

# Integrating blockchain, internet of things, and cloud for secure healthcare

K Senthur Kumaran, Ganesh Khekare, Thanu Athitya M, Aakash Arulmozhivarman,  
Arvind Pranav M, Hiritish Chidambaram N

School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India

## Article Info

### Article history:

Received May 29, 2024

Revised Sep 14, 2024

Accepted Sep 30, 2024

### Keywords:

Blockchain

Cloud security

Data immutability

Healthcare

Internet of things

Patient-centered architecture

## ABSTRACT

This research paper shows a decentralized healthcare architecture using the integration of internet of things (IoT), blockchain, and cloud to improve speed up tuple broken security as well as scalability. Real time health information (e.g., pulse rate, sugar level) from patients is captured by IoT devices and preprocessed at the fog computing layer to securely send them to a cloud platform. Immutability and transparency Patient health records recorded by blockchain solutions are highly irreversible due to the underlying technology, while smart contracts take care of data integrity and privacy. The cloud layer delivers storage that scales and works, also including real-time analytics to access patient data from anywhere for healthcare providers while the core helps manage long-term information architecture. It does so by automating healthcare workflows and taking some of the manual interventional processes out such that care delivery becomes even more efficient. Together, these technologies provide a secure, efficient, patient-centered healthcare system whose architecture can easily support future needs in remote patient monitoring and inter-institutional collaboration, responding to emerging demands from modern healthcare systems.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Ganesh Khekare

School of Computer Science and Engineering, Vellore Institute of Technology

Vellore-632014, Tamil Nadu, India

Email: khekare.123@gmail.com

## 1. INTRODUCTION

The article shows the state-of-the-art architecture of integrating blockchain into cloud systems for massive security, high performance, and scalability in several areas, including healthcare. It solves a number of key security-related issues by leveraging the decentralized nature and cryptographic capabilities of blockchain: data integrity and unauthorized access. Besides, the suggested architecture includes internet of things (IoT) devices for real-time data gathering, while cloud computing makes the architecture scalable enough for both data storage and processing. The study, based on recent technological developments, theoretically underpins how best to optimize healthcare data security, operational efficiency, and scalability. It presents a discussion on how blockchain will be important to address challenges persisting in cloud computing for data protection and system robustness in this ever-evolving field.

The blockchain data structure [1] consists of a series of slots in which every slot consists of a series of iterations [2], a nonce, a timestamp [3], the Merkle root summarizing transaction hashes, and the hash of the previous block [4]. In such a structure, the data cannot be modified, and any single transaction can be verified instantly. Conventional approaches to handling healthcare data are highly vulnerable to breaches, inefficient in handling, and cannot be monitored in real time [5]. With the great increase in healthcare data over some time

including sensitive information about patients [6], there is a high demand for solutions that are more secure [7], scalable, and efficient. IoT integrated [8] with blockchain [9] and cloud computing [10] securely addresses issues such as integrity, real-time monitoring, and scalable solution needs in management [11].

The framework proposed in this paper enhances healthcare data security and ensures continuity of access and dependability of the data. Optimally managing the ever-growing volume of healthcare data using blockchain to provide immutability of data and cloud computing for dynamic scalability. Consequently, there would be improved patient care, expedited treatment, and seamless health management.

## 2. LITERATURE REVIEW

The literature exposes the necessity for a new solution that was to be at the center of an exponentially growing number of IoT devices and data [12], thus opening ways to more advanced, secure [13], and efficient healthcare systems [14]. IoT technology, as applied in different aspects of healthcare [15], has changed the dimensions of patient monitoring, electronic health records (EHR) management [16], and disease prediction. Several literatures have discussed many models of IoT with AI and machine learning integrations that should improve medical services [17]. For instance, the early detection of chronic diseases by using IoT devices along with the employment of AI models tends to show promising results [18].

