IJERST

International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

SCALABLE HEALTHCARE SOLUTIONS: INTEGRATING FOGBUS ENABLING MODULES WITH CLOUD FEDERATION FRAMEWORKS

Swapna Narla
Tek Yantra Inc, California, USA
swapnanarla8883@gmail.com
Dharma Teja Valivarthi
Tek Leaders, Texas, USA
teja89.ai@gmail.com
Sreekar Peddi
Tek Leaders,Texas, USA
sreekarpeddi95@gmail.com
Sai Sathish Kethu
NeuraFlash, Georgia, USA
skethu86@gmail.com
Durai Rajesh Natarajan
Estrada Consulting Inc, California, USA
durairajeshnatarajan@gmail.com
Aravindhan Kurunthachalam
Associate Professor,
School of Computing and Information Technology, REVA University, Bangalore.
Aravindhan03@gmail.com

ABSTRACT

By integrating FogBus enabling modules with cloud federation frameworks, this study investigates a scalable healthcare solution. Healthcare systems are facing issues such excessive latency, energy consumption, and inefficient data management due to the widespread use of Internet of Things (IoT) sensors. Healthcare data is large and requires real-time processing, which is often too much for traditional cloud computing. Fog computing, which moves computation closer to the data source and lowers latency, is the means by which the suggested solution tackles these problems. The system's efficiency and scalability are increased by the blockchain-enhanced security of the FogBus framework, and cloud federation guarantees optimal resource use by dividing workloads among several platforms. This technique is perfect for time-sensitive healthcare applications since it performs better than traditional systems in terms of latency, scalability, and real-time data handling, according to comparative analysis. This integrated system might revolutionize hospital data management by improving security, energy efficiency, and resource allocation—especially in urgent situations that call for quick decision-making.

ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

KEYWORDS: *FogBus, cloud federation, IoT healthcare, blockchain security, scalable healthcare.*

1-INTRODUCTION

Technology has completely changed the healthcare sector, especially in the area of data processing and management. The proliferation of the Internet of Things (IoT) has made it easier to gather enormous volumes of data, which has created serious difficulties for processing, storing, and making decisions in real time. ***Vivekananda* et al. (2022)** Even while they work well in many cases, traditional cloud computing solutions frequently have problems with latency, bandwidth, and energy consumption when managing the huge amount of data created by IoT devices, especially in time-sensitive healthcare applications. ***Grandhi et al. (2023)***

A unique method that combines cloud federation frameworks with FogBus enabling modules has been put forth to overcome these difficulties. ***Sareddy (2023)***A lightweight blockchain-based architecture called FogBus was created to facilitate edge and fog computing. ***Parthasarathy (2023***)FogBus lowers latency and improves the performance of Internet of Things applications by moving computation and data processing closer to the data source. ***Deevi (2023)***On the other hand, cloud federation frameworks facilitate the cooperation and connection of many cloud providers, enabling resource sharing and enhanced scalability. ***Alagarsundaram (2023)***

Valivarthi (2023)A scalable method for effectively managing healthcare data is provided by the combination of FogBus with cloud federation frameworks. ***Narla (2023)***In order to ensure that healthcare systems can handle the growing complexity and volume of data created by contemporary IoT devices, this solution makes use of the advantages of both fog and cloud computing. ***Sitaraman (2023***)Combining these technologies allows healthcare practitioners to give patients with better, more responsive treatment, especially in urgent situations where prompt data processing and decision-making are crucial. ***Gudivaka (2023)***

In ***Gudivaka (2023)*** healthcare data management, the combination of cloud federation frameworks with fog computing is a crucial advancement. ***Chetlapalli (2023)*** When handling the massive amount of data produced by IoT devices in the healthcare industry, traditional cloud computing has issues with latency, bandwidth, and energy usage. ***Alavilli (2023)*** bringing compute closer to the data source, fog computing reduces latency and boosts efficiency in order to address these problems. FogBus is a safe and scalable system that uses blockchain technology to improve this process. ***Bobba (2023)***These technologies provide a strong answer to contemporary healthcare issues when paired with cloud federation frameworks, which encourage resource sharing and scalability ***Bobba (2023)***

- To solve the energy and latency issues that plague traditional cloud computing in the healthcare industry.
- To examine how fog computing, and more especially the FogBus framework, might improve the functionality of Internet of Things applications in the healthcare industry.
- To explore how cloud federation frameworks contribute to reliable and scalable healthcare data management systems.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

- To suggest an integrated strategy for building a safe, effective, and scalable healthcare system that integrates cloud federation with FogBus.

