e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 5, Issue 10, October 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 10, October 2022 |

| DOI:10.15680/IJMRSET.2022.0510003|

Cloud-Based IoT Healthcare System for Secure Data Management and Patient Monitoring

Gabriel Ayodeji Ogunmola[1]

Faculty of Management, Department of Business Administration, Sharda University

73 Boburshox kochasi, Andijan, Uzbekistan.

ABSTRACT: The increased use of internet-based devices has changed how monitoring happens in patient health- data on important health parameters. However, sensor faults and privacy data problems continue to affect the effectiveness of the Internet of Things (IoT) healthcare systems. The study aims is to develop an IoT-enabled cloud-based healthcare monitoring system for patient health tracking and data analysis. The proposed methodology includes data collection from IOT devices, outlier detection for pre-processing, data encryption with the use of Fernet along with secure cloud storage to provide an easy and secure healthcare monitoring system. The results show that Fernet encryption takes approximately 20 seconds for 5000 data points, significantly outperforming the existing method, which takes 80 seconds. Additionally, IoT device integration causes response times to increase from 300 ms at 25,000 devices to over 500 ms at 200,000 devices, The steady increase in security performance, rising from a value of 20 at stage 1 to 100 at stage 5, indicating significant improvements across performance stages, improve data reliability and privacy offering a comprehensive solution for effective healthcare data management.

KEYWORDS: Internet of Things, Healthcare, Fernet Encryption, Data Security and Cloud-based storage.

I. INTRODUCTION

Changing the landscape of many industries, cloud computing has provided scalable, flexible, and cost-effective solutions to those in need [1]. Cloud platforms for the healthcare domain allow the healthcare provider to store, process, and analyse large quantities of patient data without having to invest in expensive infrastructure [2]. This, in other words, refers to cloud computing; secure access to a plethora of information by healthcare systems also enhances the decision-making process and improves operational activities. The performance of the Quality of Service aware service selection architecture for healthcare IoT systems reported by Rama Krishna Mani Kanta Yalla (2021) [3] provides an important contribution to the optimization of service selection and decision-making, which will directly benefit cloud-based patient monitoring. Using cloud solutions, the healthcare institution can scale up or down based on demand while keeping the patient data safe and accessible across multiple locations. Quite an advantage for any healthcare data management in this digital age, indeed.

In addition, cloud computing in healthcare strengthens collaboration by providing data sharing across healthcare providers, thus enhancing communication and the provision of crucial information for decision-making [4]. By virtue of cloud platforms, multiple healthcare institutions and providers can collaborate by sharing patient data and medical record information in a secure manner. This helps reduce duplication of efforts and increases the quality of care, thus facilitating accurate diagnoses and personalized treatment plans [5].

One of the most data-heavy industries is healthcare; huge amounts of patient records, medical images, test results, and monitoring devices generate daily information. This presents an increasing urgency in the effective and secure management of this information [6]. The healthcare providers need to maintain data security with privacy compliance and regulations, all while improving quality of care and operational efficiency. The dynamic evolution of the healthcare industry is therefore relying heavily on the integration of technology solutions like cloud computing and IoT for better healthcare delivery and patient outcomes.

The IoT devices are very prominent in the healthcare field, ensuring continuous tracking and data collection. These devices, from wearable health trackers to sophisticated medical equipment, create health data points: heart rate, glucose, oxygen saturation, etc. By virtue of IoT devices, health providers can obtain accurate and up-to-date health information from patients, and hence make informed decisions and provide personalized care [7]. While these devices can generate huge volumes of data, working in tandem with cloud computing ensures efficient storage, processing, and analysis of this data. The integration of cloud-based technologies with healthcare through IoT devices provides

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 10, October 2022 |

| DOI:10.15680/IJMRSET.2022.0510003|

excellent solutions for the overall management of the patient data. With the secure transfer of data examined from IoT devices to the cloud, healthcare industries will be able to store massive amounts of data, free from all sorts of physical limitations. It allows clients access to their health information, with doctors able to access patient records anywhere across the globe. Cloud is available with big storage as well as advanced analytical capabilities to improve patient care, managing chronic conditions, and complete delivery of health services within a very high standard of data security and privacy.

Cloud computing, coupled with the IoT technologies in healthcare, offers the possibility of managing patient data in a scalable, secure, and efficient manner. Connected medical apparatuses and wearables measure heart rate, blood pressure, glucose level, and oxygen concentration, thus continuously gathering and streaming data into cloud-based platforms. Hence, there is no need for localized storage, and one can access the data centrally without being hampered with the limitations of any physical infrastructure [8]. Full patient documentation is available anywhere for health-service providers to make informed decisions and coordinate intelligently across departments. With all this data, continuity of care is ensured from an operational perspective. Patients, on the other hand, are given greater access to their health records, which allows them to take responsibility for monitoring their own health. The Cloud now handles that transformation with virtually boundless storage and advanced analytical tools that assist healthcare organizations in processing composite datasets rapidly. By trends, track patient history, and predictive analytics, cloud-enabled systems migrate toward more individualized and further proactive healthcare delivery, especially in chronic case management and massive patient records. The integration of AI and Big Data facilitates customized learning in music education and can equally be used in healthcare systems to provide personalized patient care through IoT device data analysis, as indicated by Basava Ramanjaneyulu Gudivaka (2021) [9].

The organization of the paper is as follows: A literature review concerning the IoT healthcare system, security challenges, and cloud computing integration is discussed in Section 2. The proposed methodology is explained in detail in Section 3. Section 4 discusses the results and analysis. Lastly, the paper concludes in Section 5.

II. LITERATURE SURVEY

Cloud computing has undergone a rapid transformation from what began as internetwork service capability for ISPS to a public service which has been widely embraced by all major companies, large institutions, and most government organizations [10]. Key milestones in this journey are the core papers by Google in 2003, followed by the establishment of their commercial service through Amazon EC2 in 2006. Today, not only does cloud computing serve the intended purpose of cost savings, but also serves as a source of revenue. This paper delves into its concept, history, advantages, disadvantages, value chain, and standardization efforts that have been made over time. The IIoT has resulted in massive data that cannot depend on local storage on IIoT devices with energy and storage restrictions. To solve this problem, self-organization and short-range IoT networking help facilitate data outsourcing to cloud computing from device constraints. This research focuses on hitches and computing techniques that make IoT integrated with cloud computing in a seamless manner, underlining the efficiency of cloud solutions and emerging data storage styles.

