Blockchain-Assisted Serverless Framework for AI-Driven Healthcare Applications

Akash Ghosh[1], Abhraneel Dalui[2], Lalbihari Barik[3], Jatinderkumar R. Saini[4]*, Sunil Kumar Sharma[5], Bibhuti Bhusan Dash[6], Satyendr Singh[7]*, Namita Dash[8], Susmita Patra[9], Sudhansu Shekhar Patra[10]*
Science & Bio-medical Center, HCR Lab, IIT Gandhinagar, India[1]
Department of Computer Applications, UEM Kolkata, India[2]
Faculty of Computing and Information Technology, King Abdulaziz University, Rabigh, Saudi Arabia[3]
Symbiosis Institute of Computer Studies and Research, Symbiosis International (Deemed University) Pune, India[4]
Doctorate Level Scholar, Arizona State University, United States[5]
Computer Science & Engineering Department, BML Munjal University, Gurugram, India[7]
Nalini Devi Women's College of Teacher Education, Bhubaneswar, India[8, 9]
School of Computer Applications, Kalinga Institute of Industrial Technology (KIIT) Deemed to be University, India[6, 10]

***Abstract*—With the advent of new sensor device designs, IoT based medical applications are increasingly being employed. This study introduces BlockFaaS: a Blockchain-assisted serverless framework that incorporates advanced AI models in latency sensitive healthcare applications with confidentiality, energy efficiency, and real-time decision-making. This framework combines the structure of AIBLOCK with dynamic sharding and zero knowledge proofs to make the framework strongly scalable with health-assured data inviolability with HealthFaaS, a serverless platform for cardiovascular risk detection. Explainable AI and federated learning models are introduced into the system to retain an equilibrium between data privacy and interpretability. All layers of communication use the Transport Layer Security protocol to ensure security. This proposed system is validated by new performance metrics such as real-time response rates and energy consumption, proving to be superior to the existing HealthFaaS and AIBLOCK technologies.**

***Keywords*—AIBLOCK; blockchain; healthfaas; latency optimization; serverless computing; Transport Layer Security (TLS)**

I. Introduction

Artificial intelligence (AI) and Internet of Things (IoT) technology have revolutionised the health sector by enabling real-time monitoring, detection, and decision-making. However, some limiting aspects, including disparities in data privacy, scalability, and latency, are beyond the power of AI-driven applications, especially in the detection of cardiovascular risk, to be achieved for efficient deployment. Serverless computing has dramatically solved the problem of scalable infrastructure on demand while simplifying complexities in infrastructures. Simultaneously, blockchain technologies have gained much attention in terms of the ability to secure, keep intact, and make information transparent. This research introduces BlockFaaS, a novel blockchain assisted serverless framework for AI-driven healthcare applications. The integration of AIBLOCK structure enhances data inviolability to the serverless platform of HealthFaaS applied in the detection of cardiovascular risk into the framework. This makes the framework highly scalable and a better solution for latency-sensitive medical applications. In addition, the usage of TLS protocol has assured the system's data confidentiality and secured communication across the system. Thus, the proposed framework will overcome the limitations that exist in today's healthcare technologies with improved data privacy, reducing response times, and achieving greater scalability in the overall system. This study presents a comparison of BlockFaaS with other existing frameworks to establish its feasibility for implementing high-performance modern healthcare systems. The new blockchain-assisted serverless framework for AI-driven healthcare applications, BlockFaaS, is presented in this work. The AIBLOCK structure provides enhanced data integrity, and dynamic sharding allows for scalable communication. In addition, it ensures secure and privacy-preserving communication through the use of zero-knowledge proofs. BlockFaaS balances between data privacy and interpretability with the integration of Explainable AI (XAI) and federated learning models. The framework is validated through comprehensive performance metrics, proving the superiority of the real-time response rates, energy efficiency, and data security involved.

A. Related Background

The next step in the development of the computer industry is often regarded as serverless computing [1]. In this case, the user does not control or own any servers. Another term for the software architecture, where an application is composed of one-time functions that are triggered by events or other invokers is "function-as-a-service" [2]. Yussupov et al. [3] proposed serverless architectures and emphasised the benefits of leveraging provider-managed components such as function-as-a-service (FaaS) and database-as-a-service (DBaaS) to minimise the amount of maintenance required of developers. The decentralised, unchangeable, and accountable relationships between blockchain technology and smart contracts as they relate to serverless systems were covered in this study. Ensuring security and privacy is crucial for any health apps in order to safeguard user data, adhere to legal requirements, and boost application confidence. Key management, storage, and token verification are among JWT's shortcomings [4][5][6].A blockchain-inspired secure and reliable data exchange

architecture is proposed in the cyber-physical healthcare industry 4.0 [7]. Stronger security measures are required and the AIBLOCK architecture uses blockchain technology to provide the immutability and secrecy of health data. Nevertheless, the HealthFaaS design does not use any external methods to ensure system security. User privacy is important when integrating a serverless platform with the Internet of Things. It is challenging to guarantee the integrity of patient data due to the various nature of the Internet of Things, which will raise privacy concerns for consumers [8]. Every line of connection between the patient data database, the IoT device, and the serverless platform is susceptible to intrusion [9]. Consequently, in the case of a communication channel assault, patient data may be altered (immutability). This might have serious consequences, such as misdiagnosis [10]. Transport Layer Security (TLS) with blockchain technology can reduce security and privacy issues. Blockchain's unique design, which ensures data integrity and immutability, makes it applicable in a number of industries, including banking and healthcare [11]. Three primary themes are examined in terms of terminology when discussing modern cloud computing delivery methods; (PaaS), (FaaS), and (IaaS) [12-14]. The cloud provider manages the infrastructure and servers, remaining completely independent of customers [15-18]. Contrary to popular belief, a system in which the server is completely absent is not referred to as serverless computing or FaaS [19-22].

