*Journal of Discrete Mathematical Sciences & Cryptography*
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-B, pp. 2081–2092
DOI : 10.47974/JDMSC-2366

# Cyber security with blockchain-based cyber-physical system for key generation in medi-cloud computer systems

Vishnu Priya Arivanantham *
*Department of Computational Intelligence*
*School of Computer Science and Engineering*
*Vellore Institute of Technology*
*Vellore 632014*
*Tamil Nadu*
*India*

Hayder M. A. Ghanimi †
*Department of Information Technology*
*College of Science*
*University of Warith Al-Anbiyaa*
*Karbala 5751*
*Iraq*

*and*

*Department of Computer Science*
*College of Computer Science and Information Technology*
*University of Kerbala*
*Karbala 5751*
*Iraq*

Sagar Ramesh Rane §
*Department of Computer Engineering*
*Army Institute of Technology*
*Pune 411015*
*Maharashtra*
*India*

* *E-mail:* a.vishnupriya@vit.ac.in (Corresponding Author)
† *E-mail:* hayder.alghanami@uowa.edu.iq
§ *E-mail:* sagarrane@aitpune.edu.in

V. Jasmine Sowmya [‡]
*Department of Computer Science and Engineering*
*Koneru Lakshmaiah Education Foundation*
*Vaddeswaram 522502*
*Andhra Pradesh*
*India*

Kamal Poon [@]
*Department of College of Science and Engineering*
*Southern Arkansas University*
*Magnolia*
*AR 71753*
*United States of America*

N. Mythili [#]
*Department of Computer Science and Engineering*
*St. Joseph's Institute of Technology*
*Chennai 600119*
*Tamil Nadu*
*India*

Sudhakar Sengan [$]
*Department of Computer Science and Engineering*
*PSN College of Engineering and Technology*
*Tirunelveli 627152*
*Tamil Nadu*
*India*

Pankaj Dadheech [^]
*Department of Computer Science and Engineering*
*Swami Keshvanand Institute of Technology, Management & Gramothan (SKIT)*
*Jaipur 302017*
*Rajasthan*
*India*

[‡] *E-mail:* **vemulajasmine@kluniversity.in**
[@] *E-mail:* **kamalpoon57@gmail.com**
[#] *E-mail:* **mythilyna@gmail.com**
[$] *E-mail:* **sudhasengan@gmail.com**
[^] *E-mail:* **pankajdadheech777@gmail.com**

**Abstract**

Ensuring the confidentiality and integrity of healthcare records in Blockchain (BC)-based Medi-Cloud Systems (MCS) is vital, with a focus on Key Management Systems (KMS). This investigation presents a complete technique for Key Generation (KG), focusing on three key metrics: Key Generation Time (KGT), Operational Cost (OC), and Share Distribution Efficiency (SDE). The KGT's computation of the time required to generate the encryption keys impacts Network Throughput (NT). To optimize costs, cost control measures the costs of data centers, computer power, and network services. SDE's analysis of the key share distribution across the nodes impacts the efficiency and security of the Cyber-Physical System (CPS). To make MCS more reliable and secure, the researchers recommend the most effective method for KMS based on these data points. Integrating BC + HCS requires KMS that are secure and flexible, and the recommendation for MCS + BC ensures that this level of security is achieved.