The usage of cloud computing technology in organizations by case study approach for an understanding of innovative developments and salient features of this technology [11]. In addition to the above, it also discusses the challenges like cybersecurity, intrusion detection and prevention, and future directions for research pertaining to the cloud adoption challenges in business settings. The PCT, point cloud transformer, is a new framework for point cloud learning by employing a transformation architecture to cope with issues caused by the irregular and absent order characteristics of the point cloud data. PCT allows processing sequences of points, being permutation invariant, and augments local context capture by means of farthest point sampling as well as nearest neighbour search. Additionally, one of the problems of PCT is that, while it attains state-of-the-art results with regard to shape classification as well as segmentation tasks, it is a computationally complex process and might be difficult to scale to larger point cloud datasets.

For businesses and individuals, cloud computing has become crucial and readily acceptable since 2019 due to the low cost and on-demand mindset. Nevertheless, security remains a serious concern, which was especially clear in the year 2020, with a vulnerability presented in all three-layer levels of security: IaaS, PaaS, and SaaS. This research attempts to characterize cloud security status over the last 10 years; notwithstanding, there is a limitation arising from the fast-emerging technology of the cloud and the challenges that emerge in addressing increasing security threats with time. The current systematic review is an eye-opener for IoT-based health care systems that have been analysed in and

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 10, October 2022 |

| DOI:10.15680/IJMRSET.2022.0510003|

around their architecture, performance, and data management especially during health monitoring and disease prediction for the elderly care [12]. However, the greater emphasis of the study has been on the efficiency of IoT in symptom detection and disease prediction, which show other major drawbacks such as high-power consumption, resource starvation, and security issues owing to multiple devices used, all these affecting severely the whole performance and sustainability of IoT health care systems solution.

Various IoT devices such as smartwatches and health-monitoring bracelets; for example, in healthcare using to track the physiological signals and improve the remote health monitoring. The IoT healthcare market continues to grow tremendously with some of the significant issues such as privacy concerns, security risks, and the effects of health data information shared by individuals in their actions critical. Contemporary strategies have been advanced within the paper to address these issues [13]; however, the challenges include the security of IoT devices and gaining users' trust in assuring that their data is protected.

Critical examination of IoT healthcare platform limitations focuses on resource constraints and interoperability issues among commercial systems, especially in India, where the doctor-patient ratio is low. The study focuses on the promise of IoT for improvement in delivery of care, yet it mentions barriers such as limitations in device resources and a lack of communication between proprietary platforms [14]. Though the paper proposes enhancements for IoT healthcare, it is constrained by issues yet to be standardized-communication protocols-as well as the effective integration of heterogeneous healthcare platforms.

III. PROBLEM STATEMENT

These IoT devices, capable of merging with and making healthcare monitoring, primarily present limitations such as hardly working with power supply, CPU, memory, and bandwidth requirements, all of which hinders the emergence of advanced applications in healthcare. Furthermore, due to the unstandardized communication protocols between diverse proprietary platforms having various architectures, a considerable challenge thereby arises in integrating and sharing data among healthcare systems, lessening the effectiveness of IoT solutions to better healthcare delivery [15]. Furthermore, the absence of uniform communication protocols for different proprietary systems with different architectures poses enormous hurdles to data integration and interoperability. This lack of uniformity in system communications leads to challenges in sharing and retrieving healthcare information across systems, weakening the overall performance of IoT solutions in enhancing healthcare delivery. Therefore, the smooth embedding of IoT into healthcare systems continues to be a significant challenge, restricting the possibility of taking advantage of the complete range of data-driven insights to inform patient care and operational optimization.

To overcome the challenges of IoT devices in healthcare including power, CPU, memory, and bandwidth constraints, as well as the problem caused by unstandardized communication protocols, the envisioned Cloud-Based IoT Healthcare System for Secure Data Management and Patient Monitoring provides a strong solution. By using the cloud infrastructure, the system handles resource limitation by offshoring the data processing and storage such that the IoT devices are not burdened by computationally intensive work. Sharadha Kodadi (2021) demonstrated how Markov Decision Processes can be used to plan deployment alternatives based on non-functional aspects. This approach can be adapted for healthcare systems to achieve optimal deployment of IoT devices, and proves to be a helpful strategy for enhancing efficiency, reliability, and overall system performance in healthcare applications [16]. Further, the cloud platform of the system is interoperable with other health information systems over standardized communication protocols so that patient data is shared efficiently and patient monitoring is done. This ensures that sensitive healthcare data are securely handled, whereas enhancing the interoperability of IoT devices, leading to improved patient care quality and efficient health operations [17].

3.1 OBJECTIVES

The goal is to create an efficient, safe, and scalable IoT health system in the cloud to facilitate integration, data management, monitoring of health indicators of patients, privacy through encryption, and full optimization [18].

- Build a cloud-based IoT health system to ensure safe management of patient health data and to assess monitoring of health indicators.
- Acquisition of health-related data through potentially IoT sensors such as wearables, or through health monitoring systems for continual health surveillance.
- Apply outlier detection methods to purge the data, removing any false venting that could occur due to sensor failures or transmission errors.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 10, October 2022 |

| DOI:10.15680/IJMRSET.2022.0510003|

- Protect the health data from potential breaches with Fernet encryption to protect the confidentiality and integrity of the sensitive health data before it enters the cloud.
- Monitor the performance and scalability of the system (e.g., response time, data transfer, and encryption) for future optimization of the system. The combination of K-Means and Hierarchical Clustering, as pointed out by Rajeswaran Ayyadurai (2021) [19], results in improved accuracy in recommendations, hence contributing directly to the optimization and data management objectives in cloud-based healthcare systems for IoT.

IV. METHODOLOGY

The depicted workflow showcases a structured approach of managing IoT healthcare data, beginning with the collection of vital health metrics from IoT devices. followed by outlier detection and deletion stages to ensure that any error caused due to sensor malfunction is removed completely. Such data is then subject to an encryption process using Fernet encryption so that it keeps data safe regarding storage and further use while ensuring patient privacy. Finally, encrypted data is then uploaded to the cloud for easy management and retrieval while performance metrics run continuously to assess whether the whole system is performing effectively and reliably or not.