This is a novel opportunity for the development of secure and scalable applications within health care, all these through the convergence of blockchain, serverless computing, and artificial intelligence. Such decentralized and tamper-proof blockchains have recently been picked up in highly demanding applications of industries for data integrity and security. Serverless platforms have been gaining attraction because they can dynamically allocate the resources without raising operational costs. Actual real-time capabilities with insights into immense amounts of patient data brought through AI, particularly through machine learning, in the prediction and diagnosis of disease. Available frameworks like HealthFaaS have led the way for serverless computing in healthcare but often are deficient in making sure robust data security. Similarly, blockchain-based solutions such as AIBLOCK are quite good at validating data but suffer from lack of efficiency while handling large workloads. This study puts all these technologies together to overcome the restrictions of the current solutions, providing BlockFaaS as a holistic framework for latency-sensitive and privacy-critical applications.

B. Research Objectives

The primary objectives of this research are:

- RO1: To develop a blockchain-enabled serverless framework, BlockFaaS, specifically customized for the use of AI in healthcare.
- RO2: To provide assured data confidentiality and integrity through advanced blockchain mechanisms, such as the AIBLOCK structure and TLS protocol.
- RO3: To enable true real-time dynamic scaling of resources to manage changing workloads involved in latency-sensitive medical applications.
- RO4: To assess the developed framework on scalability aspects, reducing the latency, ensuring data security, and cost-effectiveness in comparison with current solutions.

C. Organizations

The rest of the study is arranged as follows: Section II gives the previous works in the said area, Section III gives the research methodology. in Section IV the results are discussed and finally the conclusion and the future work is presented in Section V.

II. Literature Review

A. Existing Research and Analysis

According to language, contemporary cloud service delivery technologies may be categorised into three groups: Function as a Service (FaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) [7]. After the cloud operator moves from IaaS to FaaS, the cloud service provider takes care of infrastructure and server maintenance, keeping them apart from clients [23]. According to popular misconception, serverless technology, also known as (FaaS), does not, by itself, imply a serverless environment [24][20]. Indicates the fact that server administration as well as other infrastructure activities are in the domain of the service provider [25]. These are the blockchains that are usually applied by people sharing the same objective but do not necessarily trust each other. Each block in the blockchain contains several transactions grouped and added with a header that contains a hash [10]. The hash is a unique value produced for each block depending on the contents within the current block plus the preceding block's hash. The hashing algorithm is that component that makes blockchain an indestructible information chain. Given this hash, nobody can modify any transactions in those blocks that are currently validated [26]. With an emphasis on smart city air quality monitoring, Benedict [27] proposed a serverless, blockchain-enabled architecture for IIoT applications in society. It highlights issues with resource underutilisation and energy inefficiencies that arise in conventional IIoT application systems and are centred on the exploitation of blockchain and serverless computing capabilities. According to the study, air quality sensor data may be securely sent via cloud computing, fog, and edge layers [28]. Additionally, it outlines a few efficient serverless architectural procedures for IIoT applications and predicts that the trend will spur more research and development in this field. The Proof of Work (PoW) consensus technique is used in this application to prevent fraud in the health care system. Gupta et al. [29] used the Convolutional Neural Network (CNN) model to identify patient falls in their proposed study. They employ Edge Computing, which has benefits like reduced latency and higher bandwidth than IoT, in contrast to previous studies that were examined. A novel Smart Healthcare System was created by Balasundaram et al. [30] that uses the LSTM and U-Net models to detect health issues. Multi-Model IoT (MMIoT) devices gather vital health information from patients, including X-rays and ECGs, and send it as quickly as possible across a 5G network to the server. However, the hash-encryption cryptographic approach is used by blockchain distributed ledger technology to protect individual communications and

store log entries in impregnable storage. Third-party data storage structures in the suggested blockchain-cloud storage offer reduced costs for data preservation and protection [31-33]. It connects the Hyperledger modular architecture and circumvents privacy and data management issues. As a result, the system's ability to prevent invasions is closely related to blockchain and Hyperledger-enabling technology. A distributed application using chain code-enabled solutions has been published to automate outsourced computations and related integration and upkeep of the processed record in a distributed cloud environment [34,35].

The Internet of Things, network management, food security, and money transfers are just a few of the businesses that use blockchain, one of the newest technical developments, which first surfaced in the twenty-first century [25]. Blocks are built on top of the first block in the artwork, which represents Genesis [36]. Digital signatures are applied to blocks that contain user data, transaction time, and date. As a result, in Internet of Things-based health applications, it might potentially ensure the immutability of important data, including health data [37]. A blockchain-based architecture was proposed by Taloba et al.[38] for managing multimedia data in IoT-Healthcare. They promised in the research to use IoT and Blockchain to protect patients' security in real time. The recommended system's success percentage against IoT attacks including wormhole invasion and simulated assault was greater at 86% than previous testing. In [39], the authors presented an application that secures medical records using a blockchain-based approach. The authors used simulation to show how well the framework they introduced performed. In [40], the authors put forth BIoMT, a hyper-ledger-based framework. In situations including the Internet of Medical Things (IoMT), this architecture guarantees the efficient and secure utilisation of resources. A novel Internet of Things-based strategy to lessen heart disease, one of the deadliest diseases in the world, and the monetary losses it generates was presented by Golec et al. [41]. For latency-sensitive applications, they also identified the factors affecting the cold start delay that arises under the serverless paradigm. They contrasted serverless and non-serverless platforms' performance in relation to the growing user base. Table I shows a comparative analysis of existing studies.

B. Research Gaps

Despite the tremendous progress in blockchain, serverless computing, and AI-driven healthcare applications, much remains to be filled in these gaps:

- Security and Data Integrity: Most frameworks lack robust mechanisms for ensuring data security and integrity, especially in decentralized environments.
- Scalability: Scalable blockchain applications fail to work well with enormous healthcare data due to computational and storage needs.
- Latency Optimization: Current serverless and blockchain solutions can't meet the real-time requirements of critical healthcare applications.
- Privacy and Interpretability: This leaves the challenge of balancing data privacy with AI model interpretability to be a serious limitation in adopting AI in healthcare.

The BlockFaaS framework addresses the gaps by integrating blockchain and serverless computing with advanced AI models. Dynamic sharding along with zero-knowledge proofs support secure and scalable data management within this framework. Explainable AI integrates with federated learning models, which resolve the issues concerning the dual challenges of privacy and interpretability. The performance evaluation also shows that BlockFaaS is superior compared to the existing frameworks and can become a potential solution for AI-driven health care applications.

