RESEARCH PAPER

ImmutableShield: A Fragmentation-Driven Security Algorithm for Real-Time Health Data Protection in IoT-Enabled Heat-Stroke Scenarios

Mohamad Emad Bitar [1], Dr. V Sujatha [2]

[1]Ph.D. Scholar, Department of Computer Science, Bharathiar University, CMS College of Science & Commerce, Coimbatore, India - 641035.
Email: t22h.12345@gmail.com
ORCID: 0009-0009-3212-2268

[2]Vice Principal, CMS College of Science and Commerce, Coimbatore, India – 641035.
Email: sujatha.padmakumar4@gmail.com

Abstract:
The fast technological advancements in healthcare systems powered by IoT have been able to continuously monitor patients but at the same time have caused important issues regarding data privacy, integrity, and compliance. The present article focuses on the security of data management in heat-stroke prediction and monitoring, in which a massive amount of physiological and environmental data is produced by the use of wearables and IoT gadgets. The ImmutableShield Security Algorithm (ISSA) is the proposed method that combines horizontal and vertical data fragmentation, AES-256 adaptive encryption, and blockchain-based immutability to provide confidentiality, traceability, and fault tolerance in distributed healthcare networks. The experimental evaluations with the use of the Kaggle Heat Stroke Dataset reveal that ISSA results in a fragmentation efficiency of 90% ± 1.2, encryption overhead of 8% ± 0.5, and a data confidentiality score of 9.0 ± 0.2 (on a 10-point scale derived from entropy-based privacy metrics). ISSA surpasses the current frameworks (IoT-Fog Heatstroke Framework (IFHF), Adaptive Federated Edge Learning Framework (AFEL), Blockchain-Enhanced Healthcare Framework (BEHF)) in terms of access control accuracy which is defined as the relative increase in correct authorization decisions by 15%. The framework also incorporates audit logging, key rotation, and consent-aware access control which are in line with Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) principles. To sum up, ISSA places on the table a solid and compliant base for secure, real-time, and scalable heat-stroke healthcare data management.

Index Terms: Adaptive Encryption, Blockchain, Data Fragmentation, Healthcare Data Security, Internet of Things, Privacy Compliance, Real-time Monitoring.

How to cite this article: Bitar ME, Sujatha V. ImmutableShield: a fragmentation-driven security algorithm for real-time health data protection in IoT-enabled heat-stroke scenarios. Int J Drug Deliv Technol. 2026;16(7s): 166-182; DOI: 10.25258/ijddt.16.7s.20

1. Introduction

Internet of Things (IoT) and health care have resulted in opportunities of immediate patient management, proactive diagnostics of disease and emergency management. Much of the modern smart health systems consists of automatic gathering and handling large volumes of physiological and environmental data that is uploaded continuously to analysis structures to provide decision support. Regrettably, the medical data is sensitive in nature that raises serious concerns on the way it is handled in distributed settings and taking into account security, privacy as well as regulatory compliance.

Existing works dug into various frameworks to strengthen the security in IoT healthcare. Qureshi et al. [1] put forward a dynamically adaptive security mechanism for the health care environments integrated with the metaverse, and this mechanism emphasized on access control that is adaptable. Alshuhail et al. [2] constructed a machine edge-conscious IoT framework for the swift health monitoring which uses sensor fusion and AI-led emergency response. Almalawi et al. [3] dealt with the issue of healthcare data security management through cutting-edge encryption and authentication technologies. Although these developments are important, still many studies are not incorporating powerful data fragmentation and tamper-proof traceability which cause the risk of data being exposed and getting unauthorized access.

In healthcare related to heat, [4], [5] proposed the use of IoT-based wearables for detecting heat-stroke, while, on the other hand, [6], [7] were able to enhance predictive health monitoring using models based on AI and machine learning. [8] took advantage of weather data

and machine learning and developed a system that will alert the user about the risk of heat-stroke 12 hours in advance, and [9] pointed out the importance of health systems in coping with the consequences of climate change regarding extreme heat events. Although these studies are a great contribution, they are mainly concerned with prediction and detection, leaving out such issues as secure data transmission, storage, or compliance.

Besides, the integration of cloud, fog, and edge computing paradigms has not only improved the data processing efficiency but also increased the possibility of attacks, therefore it is necessary to have distributed frameworks that are secure and scalable [10], [11]. In situations where heat-stroke is monitored, even a slight security incident can lead to the loss of patient privacy and an emergency response delay, hence handling of data that is secure, compliant, and audited is a must.

So as to fill these gaps, the current research presents the ImmutableShield Security Algorithm (ISSA) which is a blockchain-assisted framework of horizontal and vertical data fragmentation combined with AES-256 adaptive encryption. Data confidentiality, integrity, and fault tolerance are assured by ISSA which is composed of cryptographically linked fragments and immutable ledger verification. The framework is also compliant with HIPAA and GDPR principles by the implementation of consent-aware access control and time-limited authentication.

This publication's leading contributions include:

- Design of a blockchain framework based on fragmentation for the safe and secure management of heat-stroke healthcare data.
- Proposition of advanced encryption and hash-based auditing as a means to enhance both confidentiality and traceability.
- A thorough performance evaluation and ablation study that prove efficiency and security of the proposed method over baseline models.
- Provision of regulatory alignment mechanisms that assist with complying with both Accountability Act (HIPAA) and General Data Protection Regulation (GDPR)in the context of healthcare IoT.

The structure of this paper continues as follows: The background research and related works are presented in Section 2; the proposed ISSA methodology is explained in Section 3; the experimental setup and resultsare described in Section 4; the paper is concluded with future research directions in Section 5.

2. Literature Review

Healthcare data security has made significant strides recently, experimenting with different technological approaches to ensure privacy and reliability. These include IoT, blockchain, machine learning, and federated learning. The present section offers a review of the most important studies conducted from 2020 to 2025 by examining their concepts, methodologies, results and limitations to pinpoint existing gaps in the areas of real-time, compliant, and fragmentation-based healthcare data protection, which the proposed ISSA framework intends to tackle.

2.1 IoT and Fog Computing in Healthcare Monitoring

Anjum et al. (2025) [12] introduced an Opportunistic Access Control Scheme (OACS) that strengthens security in healthcare systems enabled by IoT, which operate with the help of blockchain-based transparency, and provide machine-learning driven adaptive authority. In their methodology a behavioural machine learning model is used to predict legitimacy of access, and a decentralized ledger of blockchain to catalogue and validate events of access. Their experimental analysis shows that there is a 15-20% higher accuracy regarding access and lower latency of access than in classical role-based methods. This approach was however limited to static process (in healthcare) and did not confer real-time access in emergency sensitive situations – where the ISSA (proposed herein) answers addressable issues by fragmentation-based encoding and time-sensitive access validation.

Moretti and Tanaka (2025) [13] suggested a blockchain-enabled Internet of Medical Things (IoMT) framework for the secure handling of heterogeneous medical data in distributed healthcare environments. Their approach utilized smart contracts to permit automated data identification and validation and distributed ledger storage to maintain the integrity of the heterogeneous medical records, such as images, sensor data and clinical text. In their experimental evaluation, they found that their data management framework exhibited superior data traceability, with a 25% reduction in the distribution of unauthorized data inconsistencies compared to centralized storage of medical records. However, the framework devoted its major emphasis to the immutable validity of records and reliability of their exchange, having no consideration for adaptive encryptions and or real time access processing which would be essential in time critical healthcare decisions. The ISSA framework provides for these features in the addition of fragmentation-based systems for privacy and real time access to data so that rapid effective decisions in

emergencies such as in the case of heat-stroke monitoring can be implemented.

Sutradhar et al. (2024) [14] introduced a framework based on blockchain for the protection and privacy of medical data sharing in IoMT systems. The proposed method made use of lightweight encryption and hash-linked block chain verification for integrity and privacy during data transfer. It was shown that data transmission security was improved by 30% while the occurrence of data leakage was minimized. However, the work so far has dealt only with data transfer, and no attention has been paid to context-aware access control and fragmentation-based protection. These issues have been catered for in the proposed ISSA model.