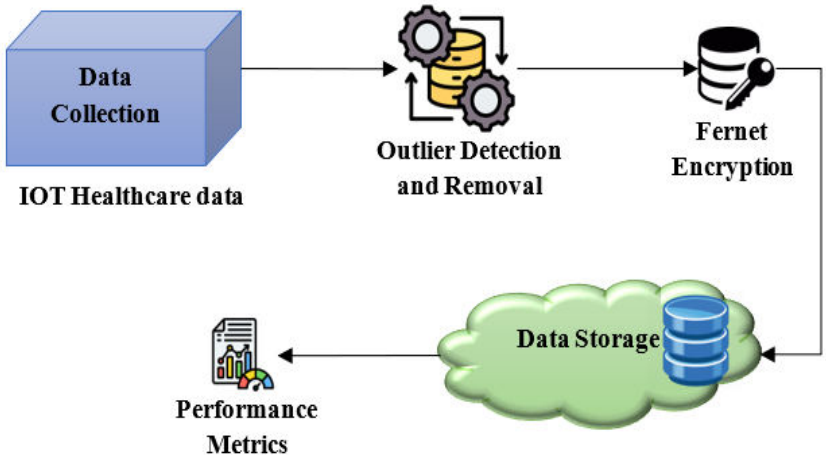

Figure 1: IoT Healthcare Data Management and Security

4.1. Data Collection

Data gathering entails acquiring healthcare data by means of IoT devices such as wearable health monitors, medical sensors, and patient monitoring systems. These capture readings of vital health parameters such as heart rate, blood pressure, glucose levels, etc [20]. The data collected form the basis of further analysis; hence, assessment of patient health is also very important in the provision of timely interventions. In processing the data, outlier detection and encryption are among the measures that enhance privacy and correctness prior to being transferred and stored for future analysis.

4.2. Data Pre-processing using Outlier Detection

Reprovisioning is needed for health care information before it can be analyzed or stored. This is to optimize the accuracy and quality of IoT based data. Raw data points will often reflect error caused by noisy sensors, transmission errors or sensor malfunctioning. Outlier detection is a basic preprocessing task that identifies uncommon data points outside normal physiological value ranges [21]. Outliers may be distribution errors or true health issues. In either case removing outliers will enhance the quality of the base data to avoid unsafe or misleading conclusions. These techniques also preserve patient anonymity by not including data from surcharge inputs in the sensitive models. Also, for machine learning models to learn well and provide better predictions they require clean data. Therefore, good outlier detection will improve the performance of the system and ultimately, clinical decision making. Machine learning enhances strategic capabilities, as highlighted by Mohan Reddy Sareddy (2021) [22], experts are still needed, just like medical practitioners interpret ML-processed information for proper decisions following strong data pre-processing.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 10, October 2022 |

| DOI:10.15680/IJMRSET.2022.0510003|

4.2.1 Statistical Methods for Outlier Detection

The Z-Score method is a statistical method for detecting outliers in data sets that are normally distributed. It calculates how far a specific data point is from the mean of the whole data set in standard deviations a data spread measure. For example, a sudden spike in heart rate or an abnormal glucose level reading caused by sensor errors might mislead healthcare providers and cause incorrect diagnosis or intervention is given in equation (1).

$$Z = \frac{X-\mu}{\sigma} \tag{1}$$

Were, X is the data point, μ is the mean of the dataset, σ is the standard deviation of the dataset. The primary rationale behind using the Z-Score approach is maintaining precision and dependability of the system by identifying automatically and discarding erroneous or unusual readings. The outliers might occur due to fleeting device malfunctioning, sensor bad contact, subject movement, or even valid but uncommon clinical incidents. Early detection of such anomalies can help healthcare systems prevent false alarms, improve the accuracy of predictive models, and initiate interventions when needed. In addition, this approach keeps data integrity intact prior to applying it to downstream processes such as anomaly detection, health forecasting, or decision-making support. Although easy and computationally lightweight, the Z-Score process makes the assumption of normally distributed data, making it optimal under that condition.

4.2.2 Interquartile Range (IQR)

Data points with a Z-score greater than 3 or less than -3 are flagged as outliers and removed. Alternatively, the IQR method defines outliers as those data points that fall outside the range of the first quartile (Q_1) and third quartile (Q_3) by more than a defined multiplier and is given in equation (2).

$$\text{Lower Bound} = Q_1 - 1.5 \times \text{IQR}, \ \text{Upper Bound} = Q_3 + 1.5 \times \text{IQR} \tag{2}$$

Were $\text{IQR} = Q_3 - Q_1$ represents the interquartile range. Data points falling outside the lower and upper bounds are considered outliers. The primary use of the IQR approach is to sanitize the data by removing outlier values that may mislead subsequent processes such as anomaly detection or predictive analytics [23]. It helps to ensure that machine learning model training data or patient alert data used is both reliable and characteristic of actual conditions. Since it does not depend on data distribution assumptions, the IQR method is very versatile, simple to calculate, and extremely effective in health monitoring systems where data variation is typical.

4.3 Data Validation and Transformation

Once outliers are detected in the healthcare IoT dataset, the next most crucial step is data validation and transformation to have a clean, consistent, and analyzable dataset. Outlier values are checked with utmost care—if clearly in error, they are rejected; otherwise, they are restored through imputation techniques. These could be replaced with the mean or median of neighboring values, linear interpolation to maintain integrity in time series, or even KNN imputation to estimate missing values or corrupted values using the values in the neighborhood and the relationships among similar data. It is important to do this to avoid bias to model in the future, and allow the data to reflect a true physiological condition.

4.3.1 Normalization and Scaling

Scaling and Normalization are important stages in data preprocessing to prevent dissimilar units or scales of value from highly influencing machine learning algorithms. In healthcare IoT, for instance, physiological parameters such as heart rate and blood glucose typically have different ranges of orders of magnitude: heart rate in bpm ranging from 60 bpm to 100 bpm, while blood glucose ranges from 70 mg/dL to 180 mg/dL. Without normalization, attributes with a higher range (such as glucose) might take over the learning process, producing biased models [24]. Normalization with Min-Max scaling scales such attributes to a similar range, say [0,1], by converting each value according to its minimum and maximum values in the dataset. This makes all attributes contribute equally to the analysis, enhancing the performance of the model. For a specific feature x, is given below in equation. (3),

$$x' = \frac{x-\min(x)}{\max(x)-\min(x)} \tag{3}$$

where x ′ is the normalized value, min(x) and max(x) are the feature's minimum and maximum values, respectively. Normalization maintains the relative differences between the values and removes scale-related biases by

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 10, October 2022 |

| DOI:10.15680/IJMRSET.2022.0510003|

rescaling the data. Standardization, another scaling procedure, is applied when data is normally distributed, scaling values so they have a mean of 0 and a standard deviation of 1 so that the data will satisfy the assumptions of most machine learning algorithms. Swapna Narla et al. (2021) guided the proposed work by demonstrating effective hybrid model integration and cloud-based preprocessing, directly influencing data quality enhancement and predictive trust in smart healthcare monitoring [25].

4.3. Data Encryption using Fernet

After the pre-processed healthcare data has been subjected to processes like outlier removal, validation, and normalization, encryption is required to ensure secure transmission and storage of sensitive patient information collected via IoT devices. Fernet encryption, a robust symmetric cryptographic algorithm, serves this purpose by employing the AES in CBC mode to ensure data confidentiality. It contains a HMAC for integrity and tamper resistance, and Base64 encoding provides secure transmission of binary data in text format [26]. The use of encryption and verification processes together provides assurance that the data can only be accessed by authorized users having the proper decryption key, supporting privacy standards compliance such as HIPAA or GDPR and creating trust in smart healthcare infrastructures.