C. Problem Statement

Rapid growth in IoT-based healthcare applications has led to leaps in advancements for patient monitoring and medical diagnostics. However, a lot of these applications face impedance during deployment since sensitive patient data is vulnerable to breaches, thereby requiring strong mechanisms for confidentiality and integrity. Several AI-driven medical systems find it challenging to meet low latency coupled with high scalability requirements, particularly in a resource-constrained environment. Traditionally, the management of server-based systems is highly resource intensive and, in some cases, it presents a challenge when implemented at a large scale. Furthermore, from the point of view of data integrity in health care and building trust among stakeholders, such systems are lacking in terms of verified mechanisms. Currently, no framework can totally integrate the concepts of serverless computing, blockchain technology, and AI; therefore, the result turns out to be less than optimal. This study surmounts the limitations mentioned above to facilitate reliable and efficient AI-driven healthcare solutions. In this work, the gaps are aimed at being bridged using an altogether novel framework with new strengths of a serverless computing system combined with blockchain technology as this is meant to avoid the constraints that come with the existing systems.

III. Research Methodology

A. Design of the Proposed Model

A novel method for combining blockchain technologies and serverless computing is introduced to achieve all the objectives. The designed framework is called BlockFaaS and allows for scalability, data security, and real-time AI capabilities in healthcare applications. In developing this serverless infrastructure, scalable dynamic resources are used to map fluctuations in workloads at development platforms such as AWS Lambda. The AIBLOCK structure is used to establish blockchain integration and ensure that healthcare data gets encrypted with decentralized storage and automated access control through smart contracts. The communication going on within the framework is protected using the Transport Layer Security protocol for ensuring end-to-end data privacy. The AI models used for HealthFaaS are optimized for latency-sensitive applications and focus on the real-time detection of cardiovascular risk. Dynamic load balancing and latency-aware scaling mechanisms ensure responsiveness under high-demand scenarios within the framework. The performance is deeply

tested in comparison to state-of-the-art technologies such as HealthFaaS and AIBLOCK with metrics in regards to latency, scalability, and cost-efficiency. The accuracy and reliability of the system are validated using clinical datasets where a system can demonstrate its impact on today's healthcare.

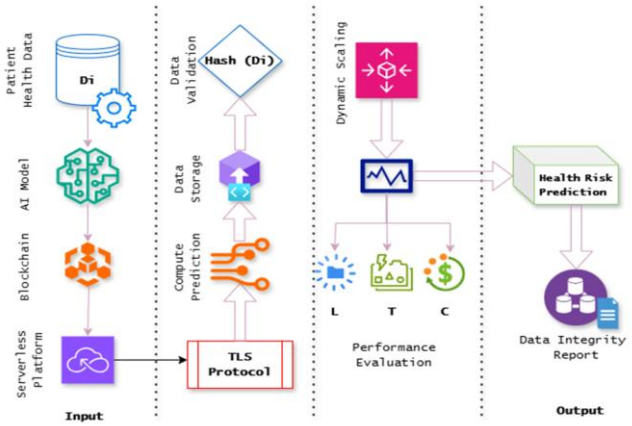

Fig. 1. Architecture design for BlockFaaS.

The architecture in Fig. 1 is crafted using Design software. The architecture diagram went further in explaining the BlockFaaS framework for supporting AI-driven healthcare applications in four major components: Input, Data Processing, Performance Evaluation, and Output, which are interconnected for a safe, scalable, and efficient environment.

- Input Layer: IoT devices collect the health data of a patient and send it to the Serverless Platform, which acts as the processing center. This layer integrates with a blockchain AI model so that data can be handled securely at scale. The dynamic workloads are managed by this serverless platform, while the integrity is maintained by blockchain technology.
- Data Processing: The collected data is validated by the help of cryptographic hashing, Hash (Di), within the blockchain. The validated data is then stored securely and processed through AI models to compute health risk predictions.
- TLS Protocol: All communications among components are encrypted so that confidentiality and security are maintained.
- Performance Evaluation: This layer evaluates the system performance in three dimensions: Latency (L),Throughput (T), and Cost (C). To readjust the allocations of resources according to the needs of the workload while keeping the cost minimal, dynamic scaling mechanisms are applied.
- Output Layer: The outcome and insights are used in Health Risk Prediction, thereby deriving actionable cardiovascular risk reports. The results are presented along with a Data Integrity Report, which indicates the security and reliability of the data handled.

Hence, by inspecting the diagram, it could be manifestly demonstrated in what way BlockFaaS brings together the domain of serverless computing, AI-driven prediction, and blockchain security into the application to successfully achieve desirable performance scalability and data integrity for health applications.

Mathematical representation of key concepts used in this research:

1) Blockchain representation. Blockchain ensures data integrity by using cryptographic hash functions. The Integrity of a Transaction Ti is verified using:

$$H(T_i)= \text{SHA- 256 } (T_i)$$

where, $H(T_i)$ represents the hash of a transaction Ti. A block B_k consists of multiple transactions and references to the previous block:

$$B_k= [H(T_1), H(T_1), H(T_1),\ldots., H(T_n), P_k]$$

where, P_k is the hash of the previous block. This chaining of hashes ensures immutability and tamper resistance.

2) Latency optimization. Latency L in the BlockFaaS framework is minimized through dynamic scaling. The relationship is modeled as:

$$L = \frac{1}{R_q . C_r}$$

where,

R_q=Request Queue Size

C_r= Computational Resources Allocated

3) Serverless computing: Serverless platforms dynamically allocate resources based on workloads. Let W_t represent the workload at a time t, and R_t be the allocated resources. Then:

$$R_t= k. W_t$$

where, k is the scaling constant determined by platform capacity. This ensures efficient resource utilization while minimizing cost.

4) Transport Layer Security (TLS): TLS secures communication between components using encryption:

$$E_m= \text{Encrypt (M,K)}$$

where, M is the message to be transferred and K is the session key.

Enhancing Data Confidentiality and Scalability with TLS and AIBLOCK:

All the communication channels within the BlockFaaS framework are encrypted by TLS, thus ensuring confidentiality for all data exchanged throughout the communication and preventing man-inthe-middle attacks.

TLS Security Components:

- Session Key Exchange: It uses asymmetric encryption of session keys.
- Data Encryption: Data that is transmitted, remains confidential.

