) systems. Several studies have focused on integrating blockchain technology with healthcare systems to ensure the secrecy and transparency of patient data. Among these, an enhanced eHealthChain system has been designed, which comprises Enhanced OAuth (EOAuth) 2.0 to enhance user security based on their trust score. It also applies a Constrained Application Protocol (CoAP) to achieve reliable transmission by controlling congestion in the network according to the Retransmission Timeout (RTO). However, the CoAP causes long inactive latency in the network, and the backoff values are constant, which do not differ in dynamic network settings. Hence, this article proposes an Enhanced CoAP (ECoAP), which adopts adaptive RTO estimation with an Adaptive Backoff Factor (ABF), Data Loss Rate (DLR) estimation, and a Refined Random Early Identification (RREI) scheme for Congestion Control (CC) in dynamic network configurations. This can be useful to reduce the number of retransmissions by predicting the variable backoff values. Moreover, this protocol achieves effective queue management and regulation of backoff values based on congestion levels. Finally, the implementation findings exhibit that the ECoAP outperforms the classical CoAP for secure and reliable transmission in blockchain-enabled clinical IoT systems. The results revealed that the proposed system achieves 24.6% unsuccessful transmissions, 4.64 seconds average service time, 0.2264 seconds average network delay, 94.96% average server usage, 16.9% average Quality of Experience (QoE), 92.4% confidentiality, 86.5% authorization, and 93.9% data integrity for 2500 transmissions.

Keywords: Blockchain-based clinical IoT system, eHealthChain, EOAuth 2.0, CoAP, RTO estimation, Backoff timer, Data loss rate, Random early identification.

1. Introduction

IoT is a key technology for intelligent data transmission, enabling physical object networks to detect, communicate, and interact with each other or external devices. It has a significant influence on daily life and user behaviour, with a broad variety and scope of networks requiring various information-sharing methods [1, 2]. The system demands include both reliable and unreliable transmissions, and security measures are necessary to protect users' information [3]. In healthcare, IoT systems are gaining attention for their promising chances in 5G healthcare systems, but face challenges in security, reliability, and transparency [4, 5].

Integrating blockchain technology with clinical IoT systems can solve these problems by securing patients' health records and eliminating intermediaries in data exchange [6]. Many blockchain-enabled clinical IoT systems, including the eHealthChain system [7], have been developed in recent years. The eHealthChain system uses OAuth 2.0 and Message Queuing Telemetry Transport (MQTT) protocols to ensure user authority and data transmission. However, the OAuth 2.0 protocol has vulnerabilities that can threaten user safety, and MQTT has limitations in resource-restricted networks, causing delays in requests. To address these issues, the EOAuth 2.0 protocol was developed [8]. It enhances user safety by incorporating a pseudonym-based sign method and a sign delegation strategy into the standard OAuth 2.0 protocol. Additionally, a certified safety facility is used to securely obtain user information and perform cryptographic operations. A trust value is then calculated for all users to identify the most trustworthy users and reduce verification time. In addition, the CoAP protocol is used instead of MQTT for reliable data exchange, based on the RTO value. However, CoAP can result in long inactive latency in the network and constant backoff values, which do not adjust to dynamic network settings.

Therefore, in this paper, an ECoAP is proposed by introducing adaptive strategies to handle congestion in the network during data exchange. In this ECoAP, 3 major functions are performed such as an adaptive RTO estimation with an ABF, DLR estimation, and RREI scheme for CC in the dynamic network configurations. It determines the RTO and Round Trip Time (RTT) adaptively to provide reliable transmission among nodes. It also controls the congestion earlier in the dynamic network scenarios and executes group interaction effectively. Thus, this can be useful to reduce the number of retransmissions by predicting the variable backoff values. Moreover, this protocol achieves effective queue management and regulation of backoff values based on the congestion levels. The order of the remaining parts is as follows: In Section 2, many applications of CoAP-based authentication systems are studied. Section 3 provides an overview of the ECoAP, while Section 4 provides examples of its effectiveness. The work is summed up and future directions are provided in Section 5.

2. Literature survey

A novel dynamic CC method was developed to improve CoAP efficiency [9] in IoT by improving the CC strategy and reducing data retransfers. However, it did not optimize values for IoT data categories, resulting in high unsuccessful transmissions and network delay. An alternate method called CoAP-R [10] was developed to control CoAP transfer rate using a rate-based method for traffic control. However, it requires inspection and interception of CoAP packets at middle nodes to control congestion, impacting QoE.

An acceptable CC approach for CoAP was proposed [11] to ensure safe system operation and optimal resource use. The RTO value used in each transaction was calculated by applying a refined CC scheme. However, the security measures were not effective in a changing network environment. A novel scheme called Congestion Control Random Early Detection (CoCo-RED) [12] was developed to perform (a) computing an RTO timer, (b) a Revised RED (RevRED) scheme, and (c) a Fibonacci Pre-Increment Backoff (FPB) technique. However, it did not cope with high congestion levels, resulting in high service time, delay, server usage, and unsuccessful transmissions.

An Integrated IoT blockchain system [13] was designed for sensing information integrity, solving scalability, identity, and data security problems in IoT systems. However, the server usage and network delay were not effective. To investigate the popular IoT session protocols, CoAP and MQTT protocols were analyzed for effective media transport over Low-power Lossy Networks (LLNs) [14]. However, CoAP-specific forward error correction values were not satisfactory, leading to a high ratio of unsuccessful transmissions.

A security method was presented for utilizing TACACS+ [15] to improve CoAP confidentiality. However, the network delay and service time were high. To investigate the performance of various CC strategies for CoAP [16] in a real-time scenario using the WiSHFUL. However, confidentiality and data integrity were not satisfactory in systems with a time-slotted access protocol.

A Context-Aware Congestion Control (CACC) technique [17] in IoT networks was developed, providing dynamic congestion management. But the QoE and service time were not effective. A new approach for optimally establishing the initial RTO and changing the RTO backoff was developed [18], taking into account current system usage. However, it was not designed to help with CC on CoAP when operating in the unverifiable mode, leading to low confidentiality and authenticity.

An Enhanced CoCo-RED (EnCoCo-RED) [19] was developed to enhance the CC strategy for CoAP observe group transmission. However, the service time and network delay were high. The blockchain-empowered Decentralized and Scalable (DS) solution [20] was developed CoAP and Ethereum blockchain. However, the service time and ratio of unsuccessful transmission were very high.