***Subject Classification:*** *93E10, 94A13.*

***Keywords:*** *Key generation, Medical data, Cost, Cloud, Security, Data privacy, Blockchain.*

## 1. Introduction

Medi-Cloud Systems (MCS) with blockchain (BC) add a layer of security to Healthcare Systems (HCS) data storage and sharing. A scalable and adaptable model, the Cloud Computing Environment (CCE), has been used by MCS. The BC, which provides autonomous and more secure records, is also used [1]. In the context of MCS+BC, the Key Management System (KMS) is a key feature that becomes accessible when addressing HCS data, which requires protection from tampering or unauthorized access [2]. To enhance the framework's capacity for communication and secure data sharing, these keys are essential. The reliability and trustworthiness of the KMS will impact the level of security the MCS provides. A significant problem with an MCS + BC is the cryptographic KMS, which is susceptible to several vulnerabilities. In addition to the distributed and accessible system of BC, previously used Key Generation (KG) methods may not be successful. Complex systems develop key elements and other related components that attempt to prevent this from happening. A technique that actively divides a key into segments and shares them with different users is Shamir's Secret Sharing Scheme (SSS). This method reduces the likelihood of key vulnerability by allowing the key to regenerate with a precise number of messages [3]. BC is predicted to provide greater security than initially anticipated through the implementation of a fixed Cyber-Physical System (CPS) for record-maintaining [4]. The BC maintains a record of all key-related transactions, such as generation, distribution, and rotation. This record enables the monitoring and storage of all KMS measures, ensuring their permanence and preventing unauthorized modifications. Because it permits computations on the encrypted data, Homomorphic Encryption (HE) is a feature of Implementing MCS via BC. This method enhances data security and confidentiality by storing sensitive data in a manner that prevents it from being

accessible in an encrypted form during data processing. Several users can perform computations on encrypted data using Secure Multi-Party Computation (MPC) techniques, which also enhance data security [5]. When integrated with BC, this *state-of-the-art* cryptography secures an accurate KMS. In addition to securing the MCS from multiple security risks, this model maintains the patient's records securely. Therefore, this study secures the security of private medical data through the use of BC, innovative encryption methods, and the invention of MCS + BC [6].

## 2. Related Works

With the application of Artificial Intelligence (AI), the CC is redefining data storage and distribution, providing new possibilities for industries such as healthcare services. Integrating CC with other AI in HCS provides reliable solutions for data analysis of diseases, disease diagnostics, and medical imaging [7-10]. This synergy facilitates digital transformation by providing flexible, reliable, and practical solutions that address the challenges of contemporary medicine. Tab. 1 summarizes the techniques used, the purposes of the studies, and the significant conclusions or findings from each source. The present research overlooks the interactions and challenges associated with implementing cloud, AI, the Internet of Things (IoT), and 5G in healthcare systems (HCS) applications. Additionally, there is a scarcity of multi-country cost-utility analyses, implementation problems, and the impact of complex algorithms on patients' outcomes. Future research should aim to close these gaps by presenting more applied studies, including cost-effective and comprehensive integration methods that can be effectively implemented (Table 1).

**Table 1**

**Comprehensive Analysis CC-based BC System**

| Reference | Techniques Used | Purpose | Inference |
|---|---|---|---|
| **[11]** | CC, AI | Medical Image Analysis (MIA) and diagnosis | Explores next-generation AI + CC for MIA, highlighting predictions in this field. |
| **[12]** | Extreme Learning Machine (ELM), Principal Component Analysis (PCA) | Diabetes detection | Proposed a cloud-based e-HCS for early diabetes detection using ELM + PCA, achieving high accuracy with a vCPU-16 virtual machine. |
| **[13]** | MediBchain, BC | Privacy-preserving mutual authentication in mobile medical cloud | Introduced MBPA for secure and efficient authentication with minimal cost, ensuring patient anonymity and resistance to attacks. |
| **[14]** | CC, Edge Computing, AI | MIA for big data | Reviewed cloud, edge, and AI benefits for IoMT, focusing on data security, resource optimization, and future research directions. |

*Contd...*

| | | | |
|---|---|---|---|
| **[15]** | Generative AI, GANs (Generative Adversarial Networks) | MIA | Discusses the potential of generative AI in improving MIA, including synthetic data generation and Anomaly Detection (AD), with considerations for its ethical implementation. |
| **[16-17]** | Internet of Medical Things (IoMT), Wireless Body Area Networks (WBANs), Fog Computing, CC | Diabetes prediction | Developed an IoMT using Fog + CC for diabetes prediction, comparing fuzzy logic on fog and various ML on the cloud. |