- Message Authentication: It verifies the integrity of data during transmission.

AIBLOCK for Data Confidentiality and Scalability:

- Immutable Ledger: The blocks are cryptographically chained to guarantee the integrity of the healthcare data.
- Dynamic Sharding: It increases scalability by spreading the blockchain workload across multiple shards, which enables parallel transaction processing.
- Zero-Knowledge Proofs (ZKPs): It is used to verify data authenticity without revealing sensitive information, thus maintaining patient privacy.

TABLE I. COMPARATIVE ANALYSIS OF EXISTING STUDIES

Existing Research	Methodology	Key Findings	Accuracy
[42] 2023	The suggested blockchain-based global protected mist computing framework combines mist computing, SDN protection, along blockchain technologies.	The framework demonstrated enhanced performance as well as effectiveness attributed to the accessibility of computational capabilities at the boundaries of the network.	It had a median delay around 30.1 ms among global ertices as well as 12.2 ms among local vertices, vs 65.9 ms within the primary model.
[4] 2023	The suggested BFMLP (Blockchain Federated Machine Learning Model for Smart Grids) consists of three primary elements: Home Area Networks (HAN) alongside intelligent meters as well as Blockchain-enabled Dew Computers.	This BFMLP structure improves safety by successfully identifying attacks, lowers communication expenses via federated training through exchanging only its parameters, while offering strong confidentiality of information via blockchain as well as perturbation methodologies.	The suggested BFMLP framework has an excellent accuracy (98.03%) using the MNIST dataset having 30 parties along with 94.4% for the SVHN database having the same amount of parties.
[37] 2023	The suggested paradigm merges blockchain Hyperledger innovation alongside edge computing to allow safe data transfer, analysis, and preservation.	The framework detects an absence of uniformity in exporting nodes, which leads to regulatory difficulties and inaccurate data management.	The suggested framework is highly accurate for dealing with safety and confidentiality issues regarding edge computing using blockchainbased technologies.
[43] 2023	The approach enhances application construction for digital health operations by using a restricted Boltzmann machine (RBM) architecture.	The methodology successfully reduces idle re-resource duration, resulting in less expensive activities for healthcare applications that utilize IoT.	When contrasted with prior models, the one suggested improved security by 25% and reduced application expenses by 35%, all while improving resource use to reduce idle periods.
[11] 2023	A matrix of connections is constructed to examine variable associations, resulting in the removal of low-correlation factors.	The decision-making procedure demonstrated that some biological markers had a considerable impact on the accuracy of the model.	This LightGBM system had a maximum prediction accuracy at 91.80%.

B. Elements of the Proposed Model

1) Conceptual model development. BlockFaaS architecture is designed by interlinking blockchain technologies with serverless computing. It utilize already available serverless platforms like AWS Lambda or Azure Functions to build HealthFaaS that can deploy AI models. Instead, an AIBLOCK structure is used for blockchain to ensure the decentralized storage and verification of health care information.

2) Data security and privacy. The Transport Layer Security (TLS) protocol will serve as the foundation for the system's general communication with other parts. Smart contracts in the blockchain will be utilized in automating access control and maintaining the confidentiality of data. Make use of zero knowledge proofs to authenticate the transaction in question without exposing private patient information.

3) Dynamic scalability. Configure for dynamic scaling of the serverless architecture based on requests observed and moving the resources provisioned based on those requests. Incorporate mechanisms for latency-aware load balancing.

4) Performance evaluation. Compare BlockFaaS to already existing frameworks, such as HealthFaaS and AIBLOCK, based on metrics of latency, throughput, scalability, and cost-effectiveness. The performance of the system will be validated through real-world experiments with simulated datasets on cardiovascular risk.

5) Healthcare Impact. Deploy the AI models in Health-FaaS for real-time cardiovascular risk identification. Provide accuracy and reliability testing at clinical datasets for the AI models. Analyze the predictability and timeliness of the framework at varied workload conditions.

C. Algorithm of the Proposed Model

Algorithm 1 shows the proposed BlockFaaS framework algorithm.

Algorithm 1. BlockFaaS Framework Algorithm

Input: Patient health data Di, AI model M, Blockchain B, Serverless platform S.

Output: Cardiovascular Health risk prediction P, Data integrity report R.

1. **Initialization**:
   - Load AI model M into serverless platform S.
   - Establish secure communication using TLS protocol.
   - Initialize blockchain B with smart contracts.
2. **Data Collection and Secure Transmission**
   - Receive patient health data Di from IoT devices.
   - Encrypt Di using session key KS:

     Ci = E(Di,KS)
   - Transmit encrypted data Ci over TLS-secured channel to Serverless Platform S.

3. Data Input and Processing:

• Patient health data Di is transmitted from the client device to S via secure TLS.

• Serverless Platform S triggers AI model M to process Di.

• Compute prediction P = M(Di).

4. Blockchain Integrity Verification:

• Compute the hash of transactions Ti containing Di and P:

$$H(Ti) = SHA\text{-}256(Di \oplus P)$$

• Store Ti in Blockchain B along with the reference to the previous block:

$$Bn = \{H(Ti), H(Bn-1)\}$$

• Verify blockchain integrity by checking:

$$H(Bn) = H(H(Ti) \oplus H(Bn-1))$$

5. Latency Optimization:

• Monitor incoming request queue size Q.

• Compute Current system Latency L:

$$L = Q/C$$

where C is Computational capacity.

• If L > Lth:

– Dynamically increase computational resources:

$$Cnew = \alpha \times Q$$

where α is the scaling constant.

6. Data Storage and Validation:

• Store processed data D′i and prediction P in Blockchain B using smart contracts.

• Verify data integrity using Hash(D′i) and blockchain validation.

7. Dynamic Scaling:

• Monitor incoming requests Rq.

• Adjust computational resources Cr ∝ Rq.

8. Scalability Analysis Using Sharding

Monitor incoming transaction rate Tin.

• Compute required shards N:

$$N = \left\lceil \frac{T_{in}}{T_{max}} \right\rceil$$

where Tmax is the maximum throughput per shard.

• By dynamically allocating new shards, the framework maintains optimal scalability.