3. Proposed methodology

This section discusses the architecture of a blockchain-enabled clinical system and a 3-tier edge-IoT system, followed by the UE-eHealthChain system and its components. The proposed ECoAP is also briefly explained.

3.1 Blockchain-enabled clinical system

Fig. 1 shows a blockchain system for handling clinical data, where various files such as medical services, insurance data, family medical data, and prescriptions are stored on a cloud server and accessed by authorized individuals.

3.2 Blockchain-based 3-tier edge-IoT system

Combining blockchain and edge computing allows chances for healthcare 4.0 applications and improves the Quality of Service (QoS), QoE, trust, confidentiality, and resource utilization. Three IoT structure models are accessible: classical cloud-IoT, edge-IoT, and 3-tier edge-IoT [21]. This study focuses on the 3-tier edge-IoT paradigm as presented in Fig. 2(a), deploying local IoT edge for decision-making within the local network. This is crucial for handling connectivity issues and limiting the dissemination of confidential information. For example, Fig. 2(b) shows the healthcare applications using the blockchain-based 3-tier edge-IoT model.

Fig. 3 emphasizes the blockchain-edge system for healthcare IoT applications, featuring multiple IoT groups linked to the corresponding edge nodes. Due to resource constraints, IoT groups are merged with edge nodes through a gateway, allowing for local data pre-processing (cleaning), storage, and transmission to meet low delay demands for critical stages.

IoT-edge networks can benefit from a lightweight private/permissioned blockchain for reliable and safe data sharing among different IoT-edge groups. Smart contracts can be used to verify data sources and participants in the supply chain, while the local blockchain ensures authentication and access control. When resources are not available locally, requests are sent to fog networks, which do not require a link to the main internet or access network base station to function. Fog networks facilitate low-latency access to resources and services in smart healthcare settings, including advanced tasks like data analytics and decision-making using artificial intelligence. Additionally, fog networks handle the orchestration and dynamic allocation of resources.

Healthcare providers can use fog networks to create data sources and delegate responsibility to their patients. Fog nodes will coordinate the sharing of critical process data, pooling it on a public or permission-less blockchain. The global network, based on centralized cloud computing models, offers greater resource capacities for data-intensive programs. The blockchain serves as an immutable ledger for all transactions between networks and institutions, and all networks must work together for the plan to succeed.

3.3 Blockchain-based 3-tier edge-IoT system

The eHealthChain system uses blockchain technology to collect, manage, and share individual medical data from clinical IoT systems [8]. It connects these systems to blockchain storage using a unique interface unit, which gathers and stores information from IoT systems. The system then retrieves and transmits this information to an app, providing a user-friendly view of the data.

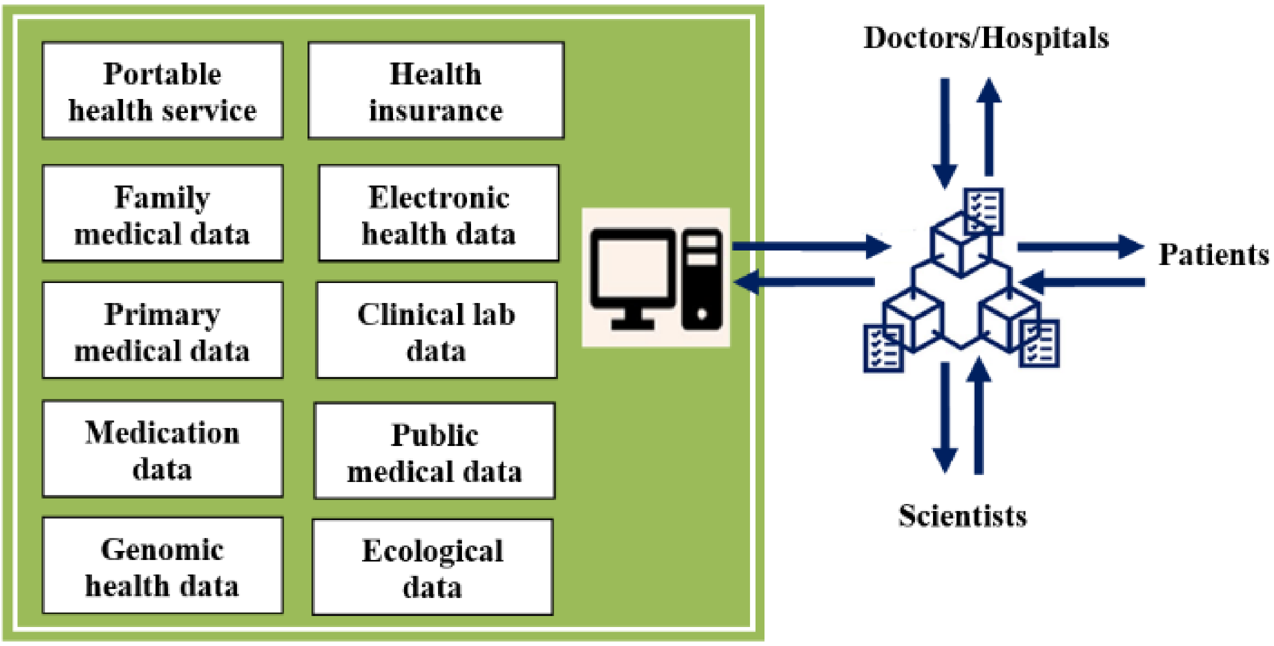
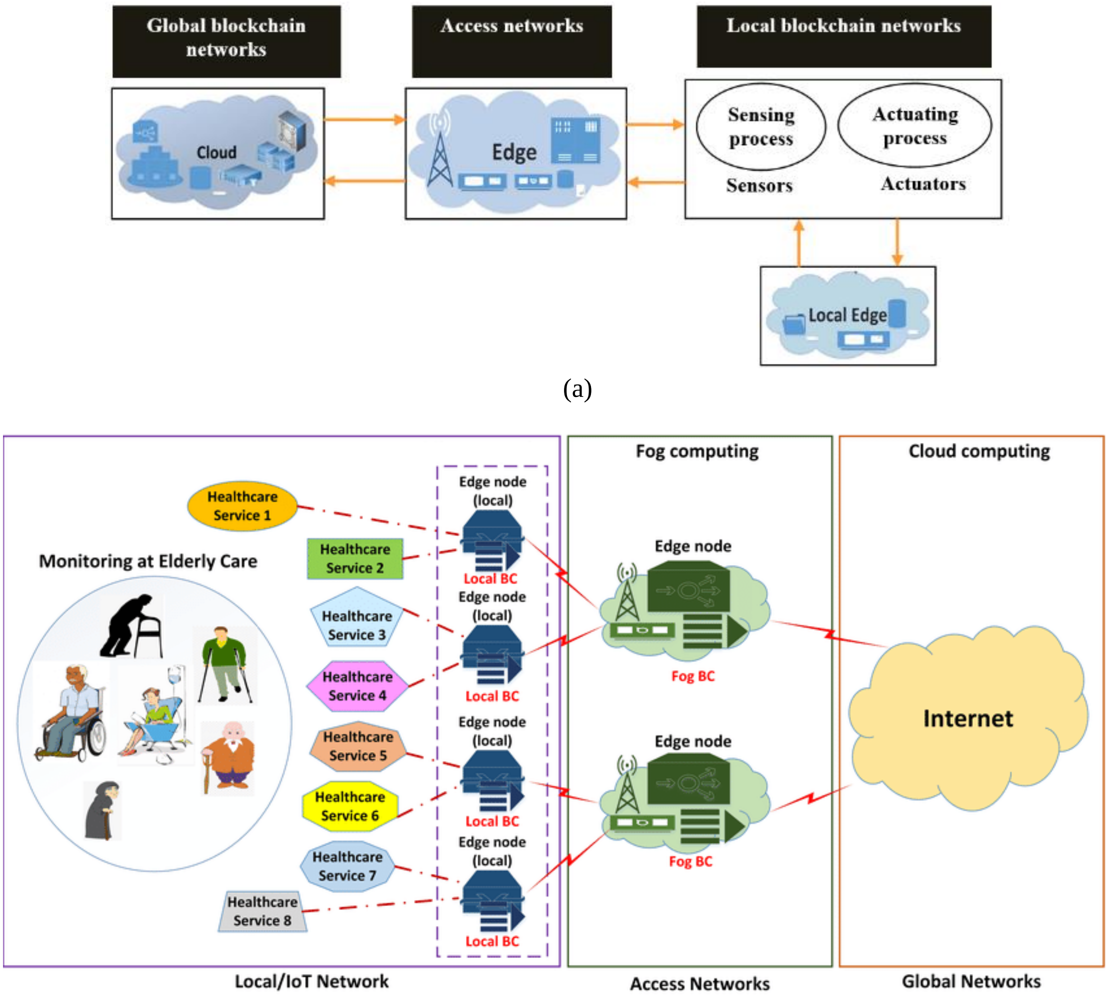