4.3.1 Fernet Encryption

Data that are pre-processed by Outlier's detection are encrypted using Fernet encryption, data confidentiality and security regarding healthcare information gathered from IOT devices are assured using the Fernet encryption mechanism. Fernet employs symmetric key encryption using AES (Advanced Encryption Standard) in CBC (Cipher Block Chaining) method for encrypting the data content and integrity. The encryption process can be defined as described in Eq. (3).

$$C = E_K(M) = AES_K(M \oplus IV) \quad (3)$$

Were, C is the ciphertext, E_K is the encryption with key K, M is the plaintext message, and IV is the initialization vector, $\oplus$ denotes bitwise XOR operation used in CBC mode. This guarantees that only those persons can access sensitive health data in the cloud as per their definition, who have a legitimate decryption key.

4.3.2 Integrity Assurance with HMAC

After encrypting the pre-processed health data using AES in CBC mode, Fernet also secures the data by constructing a Hash-based Message Authentication Code (HMAC) to ensure the integrity and authenticity of the ciphertext while it is being sent or stored. The cryptographic hash serves as a confirmation mechanism that identifies any unauthorized changes to the encrypted information prior to decryption. The HMAC is calculated based on a derived key K', which is different from the underlying encryption key K, to provide key separation from encryption and authentication functions. The HMAC computation adheres to the formula is given below in equation (4),

$$H = HMAC_{K'}(C) \quad (4)$$

Where: H is the calculated HMAC (hash-based message authentication code), K' is the derived key particularly for use in the HMAC function (not borrowed from encryption), C is the ciphertext produced during the AES encryption phase. By adding this HMAC to the ciphertext, Fernet ensures that the receiver is able to verify whether the data remains unaltered. If transmission modifies even one bit of ciphertext, HMAC validation would be inconceivable and decryption would never take place, alerting the possibility of tampering. It is especially significant in healthcare IoT systems where integrity of transmitted medical information directly supports diagnosis and treatment of patients [27].

4.3.3 Fernet Token Structure

After completing the pre- processing and encryption steps, the final step in Fernet encryption is creating a valid Fernet token to securely transfer and store in cloud systems. The token is sent by concatenating three important variables: the initialization vector (IV), ciphertext (C), and HMAC (H) then Base64 encoded to ensure interoperability between communication protocols. Mathematically, denote the structure as equation (5),

$$Token = Base64(IV \| C \| H) \quad (5)$$

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 10, October 2022 |

| DOI:10.15680/IJMRSET.2022.0510003|

Here, $C = E_K(M) = AES_K(M \oplus IV)$ is ciphertext resulting from encrypting plaintext message M with symmetric key K by AES in CBC mode and initialization vector IV. K′ (C) is the hash-based message authentication code derived by using an independent HMAC key K ′, on the ciphertext $H = HMAC_{K'}(C)$, preserving integrity and authenticity. The integration of these essential elements of encryption and authentication, ensures that the only authorized people who possess keys are able to read and authenticate the health data as well as determine if the data has changed in transmission before decrypting it. In this way, the system preserves data confidentiality, and all three aspects of privacy are preserved throughout the health data throughout secure healthcare IoT systems. The post-quantum cryptography and optimization integration by Bhavya Kadiyala and Harleen Kaur (2021) [28] affirms the proposed work's Fernet-based encryption strategy, providing secure IoT healthcare data sharing and token-based transmission.

4.4. Data Storage

A secure healthcare IoT system is storage. Data storage of de-duplicated patient data that has been pre-processed and encrypted, may be kept within a cloud-based platform to ensure confidentiality, reliability, & scalability. Cloud platforms are made to manage data confidentiality & integrity, ensuring that unauthorized personnel may not access patient records, maintaining patients' private information securely encrypted. The healthcare IoT system retains sensitive records but allows us to manage what healthcare professionals can view through the appropriate decryption key access. The storage systems are cloud-based ensuring that health data will continue to be collected at scale to keep up with the flow of health data record inflows from health monitoring devices that utilize portable wearables. Even if cloud storage accesses should get interrupted, access to patient data is made possible by redundancy and high availability in cloud services, which survive outages due to hardware failures or regular maintenance. Moreover, cloud systems enable secure relocated retrieval of the records to support timely interventions and uninterrupted monitoring of patients, whilst also maintaining the integrity of the health record. Cloud storage can bereave patients of their health information through automated backup and disaster recovery to prevent de-identified or identifiable health records from accidental deletion & ensure the historical access to a patient's health record remains informed. Thusly, combining next-level cybersecurity models, elastic resource management and compliance management (e.g. HIPAA, GDPR), provides the digital backbone to integrate intelligent healthcare services.

4.4.1 Secure Data Transmission and Ingestion

In a connected healthcare ecosystem, the transmission and ingestion of data are critical to confirm sensitive healthcare data from IoT devices reaches the cloud without compromise. After data is encrypted with Fernet, data is transmitted over secure communication protocols such as HTTPS or TLS that protect the data from interception, eavesdropping, or man-in-the-middle attacks. Once at the cloud infrastructure the data goes through authentication using the HMAC embedded in the encrypted Fernet token to verify it has not been tampered with during transit. Only after successful verification is the data routed into secure, healthcare compliant storage environments such as HIPAA aligned cloud buckets, safe vaults, or encrypted databases [29]. The storage environments are controlled for access to maintain that only authorized users are able to interact with the data. Finally, the ingested data is indexed using its metadata attributes including timestamps, patient identifiers, and sensor types, which provides efficient organization, quick query capability, and simplified retrieval that supports decision making and longer-term health analytics. Overall, this multi-faceted approach to privacy, confidentiality, identity verification, authenticity, and availability offers overall confidence in data security from end-to-end from IoT device to the cloud.