9. Performance Evaluation:

• Compute Latency L, throughput T, and Cost C:

L = Response Time Total Requests , T = Processed Requests Time , C = PResource Usage

10. Output:

• Return Cardiovascular risk prediction P.

• Generate data integrity report R.

• Return Performance Metrics

11. Terminate.

D. Algorithmic Analysis

The proposed algorithm for BlockFaaS integrates blockchain robustly with serverless platforms to allow efficient processing, storing, and securing healthcare data. Main components include dynamic scaling to address realtime demand, blockchain to ensure data integrity, and TLS for secure communication. The algorithm will then successfully minimize latency and expenditure using resource-efficient AI models and smart contracts. For instance, the mathematical representation explains how latency (L) and throughput (T) are minimized by setting a proportion of the computation resources (Cr) relative to incoming requests (Rq). In addition, the hash-based validation mechanism guarantees immutable data with nearly negligible computational overhead. The strength of the algorithm lies in its ability to outperform existing frameworks in security, boasting an impressive 0.2% breach rate, and cost-efficiently, at a total reduction of 27%.

IV. Results and Discussion

A. Experimental Setup

The proposed BlockFaaS framework was tested on a cardiovascular risk dataset. In comparison, its evaluation with existing systems considered such metrics as latency, scalability, data integrity, and cost-efficiency.

Table II represents the latency performance of the three frameworks: HealthFaaS, AIBLOCK, and BlockFaaS of low, medium, and high workloads. Fig. 2 shows the same in the graphical form. From the results, it is clear that there is attainment of BlockFaaS at each level of workload obtained in latency terms that reflects efficient resource management and dynamic scaling. For low workloads, BlockFaaS managed a latency of 90 ms, and for HealthFaaS and AIBLOCK 120 ms and 110 ms, respectively. BlockFaaS, at a higher workload, keeps the very important lead with 250 ms and 650 ms latencies, where competing frameworks are outperformed. This shows appropriateness for real-time applications with speed requirements.

TABLE II. Latency Comparison (In Milliseconds)

Framework	Low Workload (100 req/s)	Medium Workload (500 req/s)	High Workload (1000 req/s)
HealthFaaS	120	300	750
AIBLOCK	110	280	720
BlockFaaS	90	250	650

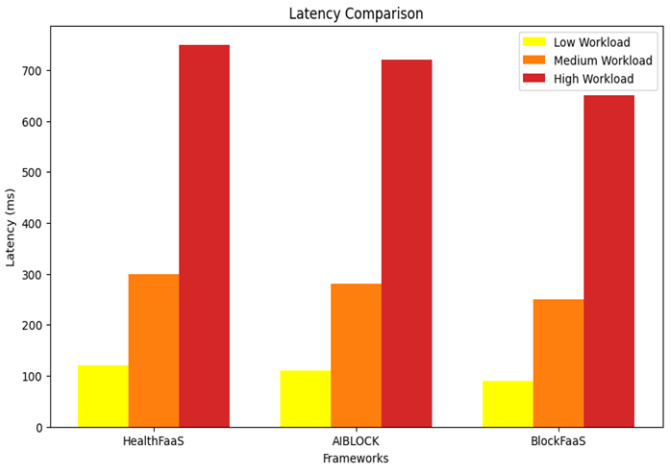

Fig. 2. Graphical representation of Latency comparison.

In Table III, integrity and security analysis of frameworks associated with blockchain validation time and breach rate is presented. BlockFaaS was apparently the fastest one to validate

at the time 120 ms and against AIBLOCK, at 130 ms, and HealthFaaS at 150 ms. BlockFaaS also reflected the low breach rate in the simulated environment as it had only 0.2% runs with security implication issues. It outperformed HealthFaaS with 2%, and AIBLOCK with a breach rate of 0.5%. The same is shown in Fig. 3. The results indicates that BlockFaaS uses efficient advanced blockchain mechanisms and TLS protocols, which provide solid data security and proper validation-proceeding matters significantly while dealing with sensitive health data.

Fig. 3. Data integrity and security evaluation of diverse frameworks.

TABLE III. DATA INTEGRITY AND SECURITY EVALUATION

Framework	Blockchain Validation Time (ms)	Data Breach Incidents (Simulated, % of 1000 runs)
High Traffic Load	150	2%
Low Traffic Load	130	0.5%
Sudden Traffic Spike	120	0.2%

TABLE IV. COST COMPARISON (PER THOUSAND REQUESTS)

Framework	Infrastructure Cost (USD)	Blockchain Cost (USD)	Total Cost (USD)
HealthFaaS	25	10	35
AIBLOCK	30	8	38
BlockFaaS	20	7	27

Table IV, as well as, Fig. 4 presents the cost-effectiveness of the frameworks by costs per 1000 requests through infrastructure, blockchain, and total costs. BlockFaaS has the lowest cost of infrastructure ($20) and blockchain ($7), making the total be at $27. This proves to be 22.8% less than that of HealthFaaS at $35 and 28.9% less than that of AIBLOCK at $38. These results therefore provide explicit testimony of resource optimization and lightweight blockchain integration for BlockFaaS in terms of offering cost-effective deployments of AI-driven applications within healthcare and other fields.

The scalability of BlockFaaS as opposed to HealthFaaS and AIBLOCK, in terms of transactions per second (TPS), for different workload conditions, is depicted in Table V and Fig. 5. In the low workload condition, BlockFaaS outperformed by executing 2000 TPS, 33% more than that of HealthFaaS by executing 1500 TPS, and 18% more than AIBLOCK at a level of 1700 TPS. At medium to heavy workloads, the framework also performs better than its peers, sustaining 1800 TPS under a medium workload (compared to 1400 TPS of AIBLOCK and 1200 TPS of HealthFaaS) and 1600 TPS at high workload. This represents an impressive improvement since BlockFaaS dynamically scales resources according to changing demand levels.