The main objective, however, remains the merging of IoT with blockchain technology so as to address issues of security, privacy challenges, and interoperability [19]. Some researchers have proposed frameworks based on blockchain for secure remote patient monitoring, EHR management, and COVID-19 patient tracking. These architectures facilitate data security and integrity, patient privacy, and system interoperability [20]. Whereas a lot has been achieved, issues related to scalability, constraints on resources, and difficulties in integration remain among others that are yet to be resolved and require further research and development. Literature review presents several smart healthcare technologies based on IoT and cloud computing. IoT was also shown in studies to have the potential to alleviate the burden on healthcare systems by adopting efficient solutions for remote patient monitoring [21]. The main applications include rapid disease diagnosis, prevention, and enhanced medical decision-making. However, issues of data security, mobility, heterogeneity, legalities, and big data management remain. Section C: describe various frameworks and models, including fog computing and blockchain-based approaches in finding ways to respond to the aforementioned challenges by increasing the efficiency of healthcare delivery systems. Fog-based frameworks ensure data processing efficiency, while blockchain offers secured, decentralized data management [22].

Overall, integrating IoT and cloud technologies in healthcare promises significant improvements, but addressing these challenges is crucial for successful implementation. The application of blockchain technology in cloud-based systems, particularly in healthcare to manage EHRs, has attracted much interest because of its capability to enhance security and privacy [23]. The integration of blockchain with cloud computing is the focus of scholars like Taşcı, Mentsiev, Cachin, Aggarwal, and Thakkar, who identified decentralized storage solutions as a way of reducing security risks common with centralized systems. The unchangeable nature of blockchain, including ledgering and cryptographic layers, directly addresses concerns regarding data tampering and unauthorized access. The medical information on the blockchain provides a reliable way of maintaining privacy and trust using open-source technologies, ensuring the safe sharing of EHRs among multiple hospitals. Decentralized applications (dApps) and enterprise solutions are built using ethereum, hyperledger, hyperledger fabric, and permissioned networks. Moreover, blockchain can be utilized for identity management, distributed storage systems, IoT, and secure file systems, which makes it an exceptional data management and collaboration enhancer across several domains apart from healthcare [24].

Cloud storage becomes more secure with the integration of blockchain technology, which guarantees data integrity through decentralized verification and immutable records, going beyond traditional audit methods. However, it is worth noting that scalability continues to be a challenge, and energy consumption also serves as another obstacle to fully realizing blockchain-based security for data management and sharing. Nonetheless, despite these limitations, blockchain remains a critical technology that offers contemporary transparent and distributed platforms for managing data. Ultimately, coming to the topic of security and auditing, let us consider a system that keeps the data safe and secure in the cloud while also ensuring no one can tamper with it. This system is called a blockchain-based decentralized public auditing scheme. It has two main phases. First, the setup phase prepares everything by passing on secret keys for secure classification and storage of the data. Second is the audit phase, which ensures the data is intact by using a smart contract on the blockchain to double-check that everything is in order [25].

Therefore, we suggest an approach we call distributed, by combining cloud servers with standard ones using blockchain techniques to focus on cloud task scheduling and address the performance overhead posed by blockchain. This whole process involves a few key players: the key generation centre (KGC), cloud server (CS), data user (U), and third-party auditor (TPA). They function together to ensure data stays safe and

nobody can mess with it. Now, there's another system called decentralized and privacy-preserving public auditing (DBPA). This structure uses algorithms such as GUI, setting, storage, gen log file, and checking log file to keep your data safe and private. It even uses blockchain to make sure everything is transparent and dependable.

### 3. METHOD

Decentralized autonomous healthcare system (DAHS) is designed on a multilayer approach built on blockchain, cloud computing, and IoT for flawless data flow, autonomous healthcare management, and real-time decision-making.

#### 3.1. IoT data collection and preprocessing

The architecture comprises IoT-enabled devices attached to a patient, which can monitor health parameters of heart bits, blood pressure level, sugar level, and physical activity. These above-mentioned IoT sensors are operational in continuous modes by monitoring vital health data. Preprocessing of data is done during the fog computing layer to filter out non-essential or redundant data that reduces the computational load on the cloud and increases real-time responsiveness.

#### 3.2. Blockchain-enabled data integrity

The filtered, crucial health data is sent to a permissioned blockchain network, where it will be immutably logged. IoT devices and healthcare providers are nodes in the network that can store the data in a decentralized way. Blockchain ensures that the records of a patient are tamper-proof, transparent, and traceable. Triggering healthcare workflows autonomously due to predefined health conditions is facilitated by smart contracts embedded within the blockchain. This may automatically trigger an alert to the provider if a patient's heart rate is high, for example, at which point action can be taken.