4.4.2 Scalability and Elastic Resource Allocation

Amazon Web Services offers high scalability and elastic resource allocation in a cloud platform that can meet the rigorous limitations of health data management. AWS provides the elastic, scalable, secure data storage infrastructure necessary for health data management, particularly through services like Amazon S3 and AWS Auto Scaling. Consider the following example: as wearables present an evolving and potentially limitless and unpredictable source of health data, a range of vital signs are consistently being captured from the sensor. Hence, the amount of data can change without any warning whatsoever. Not only can AWS S3 scale the amount of storage available automatically, with no downtime or administrator involvement, data can flow in, regardless of scale. AWS also allows for AWS Lambda (serverless) and EC2 instances (that utilize AWS Security Groups) to dynamically allocate compute resources that can be used to process incoming encrypted data [30]. In addition, AWS allows secure data transfer protocols, encryption for stored data and data in transfer, and compliance with compliance requirements for healthcare data (HIPAA, GDPR). This elasticity means less operational overhead and infrastructure costs for healthcare providers, while ensuring an uninterrupted supply of patient data for clinicians. In scenarios involving random and unexpected fluctuations in available data and demands, such as catastrophe events or sudden demand spikes, data gets stabilized. The redundant compliance systems in AWS that are scalable guarantee compliance with high availability and durability in patient information, and allowed users can easily and in time access and review files remotely, making timely and

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 10, October 2022 |

| DOI:10.15680/IJMRSET.2022.0510003|

accurate diagnoses possible in addition to individualized patient care. Rajababu Budda (2021) work on elastic resource allocation and scalable, secure cloud storage directly supports the proposed framework by enabling dynamic handling of unpredictable, large-scale health data streams with minimal overhead and ensured data privacy [31].

4.4.3 High Availability and Redundancy

Redundancy and high availability are inherent principles of cloud healthcare data management that make it possible to fetch patient data near even in case of technical failure. Major platforms such as AWS, Microsoft Azure, and Google Cloud Platform utilize data centers geographically distributed like multiple data centers located in different regions of the United States, Canada, Europe, and Asia to replicate healthcare data in different places. This geographical redundancy results in the event that one of the data centers fails as a result of earthquake, flood, cyber-attack, or hardware failure, that there is a ready back-up or recovery zone that can seamlessly take over the service with negligible data loss in the event. Moreover, load balancing algorithms divert incoming requests and store operations intelligently to numerous servers such that no single server is overburdened and performance never degrades due to a specific node. This becomes extremely significant in a crisis situation when hospital units could be completely occupied. In addition, auto-healing capabilities like the Amazon EC2 Auto Recovery and Azure's Virtual Machine Scale Sets, always monitor system health and can autonomously replace or restart affected or faulty instances or storage nodes without human intervention. This fault-tolerant intelligence can significantly reduce negligence mitigation, which minimises downtime if something should happen. People in healthcare can be certain that they are consistently getting access to the right patient information, which matters for diagnosis, monitoring, or treatment recommendations. High availability architectures allow health systems to do more than simply meet compliance regulations, such as protecting health information (PHI) to comply with HIPAA regulations. Finally, when failover happens, intelligent workload distribution, follow on work, and auto-recovery allows cloud service providers to provide service delivery reliability and trustworthiness expected for providing care in life-threatening instances of care in smart healthcare today.

4.4.4 Role-Based Access and Audit Trails

RBAC and comprehensive audit trails are key to protecting data confidentiality, integrity and accountability in cloud-based healthcare systems. RBAC ensures that every healthcare worker physician, nurse, lab technician, system administrator, or other authorized personnel accesses only that data and system functionality necessary to perform their assigned responsibilities. For example, a general practitioner may view only basic patient health metrics, while a treating specialist may view detailed diagnostic reports. Limiting what data users can access increases the possibility that they will not see information they should not view [32]. To further protect these entry points, MFA can be used, requiring users to confirm their identities through multiple modalities. Other token-based authorization systems apply time-limited, scoped access to sensitive data. RBAC and MFA and other controls generate audit trails, which are written automatically and kept in a secure location that log each event of access, data modification, and administrative event. Functions of audit trails include: identifying potential security breaches; verifying compliance with federated legal standards such as HIPAA and GDPR and; supporting forensic investigations through documented events of system activity in a sequential manner. In high-pressure and potentially life-threatening healthcare environments, these types of safeguards not only protect against insider threats and misuse of data, but also help build trust among stakeholders in transparency, accountability, and adherence to governability.

4.4.5 Backup and Disaster Recovery

Backup and Disaster Recovery solutions on cloud platforms are a foundational part of a robust healthcare IoT ecosystem, so that sensitive patient information will be safeguarded in cases of any unforeseen disaster or disruption. Major cloud platforms such as AWS, Microsoft Azure, and Google Cloud provide built-in capabilities for automatic backup, image and snapshotting, and geo-restricted replication, all of which protect patients from accidental deletions, software corruption, hardware failure, and cyberattacks. For example, AWS backup and Azure Backups help healthcare organizations implement policies that automate patient data with respect to regular backups, implement version control restore against historical patient records, and implement multiple restoration scenarios based on clinical need [33]. Also, point-in-time snapshots and geo-redundant replication allow fast disaster recovery by quickly rolling back the most recent valid data to another availability zone or region. This enables the longest realized uptime of services and preserves continuity of care quickly. Also, these types of platforms allow for a compliance-ready strategy for data retention strategies. Patient health records can be accurately and safely archived and stored for legally directed timeframes according to either HIPAA, GDPR, or local data protection regulations. Data access controls also maintain data integrity and confidentiality by making sure that backup restoration and deletion privileges are limited to individuals with administrative access. Overall, robust backup and disaster recovery programs can create a cloud storage layer that can lend intelligence and reasonable availability to a new high-value asset dedicated to compliance,

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 10, October 2022 |

| DOI:10.15680/IJMRSET.2022.0510003|

continuity of care, and trust for long-term healthcare delivery. Emphasizing both scalable cloud deployment and anomaly discovery Venkat Garikipati et al. (2021) [34] reinforce the proposed model for safe storage architectures, automatic recovery mechanisms, and also promotes the efficient practice for the management of IoT data in healthcare.

- Encrypted health data will be sent over an encrypted channel, processed, and made available in a cloud database, where the purpose is to keep sensitive patient information away from prying eyes while still giving access to authorized healthcare professionals.
- Cloud storage lends itself to provide scalable solutions to healthcare providers and can increase or decrease the storage space needed at a pace suitable for their needs, within the limits of betraying physical infrastructure [35]. As per best practices, once data volume has increased, the storage system should accommodate the influx of continuously updating data generated from IoT devices without compromising performance.
- One of the basic features of cloud platforms is that they provide high availability and redundancy features, which allow for quick access to healthcare data, even in the unlikely event of hardware failure or downtime. This characteristic is very crucial for any healthcare system that relies on constant data access to monitor events and support well-timed decisions.
- In this way it'd give quick retrieval of encrypted data from cloud storage with the right network to authorized personnel. Such secure handling gives healthcare providers access to patients' records and health metrics from anywhere, thus instituting timely interventions and personalized care.
- Cloud platforms also provide strong backup system support against loss of data through accidental deletions or system failures [36]. Automatic backups ensure patient health data files are intact, and the healthcare provider can retrieve the data whenever necessary for the ongoing monitoring of patients and to make informed decisions.