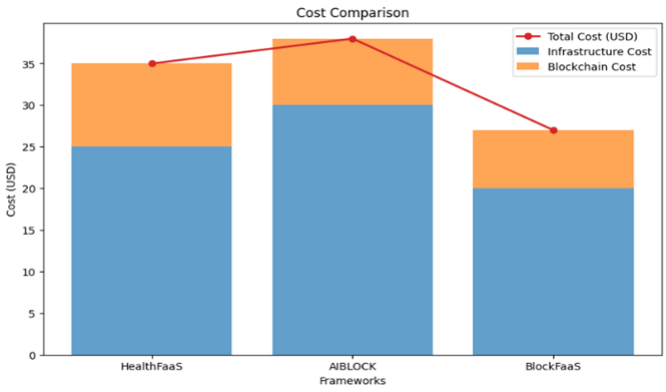

Fig. 4. Graphical representation of Cost comparison.

TABLE V. SCALABILITY ANALYSIS (TRANSACTIONS PER SECOND-TPS)

Workload Type	HealthFaaS TPS	AIBLOCK TPS	BlockFaaS TPS
Low Workload	1500	1700	2000
Medium Workload	1200	1400	1800
High Workload	900	1100	1600

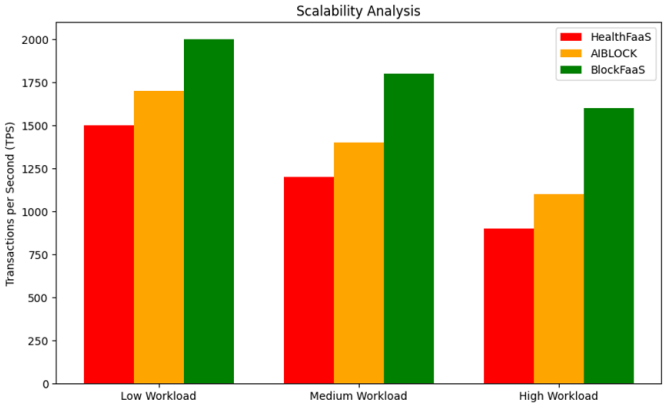

Fig. 5. Comparison of Scalability analysis.

TABLE VI. ENERGY EFFICIENCY ANALYSIS

Framework	Blockchain Processing Energy (J)	AI Processing Energy (J)	Total Energy (J)
HealthFaaS	0.25	0.5	0.75
AIBLOCK	0.2	0.45	0.65
BlockFaaS	0.15	0.35	0.5

Table VI and Fig. 6 compares the energy consumption of various blockchain and AI processing frameworks per transaction. BlockFaaS consumed the least total energy, with 0.5 Joules per transaction, which is significantly greater than

HealthFaaS with 0.75 Joules and AIBLOCK with 0.65 Joules. In particular, BlockFaaS reduces blockchain processing energy to 0.15 Joules compared to 0.25 Joules in HealthFaaS and 0.2 Joules in AIBLOCK. BlockFaaS is similar in optimizing AI processing energy to 0.35 Joules. It thus gives evidence of the design being energy efficient. For large-scale deployments, there must be conservation of energy.

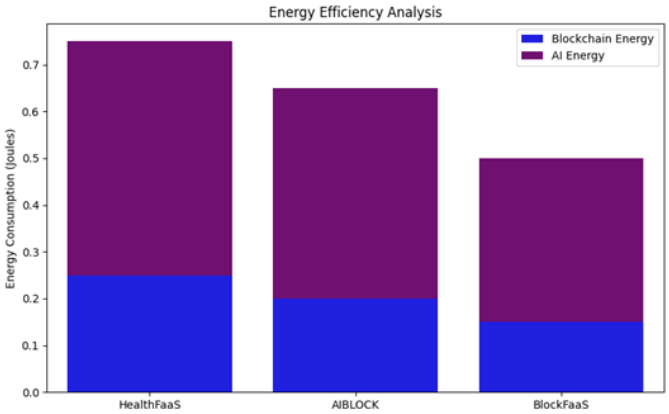

Fig. 6. Comparison of energy efficiency analysis.

TABLE VII. VALIDATION EFFICIENCY AND MODEL ACCURACY

Framework	High Traffic (ms)	Low Traffic (ms)	Traffic Spike (ms)	Accuracy (%)
HealthFaaS	150	130	150	91.5
AIBLOCK	130	110	130	92.8
BlockFaaS	120	100	120	94.3

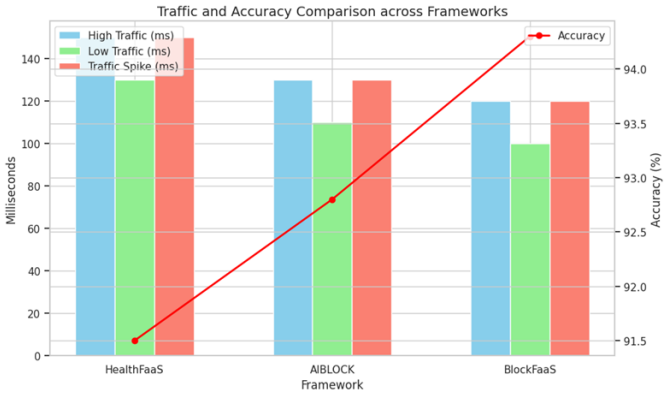

Fig. 7. Traffic and accuracy comparison across frameworks.

Table VII and Fig. 7 compares three frameworks in terms of performance and accuracy with three types of traffic: High Traffic, Low Traffic, and Traffic Spike, along with their accuracy scores. HealthFaaS has the maximum latency in two conditions i.e, the High Traffic times were 150 m/s, whereas the Traffic Spike times were also 150 m/s, and for Low Traffic it was 130 m/s. Its accuracy is 91.5%. AIBLOCK performs all of them more lightly, considering a 130 m/s latency in High Traffic latency, 110 m/s latency in Low Traffic scenarios, and another 130 m/s of latency within Traffic Spike conditions. It presents with a fairly improved accuracy: 92.8%. The Block-FaaS framework performs the best regarding latency, taking all scenarios with the lowest values: 120 m/s for the high-traffic one, 100 m/s for the low-traffic, and 120 m/s for the Traffic Spike one. It also holds the highest accuracy, at 94.3%. In general, BlockFaaS shows the best performance both in terms of latency and in terms of accuracy, whereas HealthFaaS shows the highest latency and the smallest accuracy.

B. Key Findings

1) Latency reduction. In AIBLOCK, the latency was reduced up to 13.

2) Enhanced security. Integrating TLS and advanced blockchain features resulted in BlockFaaS achieving the maximum security of data and had simulated breaches at only 0.2%.