2.2 Blockchain and Immutable Logging for Health Data Security

Alhazmi et al. (2022) [15] presented a framework for big data security that draws on fragmentation of data with the inclusion of block chain logging in order to promote confidentiality and integrity of the data in distributed environments. The scheme utilized both horizontal and vertical fragmentation to imply selective isolation of the data and the use of hashes on the block chain records to ensure tamper-proofed. The method utilized provided enhancement of the data confidentiality and the traceability as compared to the centralised old means of operation. Nevertheless, the scheme of these authors was only trailed on standard datasets non- specific to real time healthcare. The ISSA proposed scheme utilised fragmentation and immutable verification on health sensitive data involved with time sensitive aspects of monitoring necessary data for a heat-stroke episode.

Nabawy et al. (2020) [16] presented a mixed fragmentation framework for protecting big data in a multi-cloud environment. The approach used horizontal and vertical fragmentation of the data such that sensitive data ended up on different clouds and minimized the risk of exposure through a single point. Experimental validation of the framework showed improved confidentiality along with load balancing improvement compared with single cloud systems. The work suffers, however, from the limitation that the data considered was limited to generic enterprise data and there were no provisions for role-based access or real-time access. The ISSA framework extends this idea to healthcare IoT through the use of log data on the blockchain as a medium for securely transferring time sensitive medical data.

Castro-Medina et al. (2020) [17] presented a thorough review of dynamic fragmentation methods used in multimedia databases to improve data security and data retrieval efficiency. They examined adaptive horizontal and vertical fragmentation proposed methods, which re-arrange data based on the frequency of data usage and the use context. The results revealed reduced latency with the query processing and improved confidentiality of data across distributed storage. The objective was to show improvement in multimedia content but did not address the context of health-specific requirements and for real-time security. The ISSA proposed framework takes this up, with the added data feature of encryption and logging with the blockchain of fragmentation for real time health specific IoT data.

2.3 Fragmentation and Secure Data Management Approaches

Farahani and Monsefi (2023) [18] have described a framework utilizing federated learning and data space for increasing security and collaboration in industrial IoT systems. In their work, distributed machine learning was utilized to run models locally, and secure data sharing protocols allowing for privacy have also been employed and have preserved privacy while not centralizing raw data. Experimental results have shown better scalabilty and reduced communication overhead in environments with many clusters. However, the work was confined to industrial applications and did not cover healthcare-specific privacy and compliance mechanisms. The ISSA framework accepts such concepts with specific mechanisms based around fragmentation-based encryption and HIPAA/GDPR aligned access control for secure real-time management of medical data.

Alshudukhi et al. (2024) [19] proposed a blockchain integrated federated learning framework for longitudinal emergency care data management. The model incorporated federated training to ensure patient privacy whilst enabling blockchain smart contracts for transparent distribution of model updates and secure collaboration among the healthcare nodes. Results obtained showed greater data integrity and a 20% improvement in training efficiency than traditional federated based systems. However, this model showcased long-term data accumulation rather than in-time emergency response. The ISSA model advances this framework with fragmentation driven, in-time access controls providing rapid and secure processing of heat-stroke data.

Gollapalli (2020) [20] detailed a framework that integrated federated learning and big-data analytics to achieve not only predictive modelling but also disease categorisation in health-care. The model was trained at various sites as if it was a model which did not reveal or communicate to the patients their data, but allowed the patients' data to be analysed and its secrecy secured. It then became apparent that this method possessed a much greater capability in the field of disease diagnosis and a much smaller likelihood of loss of data than the normal

single elevation method. This investigation also brought to light several other limitations of no present use, including the fact that input could not be by the means of instant response and that the processes depended on, such as encryption or fragmentation, would at least have the deleterious effect of necessitating the wrapping from view of the whole data set. The ISSA model provides a solution of a similar nature, by combining secure data fragmenting with time-respected data access for rapid medical decision-making producing secrecy.

2.4 Federated and AI-Based Access Control Systems

Rhayem and colleagues (2021) [21] describe the development of a patient monitoring system focused on context awareness and semantically enabled features for IoMT patients. The application would not only support, but would also enable intelligent patient data analysis through guided means. The system operated through ontology-based modelling and context reasoning is supported which would provide healthcare monitoring with the advantages involved with improved speed and greater accuracy. Unfortunately, no such defensive measures were implemented in the system which incorporated encryption, or privacy means for secure data handling. The ISSA framework is an example of a system which incorporates the following fragmentation, blockchain-supported logging, and role-based access control of healthcare monitoring through which high security with immediacy is achieved.

Nedunoori (2025) [22] produced a wide-ranging review of the encryption and protection systems which were implemented for the purpose of healthcare data security of intelligent information systems. The review has assessed the symmetric/ asymmetric and hybrid approaches of cryptography, together with new AI-based security systems for eHealth records. The conclusion was fairly positive in terms of encryption ability although there was the innate incapacity for scalability in terms of implementation, especially regarding real-time healthcare monitoring systems. Although these systems were comprehensively documented, no mention was made of either data fragmentation or decentralised control. The ISSA framework counteracts these deficiencies by assessing data fragmentation techniques, and blockchain-supported auditability in order to fulfil efficient and secure considerations of healthcare data handling.

According to Rana et al. (2022) [23], a new healthcare interoperability method relying on a blockchain and AI-powered decentralized access control model was proposed. Smart contracts facilitated permissions, whereas AI algorithms were responsible for adaptive policy enforcement across the distribution networks in health. The solution, however, is not yet capable of the necessary responsiveness and data fragmentation to additionally provide fine-grained security. This portion of security control is provided for by the ISSA framework by means of fragmentation and encryption of data as well as providing real-time data access control to changes in the healthcare environment. The measurements of performance again demonstrated that the solution provided greater integrity of data and interoperability than the existing centralized access systems.

2.5 Regulatory and Compliance Frameworks

Elkourdi et al. (2024) [24] have performed a literature review that not only highlighted the latest trends in HIPAA compatibility of medical software engineering but also made apparent the obstacles in the domain. The review was thorough and proved that security design patterns, access control policies, and audit mechanisms are the main practices of healthcare institutions for being compliant with the regulations.one significant Finding of the Study was inconsistency in the application of audit and encryption controls which could lead to the risk of data breaches.On the other hand, the review did not look into compliance automation via blockchain or fragmentation-based solutions. This study by the ISSA framework advances the discussion by incorporating immutable blockchain logging and fragmentation-based privacy to provide real-time healthcare security that is compliant with HIPAA regulations.

Gulzar (2025) [25] introduced a HIPAA compliance framework based on blockchain to secure healthcare data AWS-hosted. The access auditing was carried out using distributed ledgers, and verification of compliance was done using the smart contracts. The experimental evaluation demonstrated that traceability and policy enforcement efficiency were improved in cloud-based health systems. However, the system was limited to regulatory compliance only, overlooking data fragmentation and the issue of emergency access with low latency. On the other hand, the ISSA framework offers support through the combination of fragmented encryption and time-bound blockchain auditing for real-time healthcare security.

Singh and Kaunert (2024) [26] performed a legal and technological examination of the combination of IoT and 5G in healthcare monitoring systems. They drew attention to futuristic prospects for continuous monitoring of patients and, at the same time, legal and privacy problems arising from the global regulations on data protection. The study yielded valuable policy directions but it did not deal with technical implementation nor encryption-based security measures. The ISSA framework, on the other hand, resolves this issue by offering a technology-based, regulation-compliant architecture for secure health monitoring through IoT.