## 3. Proposed Methodology – BC-Based MCS

The model also incorporates SSS, which helps divide and distribute the cryptographic keys with the help of a program among different parties so that only a specific set of parties (threshold as '*t*') can reconstruct the key, and the failure of individual parties would not affect the system. It is used to record and manage transactions on the significant operations of an organization using Hash Functions (HF) to enhance the immutability of data stored in the system. HE and Secure MPC allow computations on encrypted keys while maintaining the data hidden. Finally, it is noteworthy that Smart Contracts (SC) can manage vital rotation and revocation procedures to improve the CSP's security and performance. This approach guarantees reliability and security in managing the MCS's keys. Shamir's Secret Sharing ensures that an original key '*SSS*' can be reconstructed only by using '*t*' out of '*n*' shares and applying the Lagrange interpolation formula. Polynomial evaluation at points is applied in determining shares by substituting a polynomial at different points so that no two shares can result from each other to secure the key's distribution. For '*n*' distinct points '$x_i$', the share computation using polynomial '*f(x)*' is given in Eq. (1).

$$Share_i = f(x_i) = S + a_1 x_i + a_2 x_i^2 + \cdots \ldots \ldots + a_{t-1} x_i^{t-1} \quad (1)$$

Where, $x_i$ → selected so that they are distinct and non-zero to avoid singularities. The Lagrange interpolation formula for the secret reconstruction process reconstructs the secret with a real model that involves adding '*t*' shares, weighted by the points, to attain the value. For the specified shares $(Share_{i_1}, Share_{i_2}, \ldots \ldots \ldots \ldots, Share_{i_t})$, reconstruct 'S' using Eq. (2).

$$S = \sum_{j=1}^{t} Share_{i_j} \cdot \prod_{1 \le m \le t, m \ne j} \frac{x_m}{x_m - x_j} \quad (2)$$

KMS operations are recorded in a Merkle Tree Hashing (MTH) and BC consensus formula, which makes it virtually impossible for anyone to alter any transaction. MTH simplifies the transaction by using a tree structure where the hash of each node is a function of a concatenation of hashes of its child nodes, making the data more secure for a leaf node as $Leaf_i$, Eq. (3).

$$H(Leaf_i) = SHA - 256(Data_i) \quad (3)$$

The hashes are computed in the internal node using Eq. (4).

$$H(Internal_i) = SHA - 256(H(Left_{Child})||H(Right_{Child})) \quad (4)$$

The block 'B' is validated using Eq. (5) for proof-of-work-based BC.

$$H(B) < Target \quad (5)$$

where the concatenation process is specified as ||, H(B) is the block's hash, and Target is a predefined difficulty level.

Secure MPC with HE enables computation on encrypted data without revealing the data, using additive and multiplicative homomorphisms. The BC consensus mechanism verifies the validity of a block by checking the block's hash and ensuring that the computational difficulty aligns with the target for consensus. HE functions conducted addition securely on encrypted data, where the result of an operation on encrypted values retains the security of the data. Homomorphic multiplication enables the secure multiplication of encrypted values by a scalar while preserving the encrypted data. For additive HE, E(S1) and E(S2) are Eq. (6), and the multiplication of HE with a constant '*k*' is given in Eq. (7).

$$E(S_1 + S_2) = E(S_1) \oplus E(S_2) \quad (6)$$

$$E(k \cdot S) = E(S)^k \quad (7)$$

Where, $\oplus$ → The operation in the encrypted domain; $\cdot$→Multiplication in the plaintext domain.