Figure. 1 Blockchain-enabled medical data handling system

Received: December 16, 2023. Revised: January 29, 2024.



(a)

(b)

Figure. 2: (a) Structure of blockchain-based 3-tier edge-IoT network and (b) Example of blockchain-based 3-tier edge-IoT network in healthcare applications

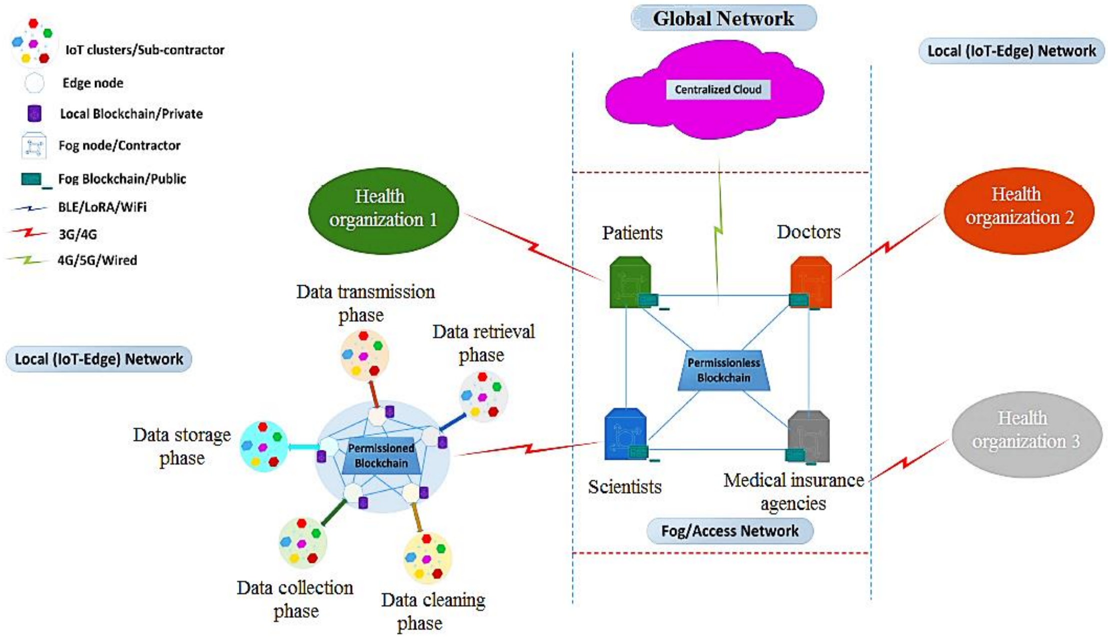


Figure. 3 Blockchain-edge model for healthcare applications

Received: December 16, 2023. Revised: January 29, 2024.

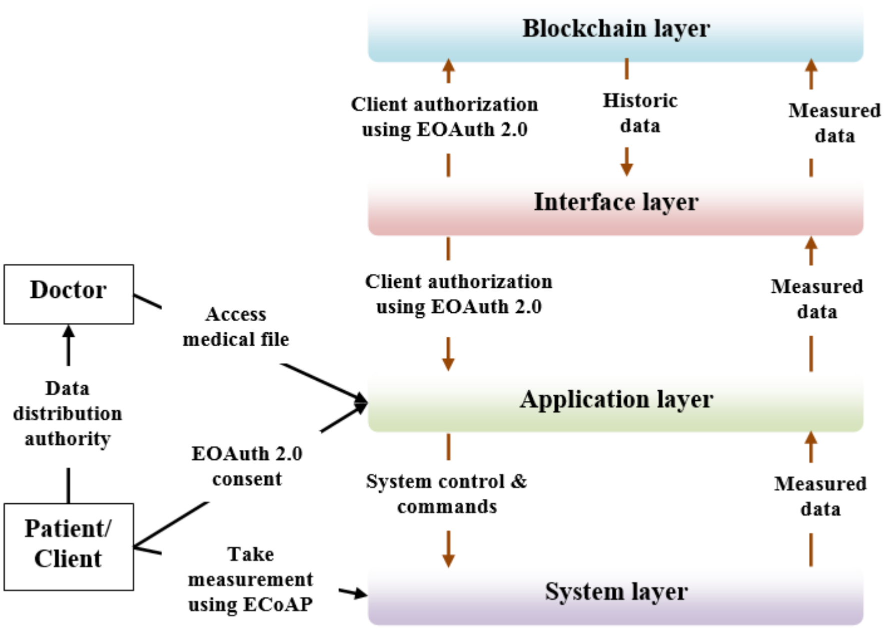


Figure. 4 Structure of enhanced eHealthChain system

Fig. 4 illustrates the structure of eHealthChain, which has the following 4 major layers:

- Blockchain layer: Blockchain is a distributed ledger that logs and verifies network transactions, including data from medical IoT devices. Access to the data is restricted to those granted permission by the owner. Maintaining network-wide ledger file consensus is an ongoing process, with each participant maintaining their copy of the ledger. Updates to the ledger are shared via ECoAP.
- Interface layer: It bridges the gap between the application layer and the blockchain layer, using the secure EOAuth 2.0 protocol to receive protected health information and the blockchain's REST APIs to record medical information.
- Application layer: Client medical device data is collected through mobile apps using the EOAuth 2.0 protocol, allowing for easier sharing with third parties. EOAuth grants limited access to client profiles for third-party apps.
- System layer: Bluetooth links clinical IoT equipment to mobile phones for updating medical records in the eHealthChain system. Patients can verify data accuracy by communicating with authorized users.

3.4 Enhanced constrained application protocol

To alleviate network congestion, the default implementation of CoAP uses a Binary Exponential Backoff (BEB) mechanism. Fig. 5 provides a high-level view of the CoAP architecture by illustrating the client-server interaction during CoAP execution. Group communication and resource monitoring are both hampered by the way CoAP is often implemented. Thus, a CC mechanism named CoCo-RED was developed [12] to track group chatter. The RTO aging process [22] and the Variable Backoff Factor (VBF) in place of BEB were introduced by CoCoA, as was the adaptive RTO computation function. To better manage network congestion, the proposed approach combines these two ideas with Data Loss Rate (DLR).

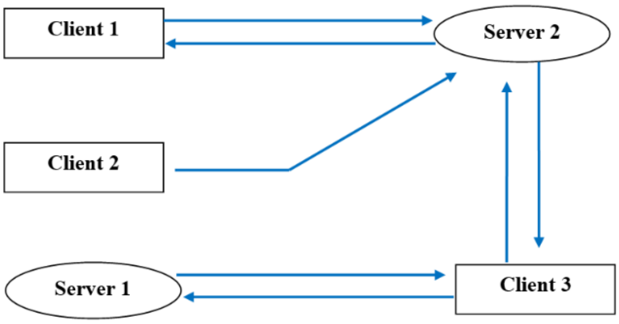


Figure. 5 Overview of CoAP structure

During the secure broadcast, confirmable (CNF) data is sent from x to the server node. When the data is not effectively sent in the initial effort, a rebroadcast is conducted. The CoAP chooses an RTO from two and three seconds for the initial broadcast at random.

The BEB raises the RTO to avoid congestion when the main broadcast fails. Since$(RTO_{update}) = 2 * RTO_{initial}$, the updated RTO_{update} is twice as long as the initial $RTO_{initial}$. However, it is not very efficient because of the disruption it creates to the network and because it does not take into account the dynamic nature of the network. The backoff parameters are fixed and do not adapt to the dynamic changes in the network. Also, this standard CoAP is ineffective at group transmission and resource monitoring.

To combat all these challenges, the ECoAP initially determines RTO by Refined Random Early Identification (RREI) scheme and Data Loss Rate (DLR). Then, rebroadcast RTO is determined by the Adaptive Backoff Factor (ABF). Then, the RREI is applied to determine the network density depending on the Mean Queue Length (MQL). The MQL is computed by the exponential weighted moving mean. The RREI rejects the arriving data before x's buffer queue overflows. This scheme performs as:

```
$\boldsymbol{if}(MQL < threshold_{mininum})$
  Arriving data is located in a queue;
  $DLR = 0$;
$\boldsymbol{elseif}(threshold_{minimum} < MQL < threshold_{maximum})$
  Reject the arriving data depending on the dropping probability;
  Calculate the DLR;
  $\boldsymbol{if}(DLR_{current} < DLR_{mean})$
    Set $RTO_{total}$ and ABF as low;
    Obtain better network efficiency and less congestion;
  $\boldsymbol{else}$
    Set $RTO_{total}$ and ABF as high;
  $\boldsymbol{endif}$
$\boldsymbol{else}(MQL > threshold_{maximum})$
  Reject the arriving data depending on the dropping probability;
  Calculate the DLR;
  $\boldsymbol{if}(DLR_{current} < DLR_{mean})$
    Set $RTO_{total}$ and ABF as low;
    Obtain better network efficiency and less congestion;
  $\boldsymbol{else}$
    Set $RTO_{total}$ and ABF as high;
  $\boldsymbol{endif}$
$\boldsymbol{endif}$
```

An exponentially weighted moving average of the RTT and the RTT variation measure is first used to dynamically establish the RTO. The primary function of the DLR is to determine the adaptive RTO timer. The RTO predictor utilizes both high and low RTTs. The RTT values from the packets for which an ACK is received before rebroadcast are called high RTO predictors. Similarly, the low RTO predictor utilizes low RTTs, i.e. RTT values taken from packets that have needed at most 2 rebroadcasts. This maximizes the probability of acquiring RTT values in the event of data losses. After measuring a low or high RTT, the corresponding low or high RTO (RTO_i) is measured as:

High and low RTTs are used by the RTO predictor. The RTT values for packets that received ACK before rebroadcast are called high RTO predictors. Also, packets that only required two rebroadcasts are used as the basis for the low RTO predictor's RTT values. In the event of data loss, this improves the chances of acquiring RTT values. The low or high RTO (RTO_i) is calculated based on the measured RTT described in Eq. (1).

$$RTO_i = SRTT_i + G_i + VRTT_i \tag{1}$$

In Eq. (1), i is either low or high, $SRTT$ is the smoothed RTT, variance of RTT represented as $VRTT$, G_{high} is 4 and G_{low} is 1. The final RTO value is calculated by a weighted sum of RTO_{low} and RTO_{high} (i.e., RTOs in advance of rebroadcast, and the absence of rebroadcast):

$$RTO_{total} = \begin{cases} \alpha \times RTO_{low} + (1-\alpha) \times RTO_{total}, \\ \qquad DLR_{current} < DLR_{mean} \\ \alpha \times RTO_{high} + (1-\alpha) \times RTO_{total}, \\ \qquad DLR_{current} > DLR_{mean} \end{cases} \tag{2}$$

In Eq. (2), α is 0.5 for the high RTO predictor and 0.25 for the low RTO predictor. This RTO_{total} is utilized to assign the initial RTO $(RTO_{initial})$ for the successive CNF broadcast. The actual value of $RTO_{initial}$ is randomly selected from the period $[RTO_{total}, 1.5 \times RTO_{total}]$. Adjustments have been made to the minimal RTO predictor as opposed to the one with a high RTO predictor to prevent an abrupt increase in RTO after identifying a low RTT and to maintain the stability of the overall RTO estimation:

1. Low RTT values are only permitted for the first two rebroadcasts to prevent extremely low RTT values and since the chance of acquiring the accurate RTT value reduces with all rebroadcasts.