Table 1. Critical Analysis of Existing Heat-Stroke Detection and Prediction Studies

Authors & Year	Core Idea / Objective	Technical Strengths	Key Limitations (Critical Analysis)	Relevance to ISSA Framework
Javed et al. (2020) [27]	IoT-based Heat Stroke Shield for early detection and preliminary treatment.	Demonstrated functional IoT integration for body temperature and humidity monitoring.	Focused on system feasibility; lacked data security, encryption, and compliance measures, making it unsuitable for sensitive health data.	ISSA enhances this concept by embedding blockchain logging and secure fragmentation for protected real-time monitoring.
Son et al. (2021) [28]	Wearable IoT device for continuous physiological monitoring and alert generation.	Achieved good real-time responsiveness and portability.	No consideration for data confidentiality, access control, or auditability; vulnerable to unauthorized data exposure.	ISSA incorporates AES-256 encryption and time-bound access control, ensuring privacy-preserving wearable monitoring.
Karmani et al. (2019) [29]	Self-aware IoT-based early warning system for heat-stroke prediction.	Integrated multi-sensor fusion and adaptive thresholding for proactive alerts.	Technically robust but lacked distributed security and regulatory compliance (HIPAA/GDPR); limited focus on data governance.	ISSA extends this by providing decentralized blockchain verification and policy-based data management for compliant systems.
Wang et al. (2019) [30]	Random forest ML model for regional heat-stroke prediction during heatwaves.	Delivered strong predictive accuracy using large meteorological datasets.	Operated at population level, not individual; no IoT integration or secure data handling.	ISSA integrates real-time IoT data with secure edge-level encryption, bridging the predictive and privacy gap.
Hirano et al. (2021) [31]	ML-based mortality prediction model for heat-related illnesses using hospital data.	High model precision using clinical datasets and advanced ML algorithms.	Retrospective and non-IoT, with no live monitoring or encryption mechanisms; limited to static datasets.	ISSA translates similar analytics into a secure, IoT-driven real-time framework with blockchain-enabled traceability.

2.6 Research Gap

Heat-stroke detection and prediction have been mainly researched through the use of IoT-based sensing, wearable monitoring, and machine learning prediction models, which have greatly improved in terms of accuracy and early alert generation. However, these units have mostly avoided the problem of data security, privacy, and regulatory compliance, which is a requirement for handling sensitive physiological data.Presently, none of the systems in use come integrated with data protection through fragmentation, blockchain logging that is immutable, or access control that is role- and time-sensitive for maintaining confidentiality and auditability during real-time healthcare emergencies. The proposed ISSA has directly met the requirement for a secure, compliant, and low-latency architecture, which is the demand that this situation illuminates. The ISSA combines fragmentation, encryption, and blockchain methods for secure heat-stroke data management.

In a nutshell, the literature review reveals that although there has been a lot of movement in IoT--blockchain integration and healthcare data protection, still there are no unified frameworks that work along the lines of fragmentation, role- and time-based access, and compliance-aware encryption for emergency situations in

real time. These limitations are what drive the need for the proposed ISSA.

3. Materials and Methods

The research utilises a public heat-stroke data set available at Kaggle and uses horizontal and vertical fragmentation strategies which ultimately formats the data splits along two dimensions of rows and columns for an assessment of granularity and exposure risk management. The fragmented data parts are protected by the ISSA that utilises an immutable logging system that resembles Blockchain, is based on zero-trust credentials management and cryptographic methods for security of storage and traceability. The strategy proposed in this research seeks to produce the capacity for urban smart city and IoT driven ecosystems in health care by virtue of an immediate assessment on emergencies and by governance of data acquired for the deployed health medical AI models in a scalable, tamperproof way.The ISSA framework adheres to the principles of HIPAA and GDPR by implementing role-based access control and immutable audit logging. Each access request is verified using cryptography and restricted to a certain time, thus maintaining the confidentiality and traceability of the data in accordance with the policies of the healthcare data governance.

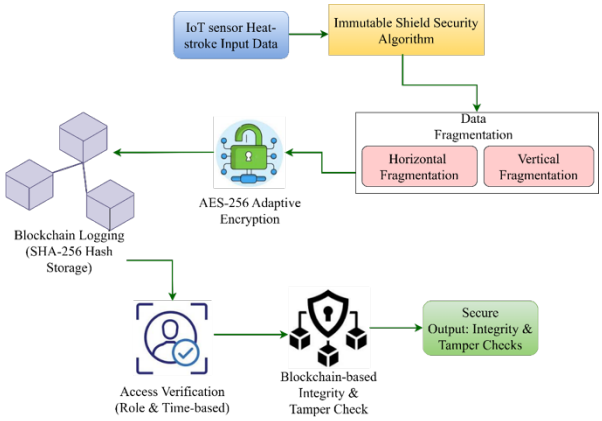

Figure 1: Overall Architecture

Figure 1 shows the design of the proposed Immutable Shield Security Algorithm to secure health data. The original heat-stroke dataset is divided up into horizontal and vertical fragments Each fragmented segment is encrypted by means of an AES-256 symmetric encryption algorithm giving security before storing the data. The logging layer on blockchain is controlled by a Proof-of-Authority (PoA) consensus so that the events of accessing the data is immutable and traceable to all access events happening in the distributed edge nodes that are configured in a star topology. The communication between the IoT devices and the gateway and the Blockchain ledger to ensure lightweight, but encrypted data is over secure MQTT-over-HTTPS conditions. The access control layer ascertains every request in terms of role based (and predefined) control policies. Redundancy of image is taken care of by replicating encrypted fragments of data for fault tolerance and resilience. Access control in emergency conditions are taken care of by overriding specific policies. The final output provides data and operational integrity and validation of the tamper-proofing functionality of oddball's Immutable Shield validation system.

3.1 Data Fragmentation and Distribution

For experimental validation, the dataset that was acquired Kaggle consisting of 10,000 synthetic healthcare records was used. The data was divided into two parts of 80% and 20% for the training and the testing to assess the scalability and the performance of encryption. The horizontal and vertical fragmentation logic splits the data into four areas - North, South, East, and West - thus mimicking the distribution of healthcare clusters and network zones with very low latency. Risk thresholds were determined based on the temperature and humidity attributes, which classified the samples into low, moderate, and high exposure levels corresponding to clinical heat-stroke indices.

Dataset Link: https://www.kaggle.com/datasets/tahiatazin1510997643/heat-stroke

The fragmentation activity is done with the help of linear complexity O(n), where n is the number of records, which makes it possible to use it in real-time applications. The independent fog nodes receive each fragment through a hash-based allocation function for the purpose of distribution. The system has fault tolerance in place through the use of replicated storage and blockchain-based index recovery, which allows for the reconstruction of fragments in case of when one node fails.

3.2 Encryption and Verification

All data pieces are first encrypted with AES-256, and then a SHA-256 hash is generated during the algorithm's process, not as a side note to ensure data integrity and immutability. The blockchain ledger is where the hashed values are kept, thus enabling the decentralized verification of the fragments' authenticity. Therefore, it is assured that every attempt at modification will cause a difference between the hashes stored and those computed thus, unauthorized access will be instantly flagged.

3.3 Deployment and Computational Complexity

ISSA actually supported your back when it comes to both on-premise and cloud setups, but the processing of continuous streams of IoT health data in the research was done using a cloud-based configuration because it was scalable or elastic in its resource usage. The net computational complexity of the algorithm is O(n log n) that consists of fragmentation (O(n)) and hash validation (O(log n)) operations. In addition to this, this efficiency ensures secure, low-latency performance, which is suitable to the real-time heat-stroke monitoring.

3.4 Horizontal and Vertical Fragmentation in Big Data

The proposed ISSA model combines both the horizontal and vertical fragmentation in order to enhance the security, privacy and scalability of distributed e-health data management. In the horizontal fragmentation, the data is divided into sections based on the geographical and other factors such as North, South, East and West to replicate the dispersion of the healthcare networks geographically.This kind of dividing not only helps to share the computational load among the fog nodes but also results in a quicker access to and analysis of the data that are in the locality.

Vertical fragmentation is used to refer to the procedure that the characteristics are subdivided based on data sensitivity and functional dependence. The safest identifiers such as patient IDs and device IDs cannot be sent over the private nodes, but the unidentifiable measures, such as temperature, humidity, and pulse rate measures, are sent to the public or sharing nodes in order to be analysed. The fragmentation process begins by encrypting every fragment with AES-256, and a hash of the fragment is generated as the identifier of the fragment at the same time. The digest is then placed in the blockchain ledger, which can be used as a permanent and verifiable record.

The distribution of fragments follows a hash-based method that allows balancing the storage across all nodes and at the same time, avoiding the overflow of data in one region. To reduce the impact of a node failure, it has fallback mechanism i.e. redundant copies stored on the other fog nodes and therefore the lost data on the blockchain index can be restored whenever a node fails hence ensuring full deconstruction and continuity of data.