The Rotation and Revolution processes include polynomial and share distribution with formulas for revoking the compromised shares and updating the BC. A new KG and share distribution revises a new secret key, computes new shares using a new polynomial, and distributes them securely to update the KMS. Generate a new secret key S′, and a new polynomial for shares is specified in Eq. (8).

$$f'(x) = S' + a'_1 x + a'_1 x^2 + \cdots + a'_{t-1} x^{t-1} \quad (8)$$

The new shares are estimated using Eq. (9).

$$share'_i = \mathrm{f}'(\mathrm{x_i}) = S' + a'_1 x_i + a'_1 x_i^2 + \cdots + a'_{t-1} x_i^{t-1} \quad (9)$$

Revocation update Eq. (10) changes the list of revoked shares by deleting compromised shares, which means these shares will not be effective anymore—issuing new shares and updating records to reflect the changes in the records. To invalidate a share as $\mathrm{Share_i}$, update the BC.

$$Revoked_{Shares} = \frac{Old_{Shares}}{Compromised_{shares}} \quad (10)$$

In the context of MCS, where CCE is understood in medical data management, the proposed KGM will guarantee the security of sensitive HCS information. SSS ensures that the key is not exposed to unauthorized personnel, while BC ensures that any transaction related to the key is not altered or compromised. Crypto-protection of medical data enables the execution of computations on the data while maintaining its confidentiality by encrypting it. SC is used to automate the procedures of key rotation and revocation, maintaining the system's security and keeping it up to date. These measures

ensure the stable and secure functioning of the MCS, thereby ensuring that legal requirements are met to protect medical data.

## 4. Result and Discussion

The simulation involves a CCE with virtual machines of varying capacities, such as vCPU-4, vCPU-8, and vCPU-16, to execute computational tasks. Hardware requirements are processing servers and storage that can meet the software's demands. Software requirements include cloud platforms such as AWS and Azure, programming languages like Python and Java, cryptographic libraries for SSS and HE, and BC platforms like Ethereum for consensus. MTH and secure MPC tools are also required. The MCS's efficiency and security are determined by comparing various performance indicators, including KGM time, operational costs, and share distribution efficiency, depending on the situation.

### 4.1 *Performance Metrics*

The KG is a method that involves several cryptographic computations, which can impact performance. The time it takes to generate keys must be minimized so that there is no delay in accessing and using them for secure operations (Figure 1 (a) and (b)).

The lower key value indicates the efficiency of the proposed system, as shown in Eq. (11).

$$T_{key} = T_{start} + T_{end} \tag{11}$$

where the time required for KG is assumed in $T_{key}$, the initiating process of KG time is assumed in $T_{start}$, and the KG process end is given in $T_{end}$. The operational cost in an MCS depends on the number and complexity of cryptographic computations, the storage needed for the keys, and the costs of sustaining the BC. Minimization of the cost necessary for optimizing the overall performance of MCS-BC. Cost containment is critical to the system's sustainability, Eq. (12).

$$C_{op} = C_{compute} + C_{storage} + C_{network} \tag{12}$$

where the whole operational cost is agreed upon as $C_{op}$, cost of computational resources by $C_{compute}$, cost of BC/keys is indicated by $C_{storage}$, and the cost of network data transmission of data is indicated by $C_{network}$.

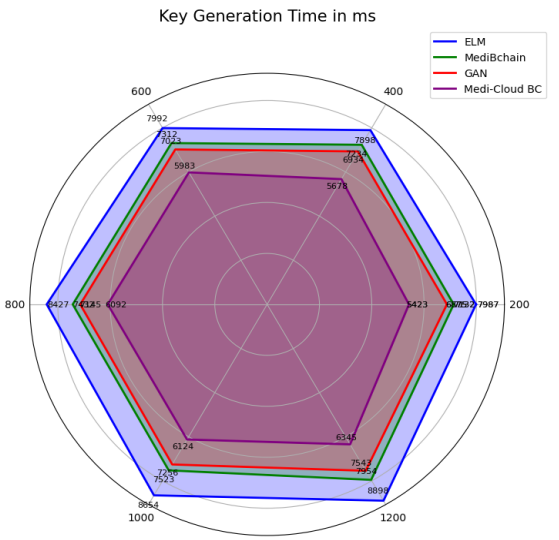
Proper share distribution eliminates time wastage when accessing the keys and ensures that whoever is involved in the share of the keys receives their share as needed. This is particularly relevant to applications that benefit from improved security through decentralized key management, as shown in Eq. (13).