2. To improve the low RTO predictor, the value of G is reduced from 4 to 1. As $VRTT$ rises, especially when rebroadcasts are used frequently, the impact of this factor on the predicted low RTO is mitigated.

3. The low RTO predictor is given less weight (0.25) than the high RTO predicted during the calculation of the total RTO. High RTTs provide more trustworthy feedback on the projected RTTs

and allow for a more accurate RTO calculation, even if a low RTT value is assumed to be necessary.

To cut down on unnecessary rebroadcasts, ECoAP uses an ABF that adjusts the backoff values according to the broadcast's original RTO. When $RTO_{initial}$ is extremely low (i.e., $RTO_{initial} < 1\,sec$), a higher backoff factor is used for rebroadcasting (i.e., $ABF = 3$). When a broadcast begins with a high RTO rate (i.e., $RTO_{initial} > 3\,sec$), a minimal backoff factor is selected for rebroadcasts (i.e., $ABF = 1.5$). For broadcasts that begin with an RTO between 1 and 3sec (i.e., $1\,sec > RTO_{initial} > 3\,sec$), the ABF is assigned to 2 (i.e., $ABF = 2$) related to BEB. Thus, regarding the backoff strategy, ECoAP updates the RTO value for rebroadcasts based on the ABF, which depends on the $RTO_{initial}$. The updated value of RTO for rebroadcasts $\left(RTO_{update}\right)$ is determined by

$$RTO_{update} = RTO_{former} \times ABF(RTO_{initial}) \quad (3)$$

There is a good likelihood that the estimated RTO numbers are no longer accurate if they haven't been updated in a while. So, the RTT can change quickly. Low and high RTO estimates are subjected to an aging policy to protect against forgeries caused by these changes. In cases when the estimated RTO is too low $1\,sec > RTO_{initial} > 3\,sec$ or too high (4x the current RTO) and no new RTT data are acquired in that time, the RTO is reset to its normal initial value. Thus, the ECoAP attains less RTO value which leads to less inactive latency in the network contrasted to the BEB of standard CoAP for all successive rebroadcasts.

4. Simulation result

This section analyzes the effectiveness of the UE-eHealthChain IoT system using iFogSim. iFogSim allows for real-time simulation of IoT applications in a fog/edge environment and analysis of network management metrics. The efficiency of UE-eHealthChain is compared to existing blockchain systems using iFogSim with parameters in Table 1. Performance metrics include percentage of unsuccessful transmission, mean service time, mean network delay, mean server usage, and mean QoE. Security analysis also evaluates EOAuth 2.0 with the ECoAP scheme for data integrity, authorization, and confidentiality.

Fig. 6 depicts the high-level blockchain-edge model for healthcare systems in the iFogSim simulator. There are three primary phases to the proposed blockchain-edge model. Initial iFogSim deployment supports lightweight blockchain integration and deployment of limited resources nodes and edge nodes. Edge nodes receive data from central nodes to process and make decisions locally. When combined with local blockchain, edge nodes can confidently share data. Advanced computing fog nodes can be deployed in the subsequent phase. Connected to several IoT-edge nodes, a single fog node provides processing, storage, and visibility into the broader network. The cloud is then deployed as the final stage, with the highest available resources and overall responsibility for application management. This means that the blockchain-edge model's method for implementation is bottom-up, orfrom local to global networks.

Table 1. Simulation parameters for blockchain-edge model

Parameters	Global networks	Fog networks	Edge networks	IoT devices
Storage abilities/RAM (GB)	16	8	4	1
Upstream bandwidth (Mbps)	150	75	30	12.5
Blockchain instructions (M)	20	11	5	-
Downstream bandwidth (Mbps)	80	37.5	18	6
Transmission delay (ms)	145	45	5	1
Processing abilities/CPU (Million Instructions Per Second (MIPS))	13000-20000	8000-11000	4000-8000	500-1500
Blockchain processing power (Watts)	20-80	12-40	1.4-20	-

4.1 Performance analysis

4.1.1 Percentage of unsuccessful transmission

It is the fraction of failed transmissions in the network.

Fig. 7 depicts the percentage of unsuccessful transmissions for the different blockchain-based IoT systems. It analyzes that the UE-eHealthChain