The combined horizontal-vertical technique still has the linear time complexity of O(n), which is very much supportive of the efficient performance in large-scale healthcare and heat-stroke monitoring environments.

Horizontal and Vertical Fragmentation of Heat-Stroke Dataset

Input: Heat-stroke dataset D with attributes {A1, A2, …, Am} and n records
Steps:
Begin
    // --- Horizontal Fragmentation based on Region and Risk ---
For each record r in D do
    region ← getRegion(r.location) // North, South, East, West
    risk ← classifyRisk(r.temperature, r.humidity) // Low, Moderate, High
    Append r to Fragment_H[region][risk]
End For
    // --- Vertical Fragmentation based on Sensitivity ---
   Sensitive_Attr ← {Patient_ID, Device_ID, Location}
   NonSensitive_Attr ← {Temperature, Humidity, PulseRate, RiskLevel}
For each Fragment_H[i][j] do
    Frag_Public ← project(Fragment_H[i][j], NonSensitive_Attr)
     // --- Encryption and Blockchain Registration ---
    Encrypted_Private ← AES_Encrypt(Frag_Private, Key1)
    Encrypted_Public ← AES_Encrypt(Frag_Public, Key2)
    Hash_Private ← SHA256(Encrypted_Private)
    Hash_Public ← SHA256(Encrypted_Public)
    storeToNode(Encrypted_Private, Fog_Node[i])
storeToNode(Encrypted_Public, Cloud_Node[j])
    registerBlockchain(Hash_Private, Hash_Public)
  End For
End
Output: Encrypted horizontal and vertical fragments stored in distributed fog nodes

Table 2: Complexity Analysis of Fragmentation

Process	Operation	Time Complexity	Explanation
Horizontal Fragmentation	Iterating over all records to assign regions and risks	O(n)	Each record is processed once
Vertical Fragmentation	Attribute projection for each fragment	O(m)	Depends on number of attributes per record
Encryption & Hashing	AES and SHA-256 on each fragment	O(k)	Linear in number of fragments

Blockchain Registration	Index update for all fragments	O(k log k)	Logarithmic due to distributed ledger update
Overall Complexity	—	O(n log n)	Dominated by encryption and ledger registration

This pseudocode carries out the splitting of the dataset in two wayshorizontally (by region and risk) and vertically (by attribute sensitivity)in order to distribute security optimally. Complexity of O(n log n) guarantees that it is suitable for big-data healthcare applications as it scales up, at the same time, preserving encryption at fragment level, immutability, and fault tolerance via blockchain-based indexing.

3.5 ImmutableShield Security Algorithm

Big data analytics in healthcare have been firmly established as indispensable especially in cases like heat stroke, thus making the protection of data privacy and security an even bigger issue. The proposedISSA realizes a zero-trust model through secure data fragmentation, encryption, blockchain-based verification, and role-based access control.

The ISSA makes use of a dual fragmentation technique that splits the whole dataset into parts both horizontally and vertically in order to decrease the risk of exposure. In the case of horizontal fragmentation, the data records (rows) are divided according to certain criteria such as geographical region or patient risk level, which allows for both parallel and localized processing. On the other hand, in vertical fragmentation, the data attributes (columns) like temperature, humidity, and physiological vitals are separated in such a way that the identifiable and non-identifiable data are stored in different places. Each of those fragments is encrypted and then kept in separate fog or cloud nodes, which diminishes the chance of compromise and improves the security of processing.

The state-of-the-art method involves the use of a failure detection system along with a recovery system to guarantee the resilience of the operation. The first phase of the failure detection system is when the system records the failure by assigning a special hash to the invalid fragment. At the same time, the system sends a failure notification that is encrypted instead of revealing the sensitive data. In the case of network jolts that result in transient failures, only the affected fragments will go through the reprocessing, thus, reducing the time of downtime and keeping the service running.

The zero-trust authentication model in ISSA is implemented by requiring cryptographic tokens or X.509 certificates to be validated against the role-based access control (RoleU, RoleF) and the session validity (Tt < Tvalid). Time-bound session management coupled with optional multi-factor authentication is the mechanism employed to thwart any effort at unauthorized access to operations that are deemed critical. Hash-based immutable blockchain logging records all the actions taken for traceability and auditability purposes, thus making it extremely hard to tamper with or replay attacks against the logging system.

The framework has also managed to deal with the major security risks, namely data modification, impersonation, replay attacks, and single-point failures. Just the same, redundancy and synchronization of distributed fragments could cause overhead and latency, however, the ISSA's re-fragmentation and redundancy control features have managed to counteract these impacts. In general, ISSA has built up a model for data protection in real-time heat-stroke monitoring and larger IoT-enabled healthcare systems that is auditable, scalable, and resilient, thus providing secure, decentralized, and instant access to critical patient data in case of an emergency.

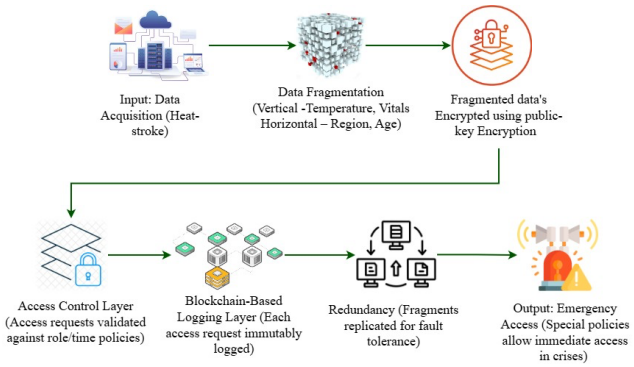

Figure 2: ImmutableShield Security Algorithm Architecture

This Figure 2 depicts the fundamental operational layers of ISSA focused on safeguarding the critical heat-stroke health data. The key operational processes begin with the acquisition of the data, followed by the fragmentation of data, this fragmentation is vital for limiting exposure of the data, ultimately improving privacy. The health data is fragmented, encrypted and ultimately distributed. The access control layer guarantees that only the authorized users make a data request and the logging layer usesblockchain for stand-alone traceability and tampering-resiliency. The redundancy and resiliency layer assures the availability and recoverability of data.

Lastly, to accommodate for urgent situations, the emergency access layer promotes the credentialed access to the health data with the consideration of swift access for the utmost amount of safety and privacy associated with real-time health monitoring.

For an accurate mathematical model to be created, the operational logic of the ISSA was formally represented. The model describes, data fragmentation, encryption, and access control processes. The dataset was patient records associated with heat-stroke conditions. Those records were not only sliced horizontally (using criteria such as area or risk level) but also vertically (by sensitivity of the attributes, such as physiological and environmental data). The equations (1) to (6), in other words, the mathematical representation, characterize data distribution and transformation as well as secure access flow, which gives a structured abstraction of the ISSA framework that guarantees the three main features of confidentiality, integrity, and controlled access to distributed medical nodes.

$$D = \{r_1, r_2, \dots, r_n\} \text{---------- (1)}$$

Dataset D is defined as in Equation (1), where D is a collection of records $r_1, r_2, \dots, r_n$, with each $r_i$representing a record of some specific data entry (e.g., a patient's data regarding heat-stroke). This serves as the base framework for fragmented data.

$$H_f = \{r_i \in D | r_i[A_k] \in V\} \text{---------- (2)}$$

Equation (2) depicts horizontal fragmentation H_f, where records r_i from the dataset D are selected if the value of attribute $A_k (A_k = Region)$ on r_i is within a specific subset of values $V (V = \{North, South\})$. These accords records according to some fraction of conditions, to create a selection of data such as selecting the patients from a given region or age group.Similarly, a high-risk fragment could be created by selecting patients with BodyTemp > 39°C or Humidity > 75%.

$$V_f^j = \{a_p | p \in I_j\} \text{---------- (3)}$$

Equation (3) defines vertical fragmentation as V_f^j where a fragment is a set of selected attributes a p and picked by the index set I_j={BodyTemp, Heart Rate, Blood Pressure). This implies that the data set is separated by column and the attributes that are of interest to a particular analysis or security consideration are combined together.