V. RESULTS AND DISCUSSION

The evaluation for encryption strength has been set under the results heading for safeguarding the confidentiality and security of healthcare data. Assessment of seamless communication and efficient data transmission between IoT devices and the system under examination [37]. With regard to throughput assessment-another parameter ensuring the capacity for the system to process and sharply handle a bunch of data, ensuring fluidity of operations and minimal delays within the process of health care-monitoring [38].

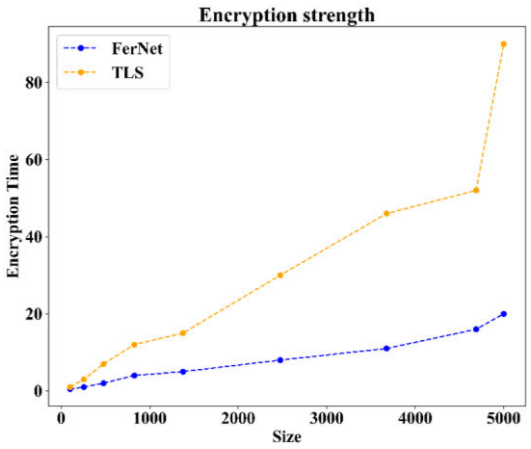

Figure 2: Fernet Encryption strength Analysis

Figure 2 compares the time to encrypt the data using Fernet encryption against an existing encryption method across different data sizes from 0 to 5000. From a few bytes to a few bytes, the time taken in encrypting increases with an increase in size with both these methods, but Fernet does that comparatively at a slower rate. For instance, at 5000 sizes, encryption using the method Fernet, takes about 20 seconds, and the existing method shoots up to almost 80 seconds. Hence, the higher efficiency of this method relates with the time taken by the growing data size in encrypted and steeper slope from its increase. Low-latency anomaly detection adopt structured cloud traffic and fast encryption corresponds to proposed system design, backed by Tab-Transformer based healthcare data security models influenced from Venkata Sivakumar Musam et al.(2021) [39].

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 10, October 2022 |

| DOI:10.15680/IJMRSET.2022.0510003|

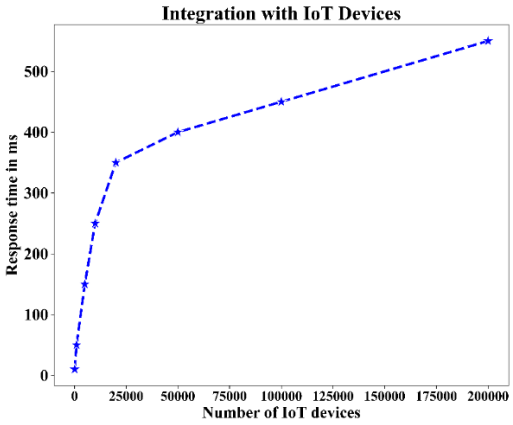

Figure 3: Integration with IoT Devices

Figure 3 indicates how the number of IoT devices and response time in milliseconds (ms) correlate an increase in IoT devices causes a significant increase in response time, appearing as an apparent exponential function [40]. Approximately 25,000 IoT devices, the response time comes in at 300 ms, whereas at 200,000 devices and above, the response time is definitely above 500 ms. This shows that the system is experiencing latency with IoT devices and indicates that there may be challenges when scaling up in larger IoT ecosystems.

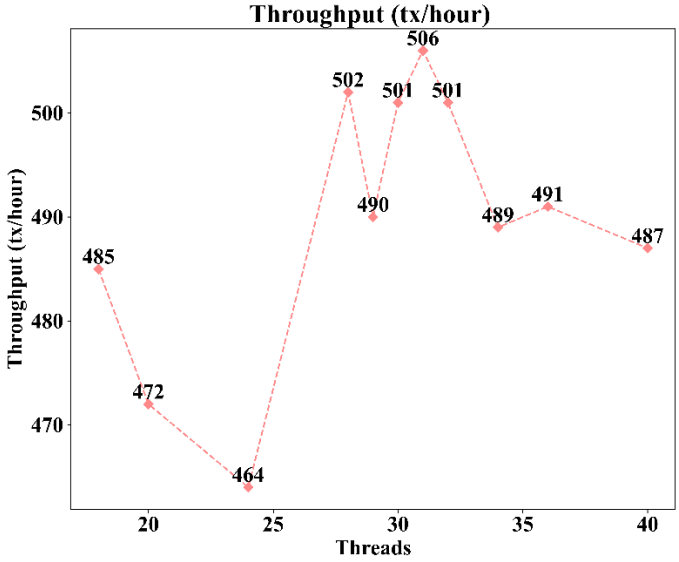

Figure 4: Throughput Performance Analysis for IoT Healthcare Data Processing

Figure 4 shows throughput as a function with respect to the number of threads used [41]. It indicates that the throughput rises with the number of threads to a maximum point, which occurs at 30 threads, and the maximum throughput is recorded at 506 tx/hour. Beyond the point of 30 threads, an increase in the number of threads shows a minor decline in the throughput to a steady level of approximately 487 tx/hour at 40 threads. This illustrates that more threads initially increase throughput, but there seems to be an optimal number, over which additional threads do not increase throughput significantly, or may slightly reduce it. Similar to results pointed by Winner Pulakhandam et. al (2021) [42], where encrypted data systems exhibit optimal throughput when concurrency can be carefully balanced within secure, privacy-preserving healthcare cloud frameworks.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 10, October 2022 |