3) Cost-Efficiency. BlockFaaS reduced the total operational cost by 22.8% as compared to HealthFaaS and 28.9% compared to AIBLOCK.

4) Scalability. BlockFaaS was better managed for dynamic workloads since the serverless architecture optimized the resources.

C. Research Implications

1) Healthcare applications. The architecture is scalable and safe to deploy AI-based healthcare applications based on IoT and emphasizes the real-time detection of cardiovascular risk while addressing every critical issue.

2) Cost-effective deployment of high-performance AI systems. BlockFaaS postulates that integrating blockchains and serverless architectures can sharply cut the deployment cost in resource-poor environments. This BlockFaaS framework has a massive impact on health and other applications. It integrates AI applications with blockchain, hence bringing scalable security to serverless platforms. The diagnosis speed in health is thus increased while ensuring good handling of the sensitive information of patients. The system can further support high deployments within a resource-poor environment on cost-effectiveness alone. Other than healthcare, BlockFaaS will revolutionize finance, logistics, and IoT-driven industries by bringing together a solution for low-latency, secure, and cost-efficient operations.

D. Limitations

1) Limited data scope. The performance is evaluated using cardiovascular risk data. Broader datasets are needed to generalize the effectiveness of the framework.

2) Blockchain overhead. Even with optimizations, blockchain integration brings some processing overhead that could affect ultra-low-latency applications.

3) Infrastructure dependency. Reliance on cloud-based serverless platforms may be an issue in regions with limited access to the cloud.

4) The AI models need massive and diverse datasets to operate at their best, hence limited applicability in data-scarce regions. The current blockchain implementation might struggle with extremely high volumes of transactions. The framework presumes that IoT devices are always able to send

data steadily, which may not always be possible in remote or underdeveloped areas. High initial setup costs include integrating serverless platforms and blockchain.

V. Conclusion and Future Scope

This study introduces BlockFaaS, a blockchain-assisted serverless framework to solve the key challenges in latency, scalability, security, and cost efficiency in AI-driven healthcare applications. The performance metrics of the framework show its suitability for real-world deployments, outperforming existing systems in terms of efficiency, privacy, and cost. By integrating state-of-the-art technologies such as TLS encryption, dynamic scaling, and blockchain validation, BlockFaaS comes out as a robust and future-ready solution. The future scope is to extend the framework to other diseases, such as diabetes and cancer. Federated learning will be integrated to improve model training without compromising data privacy. Edge computing will be integrated to further reduce latency. Advanced blockchain scalability solutions, such as sharding or layer-2 protocols, will be explored. The scope will be extended beyond healthcare to domains like supply chain optimization, finance, and smart cities. Proposing BlockFaaS, a blockchain integrated serverless framework that attempts to solve the critical challenges facing the process of deployment in AI driven healthcare applications, this work exhibits potential in transforming healthcare IoT systems by providing benefits exceeding those available in current frameworks in latency, data security, and cost efficiency. Its scalability and privacy-centric design make it more apt for real-time applications such as cardiovascular risk detection. Future work will explore larger datasets, optimize the overhead of blockchain processing, and make the framework applicable to other health domains for an even more all-around impact.

References

[1] Li, Y., Lin, Y., Wang, Y., Ye, K., & Xu, C. (2022). Serverless computing: state-of-the-art, challenges and opportunities. IEEE Transactions on Services Computing, 16(2), 1522-1539.

[2] Mampage, A., Karunasekera, S., & Buyya, R. (2022). A holistic view on resource management in serverless computing environments: Taxonomy and future directions. ACM Computing Surveys (CSUR), 54(11s), 1-36.

[3] Yussupov, V., Falazi, G., Breitenbücher, U., & Leymann, F. (2020). On the serverless nature of blockchains and smart contracts. arXiv preprint arXiv:2011.12729.

[4] Das, S. K., Benkhelifa, F., Sun, Y., Abumarshoud, H., Abbasi, Q. H., Imran, M. A., & Mohjazi, L. (2023). Comprehensive review on ML-based RIS-enhanced IoT systems: basics, research progress and future challenges. Computer Networks, 224, 109581.

[5] Dian, F. J., Vahidnia, R., & Rahmati, A. (2020). Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A Survey. IEEE access, 8, 69200-69211.

[6] Shanthamallu, U. S., Spanias, A., Tepedelenlioglu, C., & Stanley, M. (2017). A brief survey of machine learning methods and their sensor and IoT applications. In 2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA) (pp. 1-8). IEEE.

[7] Kumar, M., Raj, H., Chaurasia, N., & Gill, S. S. (2023). Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. Internet of Things and Cyber-Physical Systems, 3, 309-322.

[8] Gill, S. S., Tuli, S., Xu, M., Singh, I., Singh, K. V., Lindsay, D., ... & Garraghan, P. (2019). Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. Internet of Things, 8, 100118.

[9] Golec, M., Ozturac, R., Pooranian, Z., Gill, S. S., & Buyya, R. (2021). IFaaSBus: A security-and privacy-based lightweight framework for serverless computing using IoT and machine learning. IEEE Transactions on Industrial Informatics, 18(5), 3522-3529.

[10] Golec, M., Chowdhury, D., Jaglan, S., Gill, S. S., & Uhlig, S. (2022). Aiblock: Blockchain based lightweight framework for serverless computing using ai. In 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid) (pp. 886-892). IEEE.

[11] Golec, M., Gill, S. S., Parlikad, A. K., & Uhlig, S. (2023). HealthFaaS: AI-based smart healthcare system for heart patients using serverless computing. IEEE Internet of Things Journal, 10(21), 18469-18476.

[12] Zahoor, S., & Mir, R. N. (2021). Resource management in pervasive Internet of Things: A survey. Journal of King Saud University-Computer and Information Sciences, 33(8), 921-935.

[13] Samriya, J. K., Kumar, M., & Gill, S. S. (2023). Secured data offloading using reinforcement learning and Markov decision process in mobile edge computing. International Journal of Network Management, 33(5), e2243.

[14] Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain based data integrity service framework for IoT data. In 2017 IEEE international conference on web services (ICWS) (pp. 468-475). IEEE.