#### 3.3. Cloud computing for data storage and analysis

Elastic storage of the processed healthcare data in the cloud layer allows large-scale data management. Support for real-time health analytics is also provided, which can leverage machine learning algorithms to learn health trends from patients and predict future health insights. In cases of long-term data storage, scalability, and access are provided by the cloud; hence, healthcare providers and patients can retrieve health records at any time and from anywhere.

#### 3.4. Smart contracts for automation of healthcare actions

Autonomous health workflows rely on smart contracts that have rules and regulations predefined for the conduct of a system without the need for human intervention. These may be inbuilt rules that control access to data, alert patients in case of certain anomalies, or even health responses. For instance, they may set times for follow-up appointments independently, initiate prescriptions, or send off emergency alerts on their own based on patient data.

#### 3.5. Decentralized access and governance

Dynamic blockchain governance makes the decision-making of protocol changes, data access, and system updates decentralized. This methodology can be shared between health entities and can maintain data privacy and security for the patient.

## 4. PROPOSED ARCHITECTURE

Owing to the integration of blockchain, cloud computing, and IoT, DAHS architecture is designed as an integrated, decentralized, and autonomous paradigm in the aspect of layers. Various layers of the architecture perform various operations leading the patients to connect with the firm in real-time, automating data and security management, and making decisions autonomously. As shown in Figure 1 DAHS layers and operations are given as follows. The layerwise breakdown of system architecture for Figure 1 is shown in Table 1 and system requirements in Table 2 for the same.

#### 4.1. IoT layer

IoT layer: smart sensors are implanted in patients to gather data such as heart bit, blood pressure level cooling systems of sugar levels, and physical pendulum activity. These sensors are used to monitor patient data, and the captured data is pre-processed on edge before forwarding it for analysis in the cloud.

Here, what this process does is store the data in its original form and send over essential health information only. This layer is illustrated in the diagram as IoT patient sensor data and vital sign monitoring.

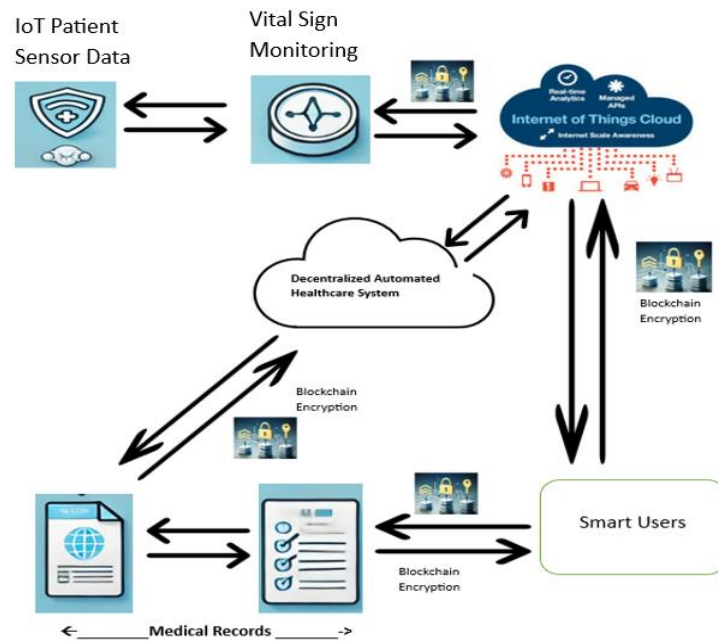


Figure 1. Decentralized automated healthcare system architecture

Table 1. Layer-wise breakdown of the system architecture

Layer	Function	Technologies used
1. IoT	Gathers patient sensor data from beacons.	Wearable sensors, IoT devices
2. Fog Computing	Pre-processes data at the edge filters essential data and sends to the cloud benefit	Fog nodes, edge computing
3. Blockchain	Security and immutability of data, as well as workflow automation through smart contracts	Permissioned blockchain, smart contracts
4. Cloud Computing	Offers scalable storage and real-time analytics of health data, providing a solution for long-term data management.	Cloud storage, distributed databases, AI
5. Application Layer	Provides built-in user interaction for patients and healthcare providers to retrieve data.	Web and mobile applications