| DOI:10.15680/IJMRSET.2022.0510003|

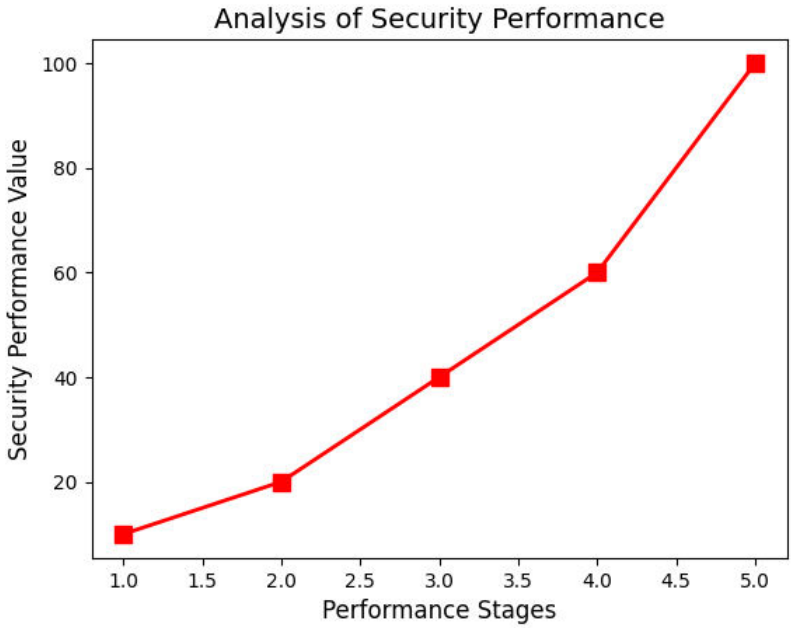

Figure 5: Security Performance Improvement Across Stages

Figure 5 indicates performance in the aspect of security at different stages ranging stage one to stage five. The performance increases, ranging from stage one, stage two, stage three, stage four, to stage five. At stage one, security performance is about 20, then rises to reach 100 at the last stage, indicating a clear positive trend in security performance. This shows that as the system goes through stages, the measure of effectiveness in its security increases. It could be due to better measures being introduced or optimizations made at each stage. The graph thus indicates the increase in security performance with the progression of stage.

VI. CONCLUSION

This research demonstrate how effective IoT applications are for healthcare data management: data collection, outlier detection, encryption, and storage on cloud environments. The research results reflect an efficient and fast implementation of the Fernet encryption mechanism, taking about 20 seconds to encrypt 5,000 points of data against 80 seconds reported for existing methods. This shows a significant advancement in performance. Whereas in reality, as integration with IoT devices increased, response times were seen to increase too, with a significant jump from 300 ms at 25,000 devices to over 500 ms at 200,000 devices. The throughput results also revealed that with various numbers of enabled threads, the system performs it's best when set to 30 threads, with peak performance at 506 tx/hour; beyond that, the performance began to decline slightly. Future work could scale up the integration of IoT devices so that they effectively manage bigger-sized networks; improvements could also be made in the encryption to reduce the processing time still further, primarily on the larger set of datasets.

REFERENCES

[1] S. Sharma, K. Chen, and A. Sheth, "Towards Practical Privacy-Preserving Analytics for IoT and Cloud-Based Healthcare Systems," IEEE Internet Comput., 2018.

[2] A. R. Nasser et al., "IoT and Cloud Computing in Health-Care: A New Wearable Device and Cloud-Based Deep Learning Algorithm for Monitoring of Diabetes," Electronics, vol. 10, no. 21, p. 2719, Nov. 2021, doi: 10.3390/electronics10212719.

[3] Yalla, R. K. M. K. (2021). Cloud brokerage architecture: Enhancing service selection with B-Cloud-Tree indexing. Journal of Current Science, 9(2).

[4] A. Goyal, H. S. Kanyal, S. Kaushik, and R. Khan, "IoT based cloud network for smart health care using optimization algorithm," Inform. Med. Unlocked, vol. 27, p. 100792, 2021, doi: 10.1016/j.imu.2021.100792.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 10, October 2022 |

| DOI:10.15680/IJMRSET.2022.0510003|

[5] M. Masud, G. S. Gaba, K. Choudhary, R. Alroobaea, and M. S. Hossain, "A robust and lightweight secure access scheme for cloud based E-healthcare services," Peer--Peer Netw. Appl., vol. 14, no. 5, pp. 3043–3057, Sep. 2021, doi: 10.1007/s12083-021-01162-x.

[6] T.-Y. Wu, L. Yang, J.-N. Luo, and J. Ming-Tai Wu, "A Provably Secure Authentication and Key Agreement Protocol in Cloud-Based Smart Healthcare Environments," Secur. Commun. Netw., vol. 2021, pp. 1–15, Sep. 2021, doi: 10.1155/2021/2299632.

[7] H. B. Aziz, S. Sharmin, and T. Ahammad, "Cloud Based Remote Healthcare Monitoring System Using IoT," in 2019 International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh: IEEE, Dec. 2019, pp. 1–5. doi: 10.1109/STI47673.2019.9068029.

[8] P. Verma and S. K. Sood, "Cloud-centric IoT based disease diagnosis healthcare framework," J. Parallel Distrib. Comput., vol. 116, pp. 27–38, Jun. 2018, doi: 10.1016/j.jpdc.2017.11.018.

[9] Gudivaka, B. R. (2021). Designing AI-assisted music teaching with big data analysis. Current Science & Humanities, 9(4), 1–14.

[10] J. Balicki, "Many-Objective Quantum-Inspired Particle Swarm Optimization Algorithm for Placement of Virtual Machines in Smart Computing Cloud," Entropy, vol. 24, no. 1, p. 58, Dec. 2021, doi: 10.3390/e24010058.

[11] Suganthi, S., Gupta, V., Sisaudia, V., & Poongodi, T. (2021). Data Analytics in Healthcare Systems–Principles, Challenges, and Applications. Machine Learning and Analytics in Healthcare Systems, 1-22.

[12] B. Abd-El-Atty, A. M. Iliyasu, H. Alaskar, and A. A. Abd El-Latif, "A Robust Quasi-Quantum Walks-based Steganography Protocol for Secure Transmission of Images on Cloud-based E-healthcare Platforms," Sensors, vol. 20, no. 11, p. 3108, May 2020, doi: 10.3390/s20113108.

[13] C. Feng, M. Adnan, A. Ahmad, A. Ullah, and H. U. Khan, "Towards Energy-Efficient Framework for IoT Big Data Healthcare Solutions," Sci. Program., vol. 2020, pp. 1–9, Jun. 2020, doi: 10.1155/2020/7063681.

[14] M. Uppal, D. Gupta, S. Juneja, G. Dhiman, and S. Kautish, "Cloud-Based Fault Prediction Using IoT in Office Automation for Improvisation of Health of Employees," J. Healthc. Eng., vol. 2021, pp. 1–13, Nov. 2021, doi: 10.1155/2021/8106467.

[15] A. R. G. Yallamelli and M. V. Devarajan, "HYBRID EDGE-AI AND CLOUDLET-DRIVEN IOT FRAMEWORK FOR REAL-TIME HEALTHCARE," Int. J. Comput. Sci. Eng. Tech., vol. 7, no. 1, 2021.

[16] Kodadi, S. (2021). Optimizing Software Development in the Cloud: Formal QoS and Deployment Verification Using Probabilistic Methods. Current Science & Humanities, 9(3), 24-40.

[17] P. E. Idoga, M. Toycan, H. Nadiri, and E. Celebi, "Factors Affecting the Successful Adoption of e-Health Cloud Based Health System From Healthcare Consumers' Perspective," IEEE Access, vol. 6, pp. 71216–71228, 2018, doi: 10.1109/ACCESS.2018.2881489.