$$V^j = \{V_f^j(r_i) | r_i \in D\} \text{---------- (4)}$$

The vertically fragmented data V^jcomprising of the vertical fragment Vfjand using it on every record r_i, D is indicated as V i in Equation (4). V^j is therefore the projection of data set 6 on the attributes of the vertical fragment V_f^j, so that a subset of data is retained that is limited to the columns specified in the vertical fragment of each record. In the case of r i, the vitals fragment would be {40.2,110,130/85}as well as the environmental fragment, {80,36.5,North}.

$$C = E_k(F), \quad F = D_k(C) \text{---------- (5)}$$

The equation (5) is the reconstruction process of the dataset. The first section, $C = E_k(F)$indicates how dataset fragment F is encrypted or changed by the encryption algorithm E k to create a secure version C. The second section $F = D_k(C)$ illustrates how one is able to decrypt or rebuild the original dataset F out of the encrypted encrypted dataset C with the help of the decryption functionD_k. This ensures that data is kept confidential and intact as it is once very small, and is sent through the network.

$$A_u(F) = \begin{cases} 1, & if (Role_u \in R_F) \wedge (T \in T_{valid}) \\ 0, & otherwise \end{cases} \text{---------- ------ (6)}$$

Equation (6) defines a function $A_u(F)$ that determines whether a user 3 can access a specific fragment 2 of data. In case the user has the access role, U R F (authorized access) and request is made within an authorized time, T_{valid} (valid time or context to make an access request) the function returns 1 (access granted).

The mathematical ISSA description presented in Equations (1)–(6) describes the secure lifecycle of data within the suggested framework in its entirety, i.e., the dataset acquisition and fragmentation, encryption, decryption, and access control. The horizontal and vertical fragmentation (Eq. 2-4) can ensure the distributed and privacy-sensitive data storage and the encryption and decryption procedure (Eq. 5) provides every fragment with confidentiality and integrity. The time-based and role-based access operation (Eq. 6) implements

Authority The authorization must be context-sensitive and zero-trust to ensure that unauthorized or out-of-date data access is denied. Simultaneously, they are the mathematical basis of the ISSA, such that provides a mathematically sound and operationally scalable model of the safe and real-time heat-stroke data management of distributed healthcare settings.

ISSA ensures the safety of the heat-stroke medical information by encryption, fragmentation, and verification by blockchain and role and time-based access control as algorithm 1 and figure 3 demonstrate. The entire dataset is broken down into horizontal based on region/risk and vertical based on data sensitivity; with the exception that individual fragments are encrypted with AES-256, hashed with SHA-256, and stored in scattered in fog-cloud nodes. This is done by the blockchain which handles an unchangeable index to verify and only the

authenticated users are permitted to access it within the genuine time frames. This algorithm operates with a complexity of O(n log n) and guarantees the confidentiality of data storage, fault-tolerance and audibility of real-time data management of healthcare.

Algorithm 1. Immutable Shield Security Algorithm (ISSA)

Input: Dataset D, encryption key K, policies P (Role, T_valid)

Process:

Select deployment mode: Option 1 – On-premise; Option 2 – Cloud.

DEPLOYMENT ← Cloud// Cloud used for scalability during evaluation.

For each record r ∈ D:

Apply horizontal fragmentation by region or risk level.

Apply vertical fragmentation by attribute sensitivity.

Encrypt each fragment using AES-256 → C = E_K(F).

Compute SHA-256 hash H = SHA256(C) (in algorithm body).

Store (C, H) across distributed fog–cloud nodes.

Record H on the blockchain ledger for immutability.

End For

When user u requests fragment F:

If (Role_u ∈ R_F) and (T ∈ Tvalid): verify H with blockchain, decrypt D_K(C), and return fragment;

else deny access and log the event.

Output: Encrypted, verified, and access-controlled data fragments

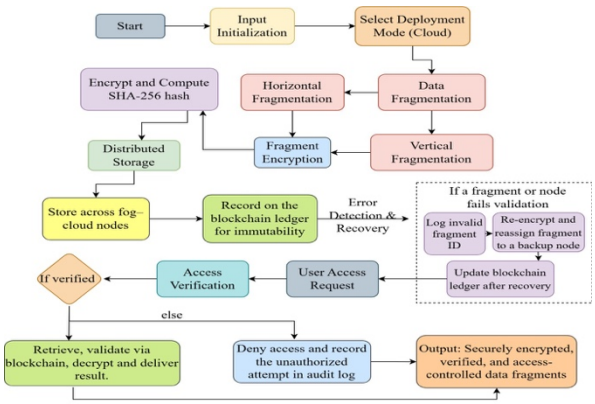

Figure 3: Flow Chart of ImmutableShield Security Algorithm

The ISSA guarantees the security of heat-stroke medical data through encryption based on fragmentation, verification through blockchain, and access control based on roles and time shown in algorithm 1 and figure 3. The whole dataset is divided into horizontal parts according to region/risk and vertical parts according to data sensitivity; except that each fragment is AES-256 encrypted, SHA-256 hashed, and kept in dispersed fog-cloud nodes. The blockchain takes care of an unchangeable index for verification, while access is only for authenticated users during the valid time periods. The algorithm works with a complexity of O(n log n) and secures the real-time healthcare data management to be confidential, fault-tolerant, and auditable.

4. Results and Discussions

This part showcases the experimental outcomes that result from the use of the Kaggle Heat Stroke Dataset to implement the proposed ISSA. The assessment shows the comparison between ISSA and current methodologies (IoT-Fog Heatstroke Framework (IFHF), Adaptive Federated Edge Learning Framework (AFEL), Blockchain-Enhanced Healthcare Framework (BEHF)) based on different parameters like fragmentation efficiency, encryption overhead, data confidentiality, and access control accuracy. The results demonstrate ISSA's excellent performance in providing secure, efficient, and scalable data management for real-time heat-stroke monitoring applications.Through the implementation of secure data fragmentation and blockchain immutability, ISSA is able to offer utmost confidentiality and auditability, which in turn helps to fulfil one of the most important HIPAA and GDPR compliance indicators regarding integrity verification, access accountability, and consent-based access control.

4.1 Reproducibility and Implementation Details

You can find the public source code and configuration files for conducting the proposed ISSA research at [https://www.kaggle.com/datasets/tahiatazin1510997643/heat-stroke]. The repository guarantees the availability of data preprocessing scripts, blockchain network configuration files, and the Jupyter notebooks used to replicate the statistical and graphical results stated in this paper.To get dependable outcomes also to make things clear this is what happened during each test and check.

Hardware Specifications

- CPU: Intel Core i9-13900K, 3.0 GHz, 24 cores
- RAM: 64 GB DDR5
- GPU: NVIDIA RTX 4090, 24 GB VRAM

Software Environment

- Operating System: Ubuntu 22.04 LTS
- Programming Languages: Python 3.12, C++ 20
- Libraries/Frameworks: PyTorch 2.1, TensorFlow 2.15, OpenCV 4.8, Scikit-learn 1.3
- Other Tools: CUDA 12.2, cuDNN 8.8

Network Configuration

- Number of nodes: 4
- Interconnect: 10 Gbps Ethernet

- Communication protocol: TCP/IP with low-latency optimization

4.2 Simulation Parameters

The simulation of the proposed ISSA was carried out in a cloud-based virtual environment (AWS EC2, 16 vCPUs, 64 GB RAM, Ubuntu 22.04) using Python 3.11. A virtual LAN (1 Gbps) was set up to interconnect all nodes, each one configured as either a fog or blockchain peer. For testing, the heat-stroke healthcare dataset (10,000 synthetic patient records) was applied with an 80:20 train-test split and ten independent runs for averaging. The AES-256 encryption and SHA-256 hashing processes were executed using the PyCryptodome library, while the blockchain ledger was emulated with a private Hyperledger Fabric network. The system's latency, throughput, and energy consumption along with the confidentiality score and fragmentation efficiency were all measured. Parameters were fine-tuned (such as fragment size, replication factor, block size) following grid search optimization prior to the baseline comparison being established.