Table 2. System requirements

Layer	Recommended specification	Description
1. IoT sensors	Low-power, high-accuracy sensors for real-time monitoring	Collects vital signs such as heart rate, glucose, and blood pressure.
2. Fog nodes	Decentralized processing units with low latency	Preprocesses information to reduce the load of cloud storage.
3. Blockchain nodes	High-performance nodes with secure data transmission	Permit immutable and decentralized control of healthcare data.
4. Cloud storage	Scalable cloud infrastructure with real-time analytics	Stores processed health data and supports predictive analytics.
5. Application platform	Mobile or web-based interface for end-users	Provides access to data by patients and healthcare providers.

#### 4.2. Fog computing layer

The fog computing layer: this is a distributed processing unit close to the network edge for pre-processing data faster before it is shifted to the cloud. By eliminating unnecessary data, it reduces the amount of information sent to the cloud and in turn optimizes real-time health monitoring. This layer allows only significant health monitors to be sent, limiting the processing time of irrelevant data. It improved system efficiency and the ability to respond to health crises by taking on preprocessing at one of the edges.

### 4.3. Blockchain layer

All the 3 layers are transparent. The blockchain layer ensures that patient records are stored in a decentralized and immutable manner. Tamper-proof health transactions: all patient data flowing between the cloud, healthcare providers, and patients themselves will be stored as health transactions in a blockchain ledger. This layer uses smart contracts to automatically kick off health workflows when particular health conditions are identified, thereby ensuring timely logic. The blockchain layer is equipped with an elliptical curve integrated encryption system (ECIES). With a permissioned blockchain only authorized entities e.g., health care providers and patients are allowed to access the data, AES-encrypted at rest and in transit ensuring transparency, and traceability as well achieves patient privacy across the system.

### 4.4. Underlying cloud computing layer (storage and analytics)

Cloud computing layer: the information collected from IoT devices is aggregated over the cloud computing layer that would in turn provide scalable storage and real-time analytics. Leveraging AI-driven algorithms, this layer processes massive amounts of health data to make sense of trends and predict the risk for future illnesses. The good thing is that the cloud offers a lot in terms of interoperability, so healthcare providers and patients can access health records whenever they want to. With secure data storage, the cloud also supports predictive analytics which can further assist in healthcare management.

### 4.5. Authentication and authorization layer

The third layer adds the dynamic blockchain governance, meaning that hospitals, regulators, and insurers can participate in allowance decisions on security updates or protocol changes as well as patient data access. Many healthcare blockchains are permission-based, using consortium chains for decentralized governance with no single control point to enforce the network and keep data sets distributed. This layer is essential to control access and make the system regulation-compliant, not only protecting patient privacy but also guaranteeing that everything inside it is intact.

### 4.6. Application layer

Users-patients and healthcare providers use mobile or web apps to interact with the system. User interaction layer they will be able to track their health status in real-time, check out the details of visits, and share them only with those they trust. On the other hand, for healthcare providers, this layer serves as a medium to avail access of patient data through alerting and reporting mechanisms so that they take necessary action based on decisions. Such a layer provides a smooth communication mechanism between the users and the healthcare system below it resulting in healthier lifestyle management, and real-time decision-making.

## 5. PERFORMANCE METRICS AND RESULTS

The use of the proposed hybrid of blockchain, IoT, and cloud computing was an improving factor in the aspect of security while enhancing the efficiency and scalability for everyday use in the healthcare system. The envisioned system and its architecture, which employs the dynamic proxy node selection algorithm or DPNS, also used sophisticated cryptographic mechanisms and eliminated key shortcomings of existing health systems.