$$E_{Dist} = \frac{S_{Delivered}}{T_{Distribution}} \tag{13}$$

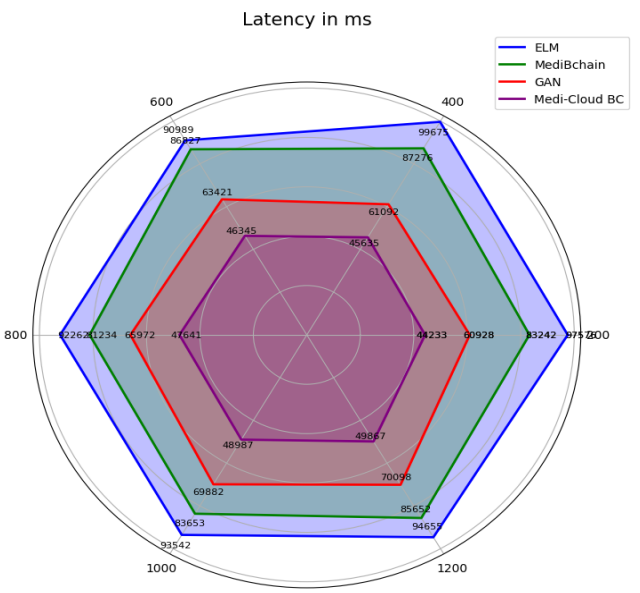
where the distribution efficiency is $'E_{dist}'$, success rate count is indicated by $S_{Delivered}$, and time utilization is indicated by $T_{Distribution}$.

End-to-End Delay (EED) refers to the delays in generating, distributing, and accessing the key related to the item. Lower EED means less response time and improves system performance, while EED Eq. (14).

$$L_{blockchain} = T_{transaction} + T_{block} + T_{confirmation} \quad (14)$$




(a) Key Generation Time




(b) Latency

**Figure 1**
**Comparison of (a) KG Time and (b) Latency**

Where, the time is taken for a single transaction as $T_{transaction}$, block inclusion in transactions is agreed upon as $T_{block}$, and the confirmation as $T_{confirmation}$.

4.2 *Simulation Discussion*

The comparative analysis of KGM process Time and EED across ELM, MediBchain, GAN, and MCS-BC reveals significant differences in performance and efficiency. For KGM-Time, MCS-BC consistently demonstrates the lowest time across all transaction counts, ranging from 5,423 *ms* at 200 transactions to 6,345 ms at 1,200 transactions (Figure 2).

This indicates its superior performance in KGM tasks compared to ELM, MediBchain, and GAN, which have higher KG times. In contrast, while having relatively higher KGM times than MCS-BC, GAN remains competitive compared to ELM and MediBchain, significantly as the transaction count increases. Regarding EED, MCS-BC exhibits the lowest EED values, with 44,233 *ms* at 200 transactions, and this increases to 49,867 ms at 1,200 transactions. This low EED indicates that MCS-BC is highly efficient in processing transactions compared to ELM, MediBchain, and GAN, which exhibit higher EED values, particularly as transaction volume increases. Operational costs are lowest for MCS-BC, starting at 712 and rising to 769, indicating cost efficiency in line with its performance metrics. Regarding Share Distribution Efficiency, MCS-BC leads achieved the highest efficiency percentages across all transaction counts, from 88% at 200 transactions to 93% at 1200 transactions. This efficiency aligns with its superior KGM performance and low EED, making MCS-BC the most balanced and effective system across the metrics evaluated (Figure 3).