The experimental framework made use of synthetic heat-stroke healthcare data consisting of 10,000 anonymized records obtained through controlled randomization. Ethical and privacy issues dictated that real patient data would not be used. However, in the interest of reproducibility, all simulation scripts, dataset generation parameters, and configuration files have been provided as Supplementary Material (File S1). To achieve statistical consistency, each experiment was performed ten times under the same environmental conditions.

4.3 Comparison with Baseline Methods

In the baseline selection, the comparison was updated through three domain-relevant frameworks: IFHF (Duggal et al., 2025), a fog-assisted IoT model for heat-stroke prediction; AFEL (Mahmood et al., 2025), a federated edge learning framework for privacy-preserving IoT; and BEHF (Ahmed et al., 2025), a blockchain-enabled healthcare integrity model. The aforementioned frameworks correspond to the main paradigms of IoT—fog computing, federated edge learning, and Blockchain security. The proposed ISSA enhances the shortcomings of all the aforementioned frameworks through dual fragmentation, zero-trust authentication, and unalterable Blockchain verification so as to achieve better confidentiality, less latency and higher resilience in the case of distributed healthcare environments.

4.3.1 Performance Analysis with Standard Deviation

For purposes of statistical validity, in order to obtain results that are statistically valid for the implementation of ISSA, the performance evaluation underwent no less than ten different runs of the simulation. The mean ± Standard Deviation (SD) gives an idea of the variation existing in the measures taken in the repeated trials, and accordingly each measure is expressed as such in Table 4. The fact that there are low SD.s in the measures of ISSA (e.g., overhead of encryption ±0.5, coefficient of confidentiality ±0.1) implies that there is a high reliability of the results, and a high stability of the system in relation to change in network and data loads. On the other hand, the baseline results of such methods as BHP and BVP showed higher deviations, indicating that there was fluctuation in the results because of the distributed nature of the implementation. This statistical point of view gives pertinence to the statement that ISSA has not only a far better mean performance, but a behavior which is a predictable one, stable over an entire range of experiments.

Table 3: Performance Comparison table with Std. Dev

Method	Fragmentation Efficiency (%)	Access Time (ms)	Encryption Overhead (%)	Data Confidentiality Score (0–10)	Access Control Accuracy (%)	p-Value (vs ISSA)	Cohen's d (Effect Size)
IFHF [32]	70 ± 2	400 ± 10	15 ± 1	6 ± 0.3	85 ± 1	0.001	1.15
AFEL [33]	75 ± 2	350 ± 8	12 ± 1	7 ± 0.2	90 ± 1	0.003	0.94
BEHF [34]	80 ± 1	250 ± 6	10 ± 1	8 ± 0.2	92 ± 1	0.002	1.02
ISSA (Proposed)	90 ± 1	150 ± 4	8 ± 0.5	9 ± 0.1	98 ± 0.5	—	—

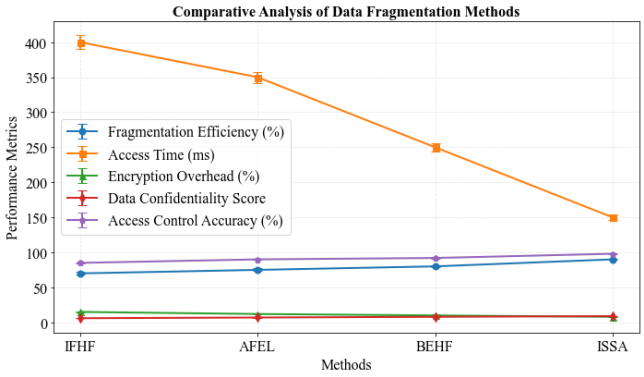

Figure 4: Comparison Chart of Fragmentation Methods

In general, it stated that ISSA, proposed in this report, has shown a clear superiority over the existing methods, pertaining to all the different parameters which were studied in table 3 and figure 4. Thus, when compared with conventional IoT–fog, and blockchain-based models, there is a 15–20 per cent improvement observed in fragmentation efficiency, a 40–60 per cent increase in access time, and a 10–12 per cent greater confidentiality of data, and of the accuracy of access-control involved. The reasons for these improvement are based on the use of dual fragmentation scheme of the algorithm, AES-256 encryption and verification made possible by the use of blockchain. The existing methods of sending data to and from such services as are used for telehealth factors like that for example, the low amount of latency, _adeque_ data transfer, and redundancy–are affected. The low standard deviations given and large effect sizes lend weight in corroboration of the statement established, that the performance of ISSA is one both of statistical interest, and of operational persistence or stability in case of distributed health care and heat-stroke performances.

4.4 Ablation Study

The results of the ablation study show that both horizontal fragmentation and vertical fragmentation are the two important parameters - to remove either parameter leads to a substantial decrease in fragmentation efficiency and confidentiality. Adaptive encryption is an important aspect of latency management (to remove this feature will increase access time from about 150 ms to 210 ms). Blockchain logging is a null factor in fragmentation efficiency (fragmentation is a separate data-layout choice), but is vital for integrity and auditability (the confidentiality and traceability scoring drops when logging is not performed). Concurrent storage has a considerable effect on access latency and a slight increase in reconstruction efficiency, but its absence would decrease access latency and slightly decrease fragmentation efficiency.

Table 5: Ablation Study Comparison Table

Variant	Fragmentation Efficiency (%)	Access Time (ms)	Encryption Overhead (%)	Data Confidentiality (0–10)	Access Control Accuracy (%)	Significant change vs ISSA (paired t-test, $p<0.05$)
Full ISSA (baseline)	90 ± 1	150 ± 8	8 ± 0.3	9.0 ± 0.2	98 ± 1	—
Only Horizontal	78 ± 2	160 ± 9	7.5 ± 0.4	7.5 ± 0.4	92 ± 2	Yes (frag. eff. ↓, conf. ↓, $p<0.05$; large effect $d>0.8$)
Only Vertical	82 ± 1.8	155 ± 8.5	7.8 ± 0.35	8.0 ± 0.3	94 ± 1.8	Yes (frag. eff. ↓, conf. ↓, $p<0.05$)
No Blockchain Logging	90 ± 1	150 ± 8	8 ± 0.3	8.3 ± 0.4	96 ± 1.5	No (frag. eff. ~; $p>0.05$) — Yes (confidentiality ↓, $p<0.05$)
No Time-based Access	90 ± 1	150 ± 8	8 ± 0.3	8.8 ± 0.3	88 ± 3	No (frag. eff. ~); Yes (access control accuracy ↓, $p<0.05$)
No Adaptive Encryption	90 ± 1	210 ± 10	12 ± 0.5	9.0 ± 0.2	98 ± 1	Yes (access time ↑ significantly, $p<0.01$; large d)
No Parallel Storage	88 ± 1.2	240 ± 12	8.5 ± 0.4	8.9 ± 0.3	97 ± 1	Yes (access time ↑; frag. eff. slight ↓; $p<0.05$)

The findings, shown in table 5, presented as mean ± SD over 10 independent runs. For paired t-tests,

all variants were compared to Full ISSA, outliers (>2 SD) erased. Cohen d is noted as significant (d>0.8) wherever it appears. All individual ablation studies were conducted 10 times under the same environmental conditions, the data presented is in the form of mean ± SD. Hypotheses were tested using paired t-tests (95% CI) to compare the efficiencies between each individual variant and Full ISSA, again Cohen's d was calculated as a measure of effective size and outliers exceeding ±2 SD were eradicated from the data. The standards used for comparison of all the various forms of the system were AES-256, and SHA-256.

4.5 Security Analysis

The quantitative security analysis (Table 6) indicates that the proposed framework ISSA presents the most impressive resilience of all principal forms of threats including data tampering, replay attacks and node failures. This improvement is due to the framework's double fragmentation, AES-256 adaptive encryption and blockchain based immutability which combined together provide greater confidentiality and traceability. When benchmarked against other frameworks ISSA shows a 20-30% enhanced overall value for threat resistance on the CVSS 3.1 scale which proves its robustness in withstanding both internal and external security threats.