The use of the proposed hybrid of blockchain, IoT, and cloud computing was an improving factor in the aspect of security while enhancing the efficiency and scalability for everyday use in the healthcare system. The envisioned system and its architecture, which employs the dynamic proxy node selection algorithm or DPNS, also used sophisticated cryptographic mechanisms and eliminated key shortcomings of existing health systems. The Figure 2 shows that when it comes to IoT devices, as the number of connected devices grew from 100 to 1,000; the system showed stable performance. Finally, our average processing time stayed at around 1.2 seconds with the only spike to almost 1.3 seconds when we were loaded on maximum capacity. It shows that the system scales efficiently, supporting many devices without major delays. Figure 3 shows the cumulative health alerts generated by smart contracts in the past 30 days. The mechanism provided a near real-time alerting capability using patient hemodynamics and identified events that fall outside of the normal range, sending 150 alerts over this time period. This graph shows the ability of the system to continuously monitor patient data, and automatically initiate alarms in response to health anomalies.

Formulas: formulas mentioned herein yield quantification of system efficiency in terms of latency, data reduction, and cloud scalability-important for performance metrics evaluation such as processing speed, storage growth, and efficiency in handling data. Total latency in the system is an important factor in determining the speed of gathering patients' data, processing it, and acting on it. The total latency in our proposed decentralized healthcare system is the aggregation of delays from the IoT layer, fog computing stage, blockchain, and cloud computing as shown in (1).

$$L_{Total} = L_{IoT} + L_{fog} + L_{Blockchain} + L_{Cloud} \tag{1}$$

Where,  $L_{IoT}$  represents the time it takes for IoT devices to collect real-time health data.  $L_{fog}$  accounts for the time spent pre-processing data at the fog layer.  $L_{Blockchain}$  is the time required for blockchain verification and recording.  $L_{Cloud}$  reflects the time needed for cloud storage and data analysis. While filtering out unnecessary data in the cloud, most of the work is done by the Fog computing layer. The effectiveness of filtering can be estimated by the data reduction ratio (R), representing the ratio of data filtered out versus the total data collected by IoT devices as shown in (2).

$$R = \frac{D_{input} - D_{filtered}}{D_{input}} * 100 \tag{2}$$

$D_{input}$  represents the original amount of data collected by IoT devices.  $D_{filtered}$  is the amount of data that has been removed by the fog layer. R is the data reduction percentage. Since the amount of patient data is increasing, it also means that the scaling for cloud storage should increase. The formula in storage growth at time t, which is represented as S(t), depicts how the evolution of storage varies as the data from IoT devices grows as shown in (3).

$$S(t) = S_0 + r * t \tag{3}$$

S(t) is the total storage required at time ttt.  $S_0$  represents the initial storage capacity. r is the rate at which data is generated (e.g., per day). t is time in days.

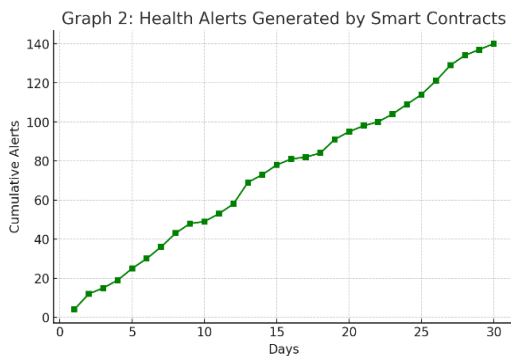


Figure 2. Data processing time vs. number of IoT devices

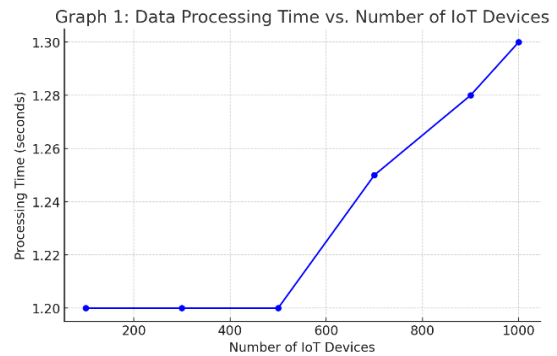


Figure 3. Health alerts generated by smart devices

**5.1. Security enhancement**

These helped to integrate blockchain technology to provide data security and privacy to prevent any third-party manipulation. The encryption of data using the ECIES in the process of the cloud storage of healthcare information offered the essential aspects of data security, namely, confidentiality and integrity. In the light of the considerations provided above the peculiar reliance on the framework provided a decentralized design that allowed for the removal of a single point for a DDoS attack or any other variety of security threats which is compliant with the high level of security required in the healthcare domain.