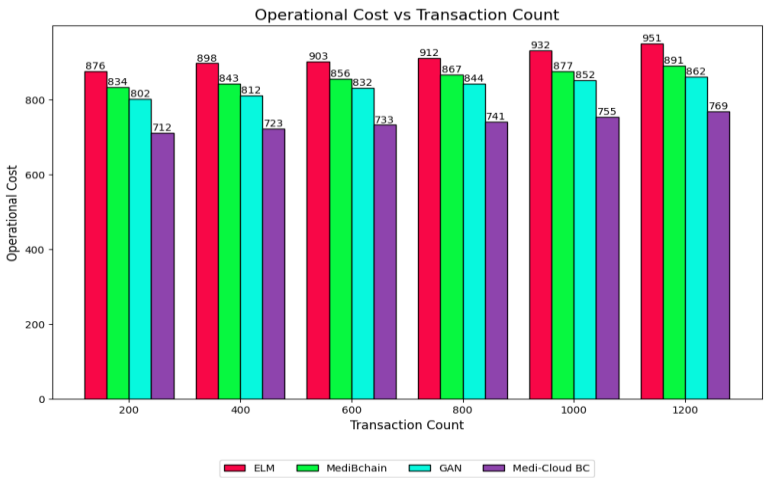



**Figure 2**
**Operational Cost**

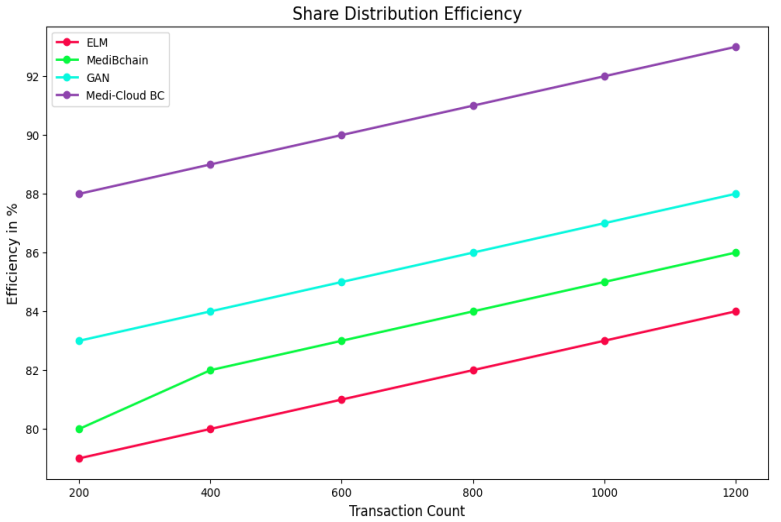



**Figure 3**
**Efficiency of Data Distribution**

## 5. Conclusion and Future Work

This paper demonstrates that the MCS is based on BC requirements to enhance KG, control operating costs, and improve the efficiency of share distribution, thereby achieving the objective of securing the CPS. Thus, by concentrating on these measures, it is possible to maintain the effectiveness of cryptographic KGM while enhancing the security and effectiveness of the model. The proposed models enhance KMS's key features, ensuring medical data is secure and accessible in a CCE. Subsequent studies should focus on improving encryption methods and exploring the potential of KGM in projecting MCS. Further studies will be devoted to improving KGM by integrating the most advanced cryptographic techniques and scaling mechanisms, thereby providing increased levels of security and efficiency in prospective MCS environments.

## References

[1] A. Motwani, P. K. Shukla and M. Pawar, "Novel framework based on deep learning and cloud analytics for smart patient monitoring and recommendation (SPMR)", *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 5, pp. 5565-5580, (2023).

[2] A. Uthiramoorthy, A. Bhardwaj, J. Singh, K. Pant, M. Tiwari and J. L. A. Gonzáles, "A Comprehensive Review on Data Mining Techniques

in managing the Medical Data cloud and its security constraints with the maintained of the communication networks", *IEEE International Conference on Artificial Intelligence and Smart Communication*, pp. 618-623. IEEE, (2023).

[3] A. E. Adeniyi, K. M. Abiodun, J. B. Awotunde, M. Olagunju, O. S. Ojo and N. P. Edet, "Implementation of a block cipher algorithm for medical information security on cloud environment: using modified advanced encryption standard approach", *Multimedia Tools and Applications,* vol. 82, no. 13, pp. 20537-20551, (2023)

[4] M. M. Islam and Z. A. Bhuiyan, "An integrated, scalable framework for cloud and IoT-based green healthcare system", *IEEE Access*, vol. 11, pp. 22266-22282, (2023).