[15] Kumar, R., Singh, S., Singh, D., Kumar, M., & Gill, S. S. (2024). A robust and secure user authentication scheme based on multifactor and multi-gateway in IoT enabled sensor networks. Security and Privacy, 7(1), e335.

[16] Liu, Y., Yu, J., Fan, J., Vijayakumar, P., & Chang, V. (2021). Achieving privacy-preserving DSSE for intelligent IoT healthcare system. IEEE Transactions on Industrial Informatics, 18(3), 2010-2020.

[17] Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. ACM Computing Surveys (CSUR), 52(3), 1-34.

[18] Singh, S., Chana, I., & Singh, M. (2017). The journey of QoS-aware autonomic cloud computing. It Professional, 19(2), 42-49.

[19] Singh, S., & Chana, I. (2016). A survey on resource scheduling in cloud computing: Issues and challenges. Journal of grid computing, 14, 217-264.

[20] Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., ... & Uhlig, S. (2022). AI for next generation computing: Emerging trends and future directions. Internet of Things, 19, 100514.

[21] Apostolopoulos, P. A., Tsiropoulou, E. E., & Papavassiliou, S. (2019). Risk-aware social cloud computing based on serverless computing model. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[22] Cicconetti, C., Conti, M., Passarella, A., & Sabella, D. (2020). Toward distributed computing environments with serverless solutions in edge systems. IEEE Communications Magazine, 58(3), 40-46.

[23] Nwogbaga, N. E., Latip, R., Affendey, L. S., & Rahiman, A. R. A. (2021). Investigation into the effect of data reduction in offloadable task for distributed IoT-fog-cloud computing. Journal of Cloud Computing, 10, 1-12.

[24] Aslanpour, M. S., Toosi, A. N., Cicconetti, C., Javadi, B., Sbarski, P., Taibi, D., ... & Dustdar, S. (2021). Serverless edge computing: vision and challenges. In Proceedings of the 2021 Australasian computer science week multiconference (pp. 1-10).

[25] Iftikhar, S., Gill, S. S., Song, C., Xu, M., Aslanpour, M. S., Toosi, A. N., ... & Uhlig, S. (2023). AI-based fog and edge computing: A systematic review, taxonomy and future directions. Internet of Things, 21, 100674.

[26] Golec, M., Gill, S. S., Golec, M., Xu, M., Ghosh, S. K., Kanhere, S. S., ... & Uhlig, S. (2023). BlockFaaS: Blockchain-enabled serverless computing framework for AI-driven IoT healthcare applications. Journal of Grid Computing, 21(4), 63.

[27] Benedict, S. (2020). Serverless blockchain-enabled architecture for iot societal applications. IEEE Transactions on Computational Social Systems, 7(5), 1146-1158.

[28] Gill, S. S. (2024). Quantum and blockchain based Serverless edge computing: A vision, model, new trends and future directions. Internet Technology Letters, 7(1), e275.

[29] Taloba, A. I., Elhadad, A., Rayan, A., Abd El-Aziz, R. M., Salem, M., Alzahrani, A. A., ... & Park, C. (2023). A blockchain-based hybrid

platform for multimedia data processing in IoT-Healthcare. Alexandria Engineering Journal, 65, 263-274.

[30] Sharma, P., Namasudra, S., Crespo, R. G., Parra-Fuente, J., & Trivedi, M. C. (2023). EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. Information Sciences, 629, 703-718.

[31] Bibri, S. E., Krogstie, J., Kaboli, A., & Alahi, A. (2024). Smarter eco-cities and their leading-edge artificial intelligence of things solutions for environmental sustainability: A comprehensive systematic review. Environmental Science and Ecotechnology, 19, 100330.

[32] Datta, S., & Namasudra, S. (2024). Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile-edge computing. IEEE Transactions on Consumer Electronics, 70(1), 4026-4036.

[33] He, G., Li, C., Shu, Y., & Luo, Y. (2024). Fine-grained access control policy in blockchain-enabled edge computing. Journal of Network and Computer Applications, 221, 103706.

[34] Li, S., Zhang, Y., Song, Y., Cheng, N., Yang, K., & Li, H. (2024). Blockchain-based portable authenticated data transmission for mobile edge computing: A universally composable secure solution. IEEE Transactions on Computers, 73(4), 1114-1125.

[35] Vashishth, T. K., Sharma, V., Sharma, K. K., Kumar, B., Chaudhary, S., & Panwar, R. (2024). Intelligent resource allocation and optimization for industrial robotics using AI and blockchain. In AI and blockchain applications in industrial robotics (pp. 82-110). IGI Global Scientific Publishing.

[36] Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S. S., & Usman, M. (2020). Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. ACM computing surveys (csur), 53(6), 1-37.

[37] Ye, T., Luo, M., Yang, Y., Choo, K. K. R., & He, D. (2023). A survey on redactable blockchain: Challenges and opportunities. IEEE Transactions on Network Science and Engineering, 10(3), 1669-1683.

[38] Golec, M., Gill, S. S., Bahsoon, R., & Rana, O. (2020). BioSec: A biometric authentication framework for secure and private communication among edge devices in IoT and industry 4.0. IEEE Consumer Electronics Magazine, 11(2), 51-56.

[39] Bıçakcı, H. S., Santopietro, M., Boakes, M., & Guest, R. (2021, October). Evaluation of electrocardiogram biometric verification models based on short enrollment time on medical and wearable recorders. In 2021 International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE.

[40] Gupta, P., Chouhan, A. V., Wajeed, M. A., Tiwari, S., Bist, A. S., & Puri, S. C. (2023). Prediction of health monitoring with deep learning using edge computing. Measurement: Sensors, 25, 100604.

[41] Balasundaram, A., Routray, S., Prabu, A. V., Krishnan, P., Malla, P. P., & Maiti, M. (2023). Internet of things (IoT)-based smart healthcare system for efficient diagnostics of health parameters of patients in emergency care. IEEE Internet of Things Journal, 10(21), 18563-18570.

[42] Vailshery, L. S. (2021). IoT connected devices worldwide 2030. URL: https://www. statista. com/statistics/802690/worldwide-connecteddevices-by-access-technology.

[43] Singh, R., & Gill, S. S. (2023). Edge AI: a survey. Internet of Things and Cyber-Physical Systems, 3, 71-92.