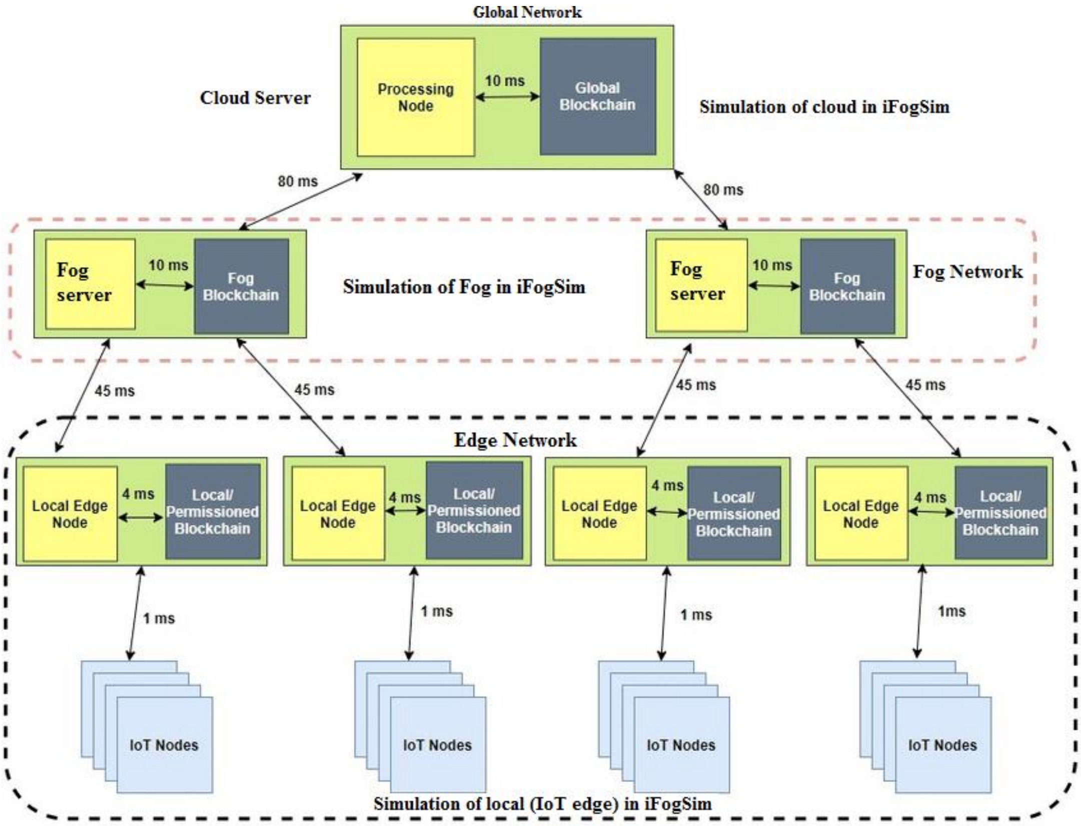


Figure. 6 High-level designs of blockchain-edge model for IoT systems in iFogSim

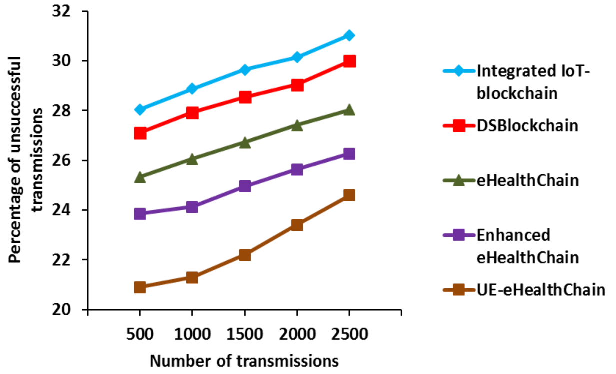


Figure. 7 Percentage of unsuccessful transmissions vs. number of transmissions

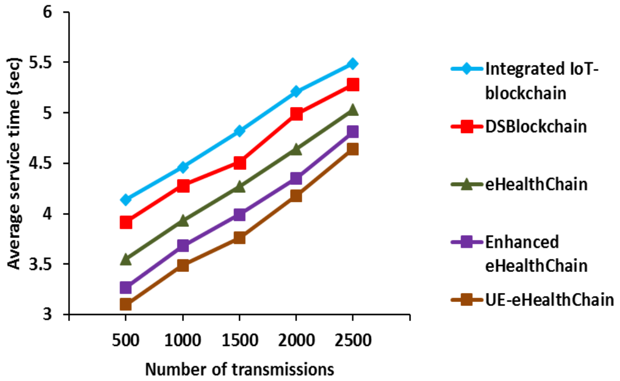


Figure. 8 Average service time vs. number of transmissions

system reduces the percentage of unsuccessful transmissions compared to the others because of using EOAuth 2.0 protocol and ECoAP. When there are 500 transmissions, the percentage of unsuccessful transmissions for UE-eHealthChain is 25.5%, 22.9%, 17.5%, and 12.4% less than the integrated IoT-blockchain, DSBlockchain, eHealthChain, and enhanced eHealthChain systems, respectively.

4.1.2 Average service time

It is computed as:

$$Avg.\,service\ time = \frac{\sum total\ processing\ time + \sum total\ network\ time}{Number\ of\ transmissions} \quad (4)$$

Fig. 8 illustrates the average service time (in sec) for the different blockchain-based IoT systems under the number of transmissions. It analyzes that the UE-eHealthChain system decreases the average service time compared to the others because of using the adaptive backoff to minimize the authentication time and inactive latency, respectively. When there are 500 transmissions, the average service time of UE-eHealthChain is 25.12%, 20.92%, 12.68%, and 5.2% less than the integrated IoT-blockchain,

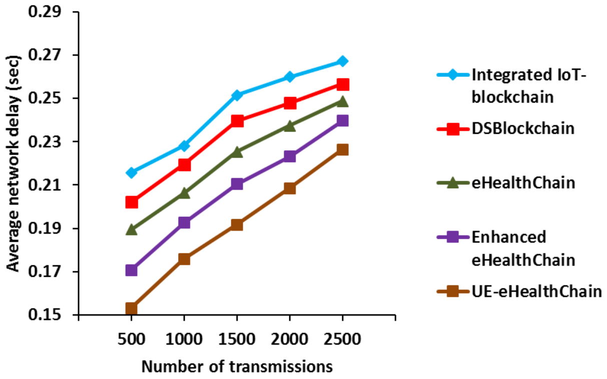


Figure. 9 Average network delay vs. number of transmissions

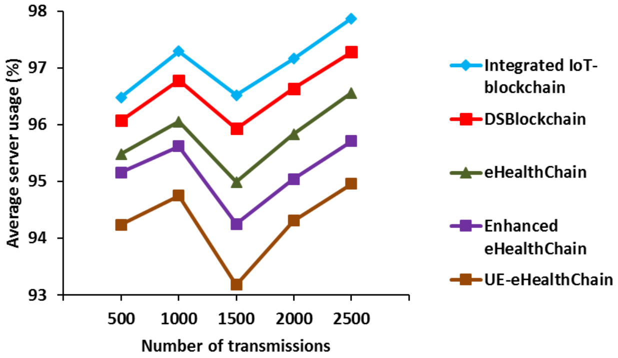


Figure. 10 Average server usage vs. number of transmissions

DSBlockChain, eHealthChain, and enhanced eHealthChain systems, respectively.

4.1.3 Average service time

It is the mean time between the client and server to transmit and access the data over a network.

Fig. 9 portrays the average network delay (in sec) for the different blockchain-based IoT systems under the number of transmissions. It observes that the UE-eHealthChain system decreases the average network delay compared to the others by decreasing the authentication time and inactive latency in dynamic network configurations. For 500 transmissions, the average network delay of UE-eHealthChain is 29.01%, 24.2%, 19.16%, and 10.25% less than the integrated IoT-blockchain, DSBlockchain, eHealthChain, and enhanced eHealthChain systems, respectively.