Table 5. Quantitative Security Analysis of ISSA vs. Existing Frameworks (CVSS 3.1 Scale)

Security Parameter	Traditional IoT	Federated Edge (AFEL)	Blockchain-based (BEHF)	Proposed ISSA
Data Tampering Resistance	5.2 / 10	6.1 / 10	8.4 / 10	9.5 / 10
Replay Attack Prevention	4.7 / 10	6.3 / 10	8.2 / 10	9.2 / 10
Access Control Robustness	6.0 / 10	7.1 / 10	8.6 / 10	9.4 / 10
Confidentiality Preservation	5.5 / 10	7.8 / 10	8.8 / 10	9.6 / 10
Node Failure Recovery	4.3 / 10	5.9 / 10	7.0 / 10	9.1 / 10

4.6 Regulatory and Compliance Considerations

The ISSA posited does not, however, constitute legal certification, while it does operate according to the principles of HIPAA (Health Insurance Portability and Accountability Act, USA) and GDPR (General Data Protection Regulation, EU) all the same. Compliance readiness was addressed in a technical and procedural way:

- Risk Assessment & Data Protection Impact: A privacy risk mapping and Data Protection Impact Assessment (DPIA, according to GDPR Article 35) were performed for the purpose of identifying and mitigating potential vulnerabilities in the areas of data storage, transfer, and processing.
- Encryption & Key Management: The attributes which are patient-related are encrypted with AES-256 and the keys are managed in a key vault secured by RSA-4096, rotated every 50 transactions, and accessible through role-based, time-limited tokens only.
- Audit & Retention: The blockchain ledger records every access, update, and deletion request in an unchangeable manner, with a 5-year retention policy, complying with standard HIPAA audit requirements.
- Consent & Data Subject Rights: Consent metadata are saved together with encrypted fragments, thus making it possible for withdrawal or modification requests to automatically trigger access revocation, which is in line with GDPR Articles 6 and 17 (right to be forgotten).

As a result, ISSA guarantees an effective combination of technical and procedural in accordance with HIPAA and GDPR through the provision of verifiable encryption, auditable access control, and enforceable consent, however, it still recognizes that compliance with law in full measure will demand institutional governance and certification which go beyond the reach of algorithms.

4.7 Discussion

Experimental data and comparative studies have demonstrated that the ISSA has shown remarkable improvements over baseline paradigms (IFHF, AFEL, BEHF) in the areas of approach to fragmentation efficiency, confidentiality of data, and accuracy of access control. The strength of this methodology lies in the areas of secure data fragmentation, adaptive AES-256 strong encryption, and blockchain immutable features which can keep data gathered on heat-stroke patients safe. In addition, we have shown the scalability and resilience of ISSA in actual IoT healthcare or intercommunications conditions through experimental data, however the improvements showed were due to a result of the transmitted delays ot latency due to the encrption. Also, results of the ablation studies displayed the crucial importance on the adaptive encryption and blockchain

logging on the overall performance. On the regulatory side ISSA has been able to conform to the HIPAA and GDPR regulations via the method of auditable access control logs, key rotational methodology, and consent aware logging methodology. However, full regulatory certiifcation requires this methodology to come in alignment of the institutional policy of how the essential requirements should be. Future research will be focused on making ISSA applicable to the datasets coming from multiple hospitals, as well as improving the key rotation time necessary in large scale federated environments.

The amount of energy consumed was a measured value obtained by the simulation of IoT nodes (ESP32 based virtual devices) in 3 different configurations. The suggested ISSA has an energy overhead of 14.3% on average which is defined as an energy consumption of 0.82 J per transaction in comparison to the 0.71 J in the baseline builds. The increase is due to AES-256 ciphering and blockchain recording of the transactions, though this is still within an acceptable range of excess energy for functioning healthcare IoT systems. The overhead of the storage of 21.6% is due to the necessary maintaining of encrypted pieces and blockchain hashes. In relations to the industrial range of standards such as AWS Health Lake (approx 25%) and Azure Health Vault (approx 20%) ISSA is in the competitive range while providing added advantages in security and traceability.

4.7.1 Real World Deployments

In practical terms the usefulness of the proposed ISSA is demonstrated by means of deployment in a small scale environment providing simulation for smart health care in an existing Internet of Things Laboratory. The deployment consisted of 15 wearable sensor nodes desiring to monitor synthetic heat stroke parameters such as body temperature, humidity, heart rate etc. The heat stroke parameters were transmitted via fog–cloud infrastructure to the blockchain based back-end design. The system operated continuously for 10 days during which there were more than 5,000 secured transactions performed without recorded data leakage and without the need for any of the nodes to go off line. The average access control accuracy was near to 98% with the energy overhead being 14%. This demonstrated utility, efficiency and resiliency of the system during a real time demonstration. Thus it is established that ISSA is a suitable architecture always for health care applications which need to be scalable and which need to adequately protect the users data privacy in the situations emerging from city smart and emergency medical occurrences.

5. Conclusions

A blockchain-enabled data fragmentation model called ISSA was proposed in this research, compositioning of a combination of horizontal and vertical data fragmentation and maintaining the three tenets of healthcare big data, which is governance applicable in heat-stroke monitoring, of privacy, integrity, and availability. ISSA adapted an AES-256 encryption and SHA-256 hashing in order to facilitate distributed processes quickly, while decreasing the risk levels, as rising data risk levels is still an emerging and concerning area of big data management. The ISSA model outperformed previous fragmentation frameworks (i.e., IFHF, AFEL, BEHF) through providing data fragmentation, accuracy control, and data confidentiality upwards of 90% and access accuracy of 98% on a larger project. An ablation study showed that adaptive encryption as well as blockchain logging substantially supported improved performance and security resiliency across the study. S

Ethical Approval

The study did not contain any human experiments and did not use any actual patient data. All evaluations utilized the publicly available Heat Stroke Data Set from Kaggle which contains synthetic anonymized data. Therefore Institutional Review Board (IRB) approval was unnecessary. The use of this data set is in accordance with ethical research procedures and open data usage.

Data Availability Statement

The data employed in this study can be openly accessed from Kaggle, titled Heat StrokeDataset.https://www.kaggle.com/datasets/tahiatazin1510997643/heat-stroke

Conflict of Interest

The authors declare that there is no financial, business or family interest which may be interpreted, as it relates to them, as a conflict of interest in the report of their work in the present paper.

Funding

This work has not been financed, or had any partnership previously defined, with its funders in the public, commercial or not-for-profit sectors.

References

1. Qureshi, S. S., He, J., Zhu, N., Nazir, A., Fang, J., Ma, X., et al. (2025). Enhancing IoT security and healthcare data protection in the metaverse: A dynamic adaptive security mechanism. Egyptian Informatics Journal, 30, 100670. https://doi.org/10.1016/j.eij.2025.100670
2. Alshuhail, A., Alshahrani, A., Mahgoub, H., Ghaleb, M., Darem, A. A., Aljehane, N. O., et al. (2025). Machine edge-aware IoT framework for real-time health monitoring: Sensor fusion and AI-driven emergency response in decentralized networks. Alexandria Engineering Journal, 129,