**5.2. Efficiency improvements**

The selection of a live proxy node reduced latency as it helped in managing the internal transfer of data between the IoT devices and the blockchain. Smart contracts control the loads within them and the dynamic selection of GPUs without the formation of bottlenecks. Also, the efficiency of access control automation enhanced the flow of data within the system, made it more sensitive, and cut out unnecessary time demands on the administrative side.

**5.3. Security enhancements**

The use of the blockchain helped to provide data security so that no one can modify or gain access to the data in any negative manner. ECIES was applied in encrypting healthcare data before its storage in the cloud affording strong confidentiality over the stored data as well as the stored data’s integrity. This made the

framework eliminate single points of failure and minimize DDoS attacks and other crazy security risks that were acceptable within the high-security requirements of the healthcare domain.

#### 5.4. Scalability

The concept of clustered IoT networks and off-chain storage to address scalability issues was found to have improved the framework's scalability, again, by a huge margin. Thus, by aggregating the devices into clusters, it was possible to extend the capacity of the system that was required for managing additional flows of information. Other methods of data storage, namely off-chain storage, made it possible to work effectively, without threatening the system's reliability and further expansion when more patients and data related to their health status would be involved.

#### 5.5. Real-time monitoring and data management

Since through IoT products, it is possible to monitor patients constantly and improve control over their health state, timely actions can be taken to prevent serious issues. Automated real-time data analysis and real-time alerting mechanisms by smart contracts greatly improved the value of patient care by providing immediate actions on adverse health status. The incorporation of cloud computing was more dynamic storing and processing demands from the numbers of data sets as generated by IoT devices.

#### 5.6. Efficiency improvements

This has ensured that through dynamic proxy node selection, there is a low latency in the transmission of data between a device within the internet of things and the blockchain. Such dynamic selection made through smart contracts also helped in achieving a proper load distribution where there were no bottlenecks. Also, the automated access control created a more efficient means of sharing data as it did not hinder functionality, and ease and cut down on time and unnecessary paperwork.

### 6. CONCLUSION

In conclusion, this research showed that the integration of IoT with blockchain and cloud computing in decentralized healthcare systems significantly improved how healthcare challenges could be addressed. This framework greatly improves the privacy, security efficiency, and scalability of the system by using IoT for real-time monitoring of patients, blockchain for secure immutable data storage, and cloud computing to obtain scalable storage or processing. Smart contracts will ensure that healthcare workflows are mostly automated, and less manual interaction is required which can improve the preciseness and speed of care. This system makes sure that patient data is secure and only available to those authorized while allowing doctors and patients to interact more efficiently. This enables better-paced response from a secure, urgent, and patient-centered architecture upon which future applications such as AI-driven predictive care for global health monitoring, and cross-border healthcare collaboration can be built. In sum, this decentralized paradigm has opened the floodgates by revolutionizing global healthcare delivery in a way that translates to better patient outcomes worldwide.