4.1.4 Average server usage

It is the mean utilization of the server during data transmission, authentication, and authorization processes.

Fig. 10 displays the average server usage (in %) for the different blockchain-based IoT systems under the number of transmissions. For 500 transmissions, the average server usage of UE-eHealthChain is 2.32%, 1.9%, 1.3%, and 0.97% less than the integrated IoT-blockchain, DSBlockchain, eHealthChain, and enhanced eHealthChain systems, respectively. It means that the usage of the server is reduced for the UE-eHealthChain system compared to other systems when the number of transmissions increases.

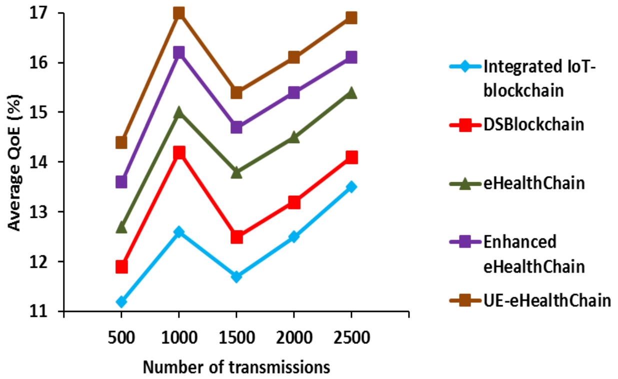


Figure. 11 Average QoE vs. number of transmissions

4.1.5 Average QoE

It is the mean QoE experienced by all clients in the network.

Fig. 11 shows the average QoE (in %) for the different blockchain-based IoT systems under the number of transmissions. It indicates that the UE-eHealthChain system decreases the average QoE compared to the other systems by decreasing the authentication time and inactive latency in dynamic network configurations. For 500 transmissions, the average QoE of UE-eHealthChain is 28.57%, 21.01%, 13.39%, and 5.88% greater than the integrated IoT-blockchain, DSBlockchain, eHealthChain, and enhanced eHealthChain systems, respectively.

4.2 Performance analysis

- Confidentiality: Any uncertified node is rejected from the data access with the help of this security service.
- Authorization: All nodes provide a unique key pair to perform cryptographic processes with the help of this security service. It is realized by applying the public key when any suspicious node desires to interact with network nodes; it requires the public key pair of the certified node.
- Integrity: It guarantees that data accepted by the target node have not been modified during transmission either by conflict or tampering by an untrustworthy node.

Fig. 12 shows the confidentiality achieved by the OAuth 2.0+MQTT, OAuth 2.0+CoAP, EOAuth

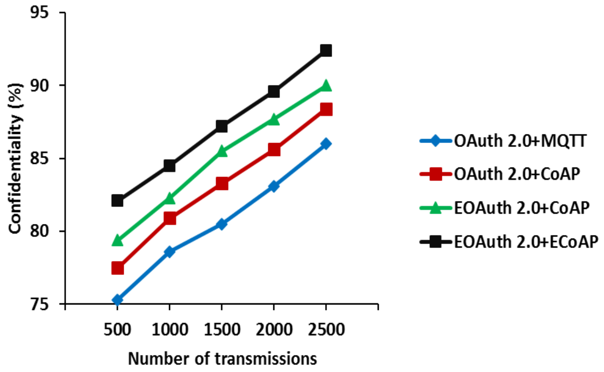


Figure. 12 Confidentiality vs. number of transmissions

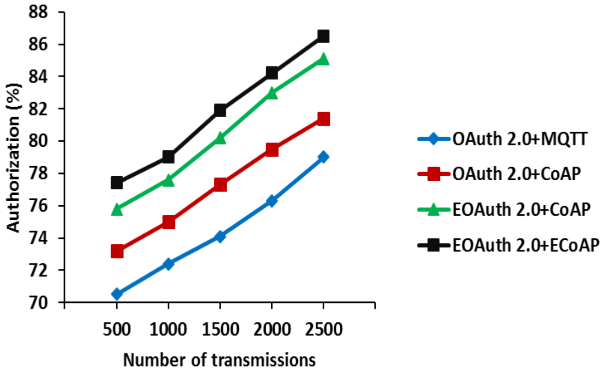


Figure. 13 Authorization vs. number of transmissions

2.0+CoAP and EOAuth 2.0+ECoAP with varying the number of transmissions. It indicates that the EOAuth 2.0+ECoAP can increase the confidentiality of data storage and access in healthcare systems compared to the others. For 1500 transmissions, the confidentiality of EOAuth 2.0+ECoAP is 8.32%, 4.68%, and 1.99% greater than the OAuth 2.0+MQTT, OAuth 2.0+CoAP, and EOAuth 2.0+CoAP, respectively. This is because of using adaptive RTO values and ABF for achieving reliable data transmission.

Fig. 13 shows the authorization attained by the OAuth 2.0+MQTT, OAuth 2.0+CoAP, EOAuth 2.0+CoAP and EOAuth 2.0+ECoAP with varying the number of transmissions. For 1500 transmissions, the authorization of EOAuth 2.0+ECoAP is 10.53%, 5.95%, and 2.12% higher than the OAuth 2.0+MQTT, OAuth 2.0+CoAP, and EOAuth 2.0+CoAP, respectively, due to the consideration of the adaptive backoff period, which reduces the authentication period and inactive latency.

Fig. 14 shows the data integrity obtained by the OAuth 2.0+MQTT, OAuth 2.0+CoAP, EOAuth 2.0+CoAP, and EOAuth 2.0+ECoAP with varying the number of transmissions. For 1500 transmissions, the data integrity of EOAuth 2.0+ECoAP is 7.82%, 3.94%, and 1.36% greater than the OAuth 2.0+MQTT, OAuth 2.0+CoAP, and EOAuth 2.0+CoAP, respectively, by enhancing the confidentiality of accessing sensitive information in the clinical systems.