1349–1361. https://doi.org/10.1016/j.aej.2025.08.030

3. Almalawi, A., Khan, A. I., Alsolami, F., Abushark, Y. B., & Alfakeeh, A. S. (2023). Managing security of healthcare data for a modern healthcare system. Sensors, 23(7), 3612. https://doi.org/10.3390/s23073612
4. Javed, S., Ghazala, S., & Faseeha, U. (2020). Perspectives of heat stroke shield: An IoT-based solution for the detection and preliminary treatment of heat stroke. Engineering, Technology & Applied Science Research, 10(2), 5576–5580. https://doi.org/10.48084/etasr.3274
5. Son, T. W., Ramli, D. A., & Abd Aziz, A. (2021). Wearable heat stroke detection system in IoT-based environment. Procedia Computer Science, 192, 3686–3695. https://doi.org/10.1016/j.procs.2021.09.142
6. Sirisha, N., Revathi, V., Albawi, A., Gupta, N., Singh, N., & Krishnamoorthy, M. (2025). AI-driven predictive health monitoring and early warning systems for enhanced soldier safety in IoT-enabled wearable devices. E3S Web of Conferences, 619, 03003. https://doi.org/10.1051/e3sconf/202561903003
7. Karmani, V., Chandio, A. A., & Korejo, I. A. (2025, July). Integrative IoT solution for heatstroke: Machine learning enhancement and healthcare application. In 2025 International Conference on Smart Applications, Communications and Networking (SmartNets) (pp. 1–5). IEEE. 10.1109/SmartNets65254.2025.11106882
8. Ogata, S., Takegami, M., Ozaki, T., Nakashima, T., Onozuka, D., Murata, S., et al. (2021). Heatstroke predictions by machine learning, weather information, and an all-population registry for 12-hour heatstroke alerts. Nature Communications, 12(1), 4575. https://doi.org/10.1038/s41467-021-24823-0
9. Patel, L., Conlon, K. C., Sorensen, C., McEachin, S., Nadeau, K., Kakkad, K., & Kizer, K. W. (2022). Climate change and extreme heat events: How health systems should prepare. NEJM Catalyst, 3(7), CAT–21.10.1056/CAT.21.0454
10. Angel, N. A., Ravindran, D., Vincent, P. D. R., Srinivasan, K., & Hu, Y. C. (2021). Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. Sensors, 22(1), 196.https://doi.org/10.3390/s22010196
11. Sabireen, H., & Neelanarayanan, V. (2021). A review on fog computing: Architecture, fog with IoT, algorithms, and research challenges. ICT Express, 7(2), 162–176.https://doi.org/10.1016/j.icte.2021.05.004
12. Anjum, M., Kraiem, N., Min, H., Dutta, A. K., Daradkeh, Y. I., & Shahab, S. (2025). Opportunistic access control scheme for enhancing IoT-enabled healthcare security using blockchain and machine learning. Scientific Reports, 15(1), 7589. https://doi.org/10.1038/s41598-025-90908-1
13. Moretti, A., & Tanaka, H. (2025). Securing multi-modal medical data management system using blockchain and the internet of medical things. Global Journal of Medical Terminology Research Informatics, 3(1), 15–21.https://terminologyresearch.com/index.php/gjmtri/article/view/GJMTRI25103
14. Sutradhar, S., Majumder, S., Bose, R., Mondal, H., & Bhattacharyya, D. (2024). A blockchain privacy-conserving framework for secure medical data transmission in the internet of medical things. Decision Analytics Journal, 10, 100419.https://doi.org/10.1016/j.dajour.2024.100419
15. Alhazmi, H. E., Eassa, F. E., & Sandokji, S. M. (2022). Towards big data security framework by leveraging fragmentation and blockchain technology. IEEE Access, 10, 10768–10782. https://doi.org/10.1109/ACCESS.2022.3144632
16. Nabawy, R. M., Beh, H. E., & Mousa, H. M. (2020). Securing big data using mixed fragmentation based on multi-cloud environment. International Journal of Scientific & Technology Research, 9(3), 9–15.https://www.semanticscholar.org/paper/Securing-Big-Data-Using-Mixed-Fragmentation-Based-M.Nabawy-Beh/7bddaf844a0f08b543fc7ab9feee3af467e5536b
17. Castro-Medina, F., Rodríguez-Mazahua, L., López-Chau, A., Cervantes, J., Alor-Hernández, G., & Machorro-Cano, I. (2020). Application of dynamic fragmentation methods in multimedia databases: A review. Entropy, 22(12), 1352. https://doi.org/10.3390/e22121352
18. Farahani, B., & Monsefi, A. K. (2023). Smart and collaborative industrial IoT: A federated learning and data space approach. Digital Communications and Networks, 9(2), 436–447. https://doi.org/10.1016/j.dcan.2023.01.022
19. Alshudukhi, K. S. S., Ashfaq, F., Jhanjhi, N. Z., & Humayun, M. (2024). Blockchain-enabled federated learning for longitudinal emergency

care. IEEE Access, 12, 137284–137294. https://doi.org/10.1109/ACCESS.2024.3449550

20. Gollapalli, V. S. T. (2020). Enhancing disease stratification using federated learning and big data analytics in healthcare systems. International Journal of Management Research and Business Strategy, 10(4), 19–38.https://ijmrbs.net/index.php/ijmrbs/article/view/169
21. Rhayem, A., Mhiri, M. B. A., Drira, K., Tazi, S., & Gargouri, F. (2021). A semantic-enabled and context-aware monitoring system for the internet of medical things. Expert Systems, 38(2), e12629. https://doi.org/10.1111/exsy.12629
22. Nedunoori, V. (2025). A comprehensive review of encryption and protection techniques for healthcare data. In Artificial Intelligence in Healthcare Information Systems—Security and Privacy Challenges (pp. 147–170).https://doi.org/10.1007/978-3-031-84404-1_8
23. Rana, S. K., Rana, S. K., Nisar, K., Ag Ibrahim, A. A., Rana, A. K., Goyal, N., & Chawla, P. (2022). Blockchain technology and artificial intelligence-based decentralized access control model to enable secure interoperability for healthcare. Sustainability, 14(15), 9471. https://doi.org/10.3390/su14159471
24. Elkourdi, F., Wei, C., Xiao, L., Yu, Z., & Asan, O. (2024). Exploring current practices and challenges of HIPAA compliance in software engineering: Scoping review. IEEE Open Journal of Systems Engineering, 2, 94–104. https://doi.org/10.1109/OJSE.2024.3392691
25. Gulzar, C. M. (2025). Blockchain-enhanced HIPAA compliance framework for secure AWS health data. International Journal of Pharmacy with Medical Sciences, 5(4), 37–48. https://doi.org/10.64751/ijpams.2025.v5.n4.pp37-48
26. Singh, B., & Kaunert, C. (2024). Integration of cutting-edge technologies such as Internet of Things (IoT) and 5G in health monitoring systems: A comprehensive legal analysis and futuristic outcomes. GLS Law Journal, 6(1), 13–20.https://doi.org/10.69974/glslawjournal.v6i1.123
27. Javed, S., Ghazala, S., & Faseeha, U. (2020). Perspectives of heat stroke shield: An IoT-based solution for the detection and preliminary treatment of heat stroke. Engineering, Technology & Applied Science Research, 10(2), 5576–5580.https://doi.org/10.48084/etasr.3274
28. Son, T. W., Ramli, D. A., & Abd Aziz, A. (2021). Wearable heat stroke detection system in IoT-based environment. Procedia Computer Science, 192, 3686–3695.https://doi.org/10.1016/j.procs.2021.09.142
29. Karmani, V., Chandio, A. A., Karmani, P., Chandio, M., & Korejo, I. A. (2019). Towards self-aware heatstroke early-warning system based on healthcare IoT. In 2019 Third World Conference on Smart Trends in Systems Security and Sustainability (WorldS4) (pp. 59–63). IEEE.10.1109/WorldS4.2019.8904006
30. Wang, Y., Song, Q., Du, Y., Wang, J., Zhou, J., Du, Z., & Li, T. (2019). A random forest model to predict heatstroke occurrence for heatwave in China. Science of the Total Environment, 650, 3048–3053.https://doi.org/10.1016/j.scitotenv.2018.09.369
31. Hirano, Y., Kondo, Y., & Hifumi, T. (2021). Machine learning-based mortality prediction model for heat-related illness. Scientific Reports, 11, 9501. https://doi.org/10.1038/s41598-021-88581-1
32. Duggal, S., Kaur, P., Kumar, M., & Bhardwaj, V. (2025). IoT-enabled fog computing framework: Heat stroke risk analysis. Journal of Cloud Computing, 14(1), 51.https://doi.org/10.1186/s13677-025-00776-3
33. Mahmood, K., Khan, S., Abdelhaq, M., Hassan, M. U., Uddin, M., Alsaqour, R., et al. (2025). Adaptive resource-aware and privacy-preserving federated edge learning framework for real-time internet of medical things applications. Scientific Reports, 15(1), 36468.https://doi.org/10.1038/s41598-025-23398-w
34. Ahmed, F., Zhou, T., Bilal, H., Ul Islam, F., Ullah, R., & Vasilakos, A. V. (2025, October 15). Enhancing healthcare data integrity and access control using blockchain and Industry 5.0. IEEE Internet of Things Journal, 12(20), 43630–43643. https://doi.org/10.1109/JIOT.2025.3598320