### REFERENCES

- [1] P. Pandey and R. Litoriya, "Securing e-health networks from counterfeit medicine penetration using blockchain," *Wireless Personal Communications*, vol. 117, no. 1, pp. 7–25, 2021, doi: 10.1007/s11277-020-07041-7.
- [2] J. Grover, "Security of vehicular Ad Hoc networks using blockchain: A comprehensive review," *Vehicular Communications*, vol. 34, 2022, doi: 10.1016/j.vehcom.2022.100458.
- [3] M. Jiang and X. Qin, "Distributed ledger technologies in vehicular mobile edge computing: a survey," *Complex and Intelligent Systems*, vol. 8, no. 5, pp. 4403–4419, 2022, doi: 10.1007/s40747-021-00603-7.
- [4] W. Hao *et al.*, "Towards a trust-enhanced blockchain P2P Topology for Enabling Fast and Reliable Broadcast," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 904–917, 2020, doi: 10.1109/TNSM.2020.2980303.
- [5] W. Al-Saqaf and N. Seidler, "Blockchain technology for social impact: opportunities and challenges ahead," *Journal of Cyber Policy*, vol. 2, no. 3, pp. 338–354, 2017, doi: 10.1080/23738871.2017.1400084.
- [6] I. A. Omar, R. Jayaraman, M. S. Debe, K. Salah, I. Yaqoob, and M. Omar, "Automating procurement contracts in the healthcare supply chain using blockchain smart contracts," *IEEE Access*, vol. 9, pp. 37397–37409, 2021, doi: 10.1109/ACCESS.2021.3062471.
- [7] E. Borgia, "The internet of things vision: Key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1–31, 2014, doi: 10.1016/j.comcom.2014.09.008.
- [8] J. Yang, J. Wen, B. Jiang, and H. Wang, "Blockchain-based sharing and tamper-proof framework of big data networking," *IEEE Network*, vol. 34, no. 4, pp. 62–67, 2020, doi: 10.1109/MNET.011.1900374.
- [9] C. Narmatha, S. Manimurugan, and P. Karthikeyan, "A smart CIoT with secure healthcare framework using optimized deep recuperator neural network long short-term memory," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 10551–10562, 2024, doi: 10.1109/JIOT.2023.3326547.
- [10] P. P. Ray, Di. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases," *IEEE Systems Journal*, vol. 15, no. 1, pp. 85–94, 2021, doi: 10.1109/JSYST.2020.2963840.





- [11] D. Chattaraj, B. Bera, A. K. Das, S. Saha, P. Lorenz, and Y. Park, "Block-CLAP: blockchain-assisted certificateless key agreement protocol for internet of vehicles in smart transportation," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 8092–8107, 2021, doi: 10.1109/TVT.2021.3091163.
- [12] G. Khekare, S. Ghugare, R. Khatri, G. Majumder, and U. Khekare, "Blockchain powered integrated health profile and record management system for seamless consultation leveraging unique identifiers," in *2nd International Conference on Emerging Trends in Information Technology and Engineering, ic-ETITE 2024*, 2024, doi: 10.1109/ic-ETITE58242.2024.10493266.
- [13] G. Khekare, S. Gambhir, I. S. Abdulrahman, C. M. S. Kumar, and V. Tripathi, "D2D network: implementation of blockchain based equitable cognitive resource sharing system," in *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2023*, 2023, pp. 908–912, doi: 10.1109/ICACITE57410.2023.10182834.
- [14] G. Nagasubramanian, R. K. Sakthivel, R. Patan, A. H. Gandomi, M. Sankayya, and B. Balusamy, "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud," *Neural Computing and Applications*, vol. 32, no. 3, pp. 639–647, 2020, doi: 10.1007/s00521-018-3915-1.
- [15] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Information Processing and Management*, vol. 58, no. 2, 2021, doi: 10.1016/j.ipm.2020.102468.
- [16] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," *Cluster Computing*, vol. 23, no. 3, pp. 2067–2087, 2020, doi: 10.1007/s10586-020-03058-6.
- [17] A. A. N. Patwary, A. Fu, S. K. Battula, R. K. Naha, S. Garg, and A. Mahanti, "FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain," *Computer Communications*, vol. 162, pp. 212–224, 2020, doi: 10.1016/j.comcom.2020.08.021.
- [18] G. Khekare and P. Verma, "Design of automatic key finder for search engine optimization in internet of everything," in *2020 IEEE International Conference for Convergence in Engineering, ICCE 2020-Proceedings*, 2020, pp. 464–468, doi: 10.1109/ICCE50343.2020.9290669.
- [19] S. Karumba, S. S. Kanhere, R. Jurdak, and S. Sethuvenkatraman, "HARB: a hypergraph-based adaptive consortium blockchain for decentralized energy trading," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14216–14227, 2022, doi: 10.1109/JIOT.2020.3022045.
- [20] E. Samir, H. Wu, M. Azab, C. Xin, and Q. Zhang, "DT-SSIM: a decentralized trustworthy self-sovereign identity management framework," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 7972–7988, 2022, doi: 10.1109/JIOT.2021.3112537.
- [21] Y. Zhang, B. Li, J. Wu, B. Liu, R. Chen, and J. Chang, "Efficient and privacy-preserving blockchain-based multifactor device authentication protocol for cross-domain IIoT," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22501–22515, 2022, doi: 10.1109/JIOT.2022.3176192.
- [22] S. Gao, Q. Su, R. Zhang, J. Zhu, Z. Sui, and J. Wang, "A privacy-preserving identity authentication scheme based on the blockchain," *Security and Communication Networks*, 2021, doi: 10.1155/2021/9992353.
- [23] G. Khekare, P. Verma, and S. Raut, "The smart accident predictor system using internet of things," *Cloud IoT: Concepts, Paradigms, and Applications*, pp. 163–175, 2022, doi: 10.1201/9781003155577-14.
- [24] M. Wazid, A. Kumar Das, and S. Shetty, "BSFR-SH: blockchain-enabled security framework against ransomware attacks for smart healthcare," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 1, pp. 18–28, 2023, doi: 10.1109/TCE.2022.3208795.
- [25] S. Itoo, A. A. Khan, V. Kumar, A. Alkhayyat, M. Ahmad, and J. Srinivas, "CKMIB: construction of key agreement protocol for cloud medical infrastructure using blockchain," *IEEE Access*, vol. 10, pp. 67787–67801, 2022, doi: 10.1109/ACCESS.2022.3185016.