[5] Z. Wang, W. Gao, M. Yang and R. Hao, "Enabling Secure Data sharing with data deduplication and sensitive information hiding in cloud-assisted Electronic Medical Systems", *Cluster computing*, vol. 26, no. 6, pp. 3839-3854, (2023).

[6] S. S. Vellela, B. V. Reddy, K. K. Chaitanya and M. V. Rao, "An integrated approach to improve e-healthcare system using dynamic cloud computing platform", 5th IEEE International Conference on Smart Systems and Inventive Technology, pp. 776-782, (2023).

[7] J. Wu, H. Wang, C. Ni, C. Zhang and W. Lu, "Case Study of Next-Generation Artificial Intelligence in Medical Image Diagnosis Based on Cloud Computing", *Journal of Theory and Practice of Engineering Science,* vol. 4, no. 2, pp. 66-73, (2024).

[8] S. K. Sharma, A. T. Zamani, A. Abdelsalam, D. Muduli, A. A. Alabrah, N. Parveen and S. M. Alanazi, "A diabetes monitoring system and health-medical service composition model in cloud environment", *IEEE Access,* vol. 11, pp. 32804-32819, (2023).

[9] S.K. Sharma, A. T. Zamani, A. Abdelsalam, D. Muduli, A. A. Alabrah, N. Parveen and S. M. Alanazi, "A diabetes monitoring system and health-medical service composition model in cloud environment", *IEEE Access,* vol. 11, pp. 32804-32819, (2023).

[10] L. Sun, X. Jiang, H. Ren and Y. Guo, "Edge-cloud computing and artificial intelligence in Internet of medical things: architecture, technology, and application", *IEEE Access*, vol. 8, pp. 101079-101092, (2020).

[11] J. Xu, B. Wu, J. Huang, Y. Gong, Y. Zhang and B. Liu, "Practical Applications of Advanced Cloud Services and Generative AI Systems in Medical Image Analysis", arXiv preprint arXiv:2403.17549, (2024).

[12] E. Yıldırım, M. Cicioğlu and A. Çalhan, "Fog-cloud architecture-driven Internet of Medical Things framework for healthcare monitoring", *Medical & Biological Engineering & Computing,* vol. 61, no. 5, pp. 1133-1147, (2023).

[13] M. A. Ghanimi, Hayder, P. Melgarejo-Bolivar, Romel, A. Tumi-Figueroa, S. Ray, D. Pankaj and S. Sudhakar, "Merkle-Damgå RD hash functions and blockchains: Securing electronic health records, *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-A, pp. 237–248, (2024).

[14] M. A. Ghanimi, Hayder T. Gopalakrishnan, D. G. Joel Sunny, K. Amarendra, D. Pankaj and S. Sudhakar, Chebyshev polynomial approximation in CNN for zero-knowledge encrypted data analysis," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, pp. 203–214, (2024).

[15] P. Vidya Sagar, M. A. Ghanimi, Hayder, L. Prabhu Arokia Jesu Raja, D. Pankaj and S. Sudhakar, "Secure multi-party computation in deep learning: Enhancing privacy in distributed neural networks," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, pp. 249–259, (2024).

[16] G. R. K. Rao, M. A. Ghanimi Hayder, V. Ramachandran, D. Al-Qahtani, D. Pankaj and S. Sudhakar, "Enhanced security in federated learning by integrating homomorphic encryption for privacy-protected, collaborative model training," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, pp. 361–370, (2024).

[17] K. Raguru Jaya, T. Gopalakrishnan, M. Divyapushpalakshmi, K. Amarendra, D. Pankaj and S. Sudhakar, "Security and privacy concerns in social networks mathematically modified metaheuristic-based approach," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-A, pp. 371–382, (2024).

*Received November, 2024*