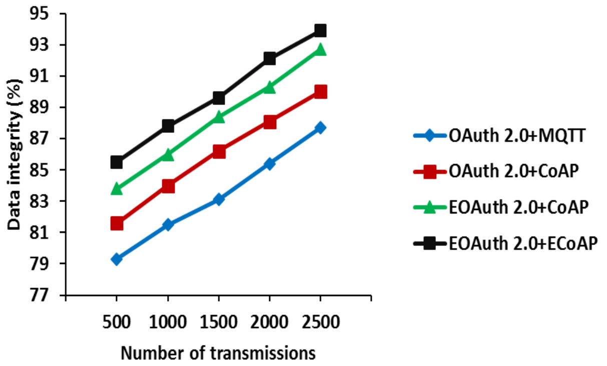


Figure. 14 Data integrity vs. number of transmissions

5. Conclusion

This paper introduces the ECoAP, a component of the UE-eHealthChain system that uses adaptive strategies for congestion control and reliable data transmission. The ECoAP includes adaptive RTO estimation with an ABF, DLR estimation, and RREI scheme to calculate adaptive RTO and RTT values. These values are used to regulate backoff values and control congestion in dynamic networks, leading to effective group transmission and minimized rebroadcasts. Implementation findings show that the ECoAP outperforms the classical CoAP in the UE-eHealthChain system with EOAuth 2.0. The results show that the UE-eHealthChain has 24.6% unsuccessful transmissions, 4.64 seconds average service time, 0.2264 seconds average network delay, 94.96% average server usage, 16.9% average QoE, 92.4% confidentiality, 86.5% authorization, and 93.9% data integrity for 2500 transmissions.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, methodology, software, validation, Saikumari; formal analysis, investigation, Victo Sudha; resources, data curation, writing—original draft preparation, Saikumari; writing—review and editing, Saikumari; visualization, supervision, Victo Sudha.

References

[1] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, “IoT Information Sharing Security Mechanism Based on Blockchain Technology”, *Future Generation*

Computer Systems, Vol. 101, pp. 1028-1040, 2019.

[2] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When Blockchain Meets Internet of Things: Characteristics, Challenges, and Business Opportunities", *Journal of Industrial Information Integration*, Vol. 15, pp. 21-28, 2019.

[3] P. M. Chanal and M. S. Kakkasageri, "Security and Privacy in IOT: A Survey", *Wireless Personal Communications*, Vol. 115, No. 2, pp. 1667-1693, 2020.

[4] A. Ahad, M. Tahir, M. Aman Sheikh, K. I. Ahmed, A. Mughees, and A. Numani, "Technologies Trend Towards 5G Network for Smart Health-Care Using IoT: A Review", *Sensors*, Vol. 20, No. 14, pp. 1-22, 2020.

[5] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, "Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives", *Journal of Food Quality*, pp. 1-20, 2021.

[6] H. M. Hussien, S. M. Yasin, S. N. I. Udzir, A. A. Zaidan, and B. B. Zaidan, "A Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges, Recommendations and Future Direction", *Journal of Medical Systems*, Vol. 43, No. 10, pp. 1-35, 2019.

[7] P. Pawar, N. Parolia, S. Shinde, T. O. Edoh, and M. Singh, "eHealthChain – A Blockchain-Based Personal Health Information Management System", *Annals of Telecommunications*, pp. 1-13, 2021.

[8] T. Saikumari and G. V. S. George, "An Enhanced Authorization Protocol in Blockchain for Personal Health Information Management System", *International Journal of Computer Networks and Applications*, Vol. 10, No. 3, pp. 277-295, 2023.

[9] R. Hassan, A. M. Jubair, K. Azmi, and A. Bakar, "Adaptive Congestion Control Mechanism in CoAP Application Protocol for Internet of Things (IoT)", In: *Proc. of IEEE International Conf. on Signal Processing and Communication*, pp. 121-125, 2016.

[10] E. Ancillotti, R. Bruno, C. Vallati, and E. Mingozzi, "Design and Evaluation of a Rate-Based Congestion Control Mechanism in CoAP for IoT Applications", In: *Proc. of IEEE 19th International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pp. 14-15, 2018.

[11] F. Ouakasse and S. Rakrak, "An Improved Adaptive CoAP Congestion Control Algorithm", *International Journal of Online & Biomedical Engineering*, Vol. 15, No. 3, pp. 96-109, 2019.

[12] C. Suwannapong and C. Khunboa, "Congestion Control in CoAP Observe Group Communication", *Sensors*, Vol. 19, No. 15, pp. 1-14, 2019.

[13] L. Hang and D. H. Kim, "Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity", *Sensors*, Vol. 19, No. 10, pp. 1-26, 2019.

[14] R. Herrero, "Analysis of IoT Mechanisms for Media Streaming", *Internet of Things*, Vol. 9, pp. 1-13, 2020.

[15] K. Khalil, K. Elgazzar, A. Abdelgawad, and M. Bayoumi, "A Security Approach for CoAP-Based Internet of Things Resource Discovery", In: *Proc. of IEEE 6th World Forum on Internet of Things*, pp. 1-6, 2020.

[16] C. Vallati, F. Righetti, G. Tanganelli, E. Mingozzi, and G. Anastasi, "Analysis of the Interplay between RPL and the Congestion Control Strategies for CoAP", *Ad Hoc Networks*, Vol. 109, pp. 1-14, 2020.

[17] G. A. Akpakwu, G. P. Hancke, and A. M. Abu-Mahfouz, "CACC: Context-Aware Congestion Control Approach for Lightweight CoAP/UDP-Based Internet of Things Traffic", *Transactions on Emerging Telecommunications Technologies*, Vol. 31, No. 2, pp. 1-19, 2020.

[18] P. Aimtongkham, P. Horkaew, and C. So-In, "An Enhanced CoAP Scheme Using Fuzzy Logic with Adaptive Timeout for IoT Congestion Control", *IEEE Access*, Vol. 9, pp. 58967-58981, 2021.

[19] C. Suwannapong and C. Khunboa, "EnCoCo-RED: Enhanced Congestion Control Mechanism for CoAP Observe Group Communication", *Ad Hoc Networks*, Vol. 112, pp. 1-10, 2021.

[20] A. Aldribi and A. Singh, "Blockchain Empowered Smart Home: A Scalable Architecture for Sustainable Smart Cities", *Mathematics*, Vol. 10, No. 14, pp. 1-22, 2022.

[21] T. Kumar, E. Harjula, M. Ejaz, A. Manzoor, P. Porambage, I. Ahmad, and M. Ylianttila, "BlockEdge: Blockchain-Edge Framework for Industrial IoT Networks", *IEEE Access*, Vol. 8, pp. 154166-154185, 2020.

[22] A. Betzler, C. Gomez, I. Demirkol and J. Paradells, "CoAP Congestion Control for the Internet of Things", *IEEE Communications Magazine*, Vol. 54, No. 7, pp. 154-160, 2016.