## BIOGRAPHIES OF AUTHORS






**K Senthur Kumaran**     is a computer science engineering student specializing in the internet of things at VIT Vellore, he driven by a deep passion for technology and innovation. I've supplemented my academic journey by completing the foundation program and pursuing a diploma B.S. in data science at IIT Madras, honing skills in machine learning, statistics, python programming, and computational thinking. His proactive involvement extends to groundbreaking research in cloud security, where he presented a paper on integrating blockchain to bolster cloud systems against advanced threats. Overall, his academic and professional experiences have equipped me with a diverse skill set, fostering a practical approach to solving complex challenges in computer science and data science. He can be contacted at email: senthurkumaran2004@gmail.com.






**Ganesh Khekare**     holds a doctor of computer science and engineering from Bhagwant University, India in 2021. He is a postdoc fellow from Lincoln University, Malaysia. He also received his B.E. and M.E. (CSE) from Nagpur University, India in 2010 and 2013, respectively. He is currently an associate professor at the computer science and engineering department at Vellore Institute of Technology, Vellore, India. His research includes artificial intelligence and machine learning, data science, networks, and internet of things. He has published over 70 papers in international journals and conferences. He has done 5 Patents and 10 Copyrights. He is an active member of various professional societies like ACM, ISTE, IEEE Senior Member, and IEI. He can be contacted at email: khekare.123@gmail.com.








**Thanu Athitya M**    is a third-year computer science student at Vellore Institute of Technology, Vellore. He is passionate about artificial intelligence, machine learning, and cloud computing, aiming to leverage these technologies to innovate and solve complex problems. His dedication and curiosity drive him to excel in his academic and personal projects. He can be contacted at email: [thanuathitya1612@gmail.com](mailto:thanuathitya1612@gmail.com).






**Aakash Arulmozhiarman**    is a dynamic professional with expertise in computer science engineering and project management. He excels in optimizing processes and implementing innovative solutions. Aakash's strong analytical skills and attention to detail enable him to contribute effectively to diverse projects. He is committed to driving efficiency and achieving excellence in all his endeavors. He can be contacted at email: [akshvarman05@gmail.com](mailto:akshvarman05@gmail.com).



**Arvind Pranav M**    is a third-year computer science student at Vellore Institute of Technology, Vellore. He is passionate about artificial intelligence, machine learning, and cloud computing, aiming to leverage these technologies to innovate and solve complex problems. His dedication and curiosity drive him to excel in his academic and personal projects. He can be contacted at email: [arvindpranav2012@gmail.com](mailto:arvindpranav2012@gmail.com).



**Hiritish Chidambaram N**    is an ambitious and motivated individual with a strong background in engineering and technology. He is skilled in various programming languages and has a keen interest in software development. He is known for his innovative problem-solving abilities and dedication to continuous learning and professional growth. He can be contacted at email: [hiritish@gmail.com](mailto:hiritish@gmail.com).