[18] L. Greco, G. Percannella, P. Ritrovato, F. Tortorella, and M. Vento, "Trends in IoT based solutions for health care: Moving AI to the edge," Pattern Recognit. Lett., vol. 135, pp. 346–353, Jul. 2020, doi: 10.1016/j.patrec.2020.05.016.

[19] Rajeswara, A. (2021). Advanced Recommender System Using Hybrid Clustering and Evolutionary Algorithms for E-Commerce Product Recommendations. International Journal of Management Research and Business Strategy, 10(1).

[20] A. Mehmood, F. Mehmood, and W.-C. Song, "Cloud based E-Prescription management system for healthcare services using IoT devices," in 2019 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea (South): IEEE, Oct. 2019, pp. 1380–1386. doi: 10.1109/ICTC46691.2019.8939916.

[21] B. Pradhan, S. Bhattacharyya, and K. Pal, "IoT-Based Applications in Healthcare Devices," J. Healthc. Eng., vol. 2021, pp. 1–18, Mar. 2021, doi: 10.1155/2021/6632599.

[22] Sareddy, M. R. (2021). The future of HRM: Integrating machine learning algorithms for optimal workforce management. International Journal of Human Resources Management (IJHRM), 10(2).

[23] Y. Liu et al., "A Novel Cloud-Based Framework for the Elderly Healthcare Services Using Digital Twin," IEEE Access, vol. 7, pp. 49088–49101, 2019, doi: 10.1109/ACCESS.2019.2909828.

[24] V. Gupta, H. Singh Gill, P. Singh, and R. Kaur, "An energy efficient fog-cloud based architecture for healthcare," J. Stat. Manag. Syst., vol. 21, no. 4, pp. 529–537, Jul. 2018, doi: 10.1080/09720510.2018.1466961.

[25] S. Narla, "Optimizing Predictive Healthcare Modelling in a Cloud Computing Environment Using Histogram-Based Gradient Boosting, MARS, and SoftMax Regression," Int. J. Manag. Res. Bus. Strategy, vol. 11, no. 4, 2021.

[26] R. Sivan and Z. A. Zukarnain, "Security and Privacy in Cloud-Based E-Health System," Symmetry, vol. 13, no. 5, p. 742, Apr. 2021, doi: 10.3390/sym13050742.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 10, October 2022 |

| DOI:10.15680/IJMRSET.2022.0510003|

[27] I. D. M. B. Filho, G. Aquino, R. S. Malaquias, G. Girao, and S. R. M. Melo, "An IoT-Based Healthcare Platform for Patients in ICU Beds During the COVID-19 Outbreak," IEEE Access, vol. 9, pp. 27262–27277, 2021, doi: 10.1109/ACCESS.2021.3058448.

[28] B. Kadiyala and H. Kaur, "Secured IoT Data Sharing through Decentralized Cultural Co- Evolutionary Optimization and Anisotropic Random Walks with Isogeny- Based Hybrid Cryptography," J. Sci. Technol., vol. 06, no. 06, 2021.

[29] F. Farid, M. Elkhodr, F. Sabrina, F. Ahamed, and E. Gide, "A Smart Biometric Identity Management Framework for Personalised IoT and Cloud Computing-Based Healthcare Services," Sensors, vol. 21, no. 2, p. 552, Jan. 2021, doi: 10.3390/s21020552.

[30] A. Darwish, A. E. Hassanien, M. Elhoseny, A. K. Sangaiah, and K. Muhammad, "The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems," J. Ambient Intell. Humaniz. Comput., vol. 10, no. 10, pp. 4151–4166, Oct. 2019, doi: 10.1007/s12652-017-0659-1.

[31] R. Budda, "Integrating Artificial Intelligence And Big Data Mining For Iot Healthcare Applications: A Comprehensive Framework For Performance Optimization, Patient-Centric Care, And Sustainable Medical Strategies," Int. J. Manag. Res. Rev., vol. 11, no. 1, 2021.

[32] Chinmay Mukeshbhai Gangani, "Data Privacy Challenges in Cloud Solutions for IT and Healthcare," Int. J. Sci. Res. Sci. Technol., 2020.

[33] M. Mahmud et al., "A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications," Cogn. Comput., vol. 10, no. 5, pp. 864–873, Oct. 2018, doi: 10.1007/s12559-018-9543-3.

[34] V. Garikipati, N. R. Dyavani, B. S. Jayaprakasam, C. Ubagaram, and R. R. Mandala, "Leveraging Deep Neural Networks for Cloud-Based Network Traffic Anomaly Detection and Security Enhancement," J. Sci. Technol., vol. 6, no. 06, 2021.

[35] S. Ali et al., "Towards Pattern-Based Change Verification Framework for Cloud-Enabled Healthcare Component-Based," IEEE Access, vol. 8, pp. 148007–148020, 2020, doi: 10.1109/ACCESS.2020.3014671.

[36] A. Simeone, A. Caggiano, L. Boun, and R. Grant, "Cloud-based platform for intelligent healthcare monitoring and risk prevention in hazardous manufacturing contexts," Procedia CIRP, vol. 99, pp. 50–56, 2021, doi: 10.1016/j.procir.2021.03.009.

[37] R. Saha, G. Kumar, M. K. Rai, R. Thomas, and S.-J. Lim, "Privacy Ensured ${e}$ -Healthcare for Fog-Enhanced IoT Based Applications," IEEE Access, vol. 7, pp. 44536–44543, 2019, doi: 10.1109/ACCESS.2019.2908664.

[38] K. S. Awaisi, S. Hussain, M. Ahmed, A. A. Khan, and G. Ahmed, "Leveraging IoT and Fog Computing in Healthcare Systems," IEEE Internet Things Mag., vol. 3, no. 2, pp. 52–56, Jun. 2020, doi: 10.1109/IOTM.0001.1900096.

[39] V. S. Musam, "Enhancing Network Security in Cloud Environments Using Tab- Transformer Based Intrusion Detection Systems," J. Curr. Sci., vol. 09, no. 9726, 2021.

[40] A. A. Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," Future Gener. Comput. Syst., vol. 95, pp. 511–521, Jun. 2019, doi: 10.1016/j.future.2018.12.044.

[41] T. Alam, "Cloud-Based IoT Applications and Their Roles in Smart Cities," Smart Cities, vol. 4, no. 3, pp. 1196–1219, Sep. 2021, doi: 10.3390/smartcities4030064.

[42] W. Pulakhandam, "Enhancing SHACS with Oblivious RAM for Secure and Resilient Access Control in Cloud Healthcare Environments," Int. J. Eng. Res. Sci. Technol., vol. 17, no. 2, 2021.

Impact Factor
7.54

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com