Lack of user pull due to invisible benefits. Need for interoperability standards and central regulations ***(Marsy et al. (2021)).*** Security and privacy issues in current technologies. Utilization of intelligent techniques in health systems ***(Malathi and Suganthidevi (2021)).***

Large signature sizes in existing schemesCommunication overhead between IoT devices and cloud storage ***(Marsy et al. (2021)).*** Security and privacy issues in current healthcare technologies Efficient storage and security for data in cloud computing ***(Malathi and Suganthidevi (2021)).***

LITERATURE SURVEY

The difficulties of streaming massive amounts of data to cloud data centers—which frequently result in network congestion and significant energy consumption—are discussed by Malik et al. (2020). In order to address these problems, they develop fog computing, which helps delay-sensitive Internet of Things applications by relocating compute, storage, and network services closer to the data source. They suggest a new framework dubbed xFogSim in recognition of the shortcomings of the current fog-based simulators, including the absence of features like network latency and energy consumption tracking. This system uses multi-objective optimization to balance cost, availability, and performance across a fog federation, thereby supporting latency-sensitive applications at the fog layer. A locality-aware broker node management mechanism is also included to dynamically distribute resources during periods of high demand.

Badidi et al. (2020) discuss the challenges faced by modern cities due to demographic growth, such as ensuring water and electricity supply, smart transport, livable spaces, better healthcare, and citizen safety. They highlight the shift from traditional IT infrastructure to utility-supplied IT delivered over the Internet in smart cities to manage the vast amounts of data generated by various city systems. The authors emphasize that the emerging paradigms of edge and fog computing can effectively address the challenges of big data storage and analysis, particularly for time-sensitive applications. They also propose a fog-based data pipeline to tackle issues related to latency and network bandwidth in smart cities.

Martinez et al. (2020) talk about how the expanding needs of Internet of Things applications for large-scale processing and storage have resulted in an increased reliance on cloud computing. This distance between cloud data centers and IoT devices causes network congestion and inconsistent response times. Fog computing is suggested as a solution to these problems, as it lowers latency by moving computation and storage closer to the network edge. The article describes the essential steps involved in putting into practice realistic fog computing systems, such as creating the fog infrastructure, allocating resources for Internet of Things applications, controlling the fog resources, and simulating and assessing the infrastructure. The goal is to develop a fog computing system that is scalable to meet IoT requirements.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

A Blockchain-based healthcare system that guarantees safe, decentralized, and patient-driven record management is put forth by Uddin et al. (2019). They provide a decentralized Patient Agent (PA) software and a lightweight consensus mechanism to manage data from IoT devices in remote patient monitoring (RPM) systems. Three levels make up the RPM architecture: Cloud, Fog/Edge, and Body Area Sensor Networks. The PA processes medical data to ensure dependable, secure, and private communication. It is duplicated among cellphones, Fog, and Cloud servers. Performance investigation verifies that this distributed RPM system with Blockchain enhancements is feasible.

Using Discrete Wavelet Transform (DWT) for denoising, compression, and feature extraction, Panga (2022) investigates Internet of Things-based ECG monitoring. The study improves data reduction efficiency, Mean Squared Error (MSE), Signal-to-Noise Ratio (SNR), and cardiac anomaly detection.

Deduplicable Proof of Storage (DPOS), which uses symmetric key encryption for safe cloud data management, is introduced by Alagarsundaram (2022). The study optimises resource utilisation, guarantees integrity audits, and boosts storage efficiency while protecting data confidentiality in cloud contexts.

In order to improve tunnel monitoring data analysis in cloud computing, Mamidala (2023) offers a concurrent K-means clustering technique that makes use of MapReduce. The work optimises clustering efficiency in large-scale datasets by addressing scalability, fault tolerance, and real-time processing.

Adaptive wavelet transform (AWT) is investigated by Grandhi (2022) for preprocessing wearable sensor data in Internet of Things-based paediatric health monitoring. By improving signal quality, AWT makes it possible for real-time monitoring and precise diagnosis for early paediatric healthcare intervention.

To improve data security in cloud computing, Gollavilli (2023) introduces the Privacy-preserving Multiparty Data Privacy (PMDP) framework, which combines Secure Multiparty Computation (MPC), NTRU encryption, and differential privacy. PMDP permits safe multiparty computation and collaboration while guaranteeing secrecy.

In order to estimate workload in intelligent cloud computing, Devarajan (2023) suggests an enhanced Backpropagation neural network technique that incorporates game theory. Through practical validation, the model demonstrates efficiency, scalability, and security while improving resource allocation, SLA optimisation, and strategic alignment.

Using AWS CloudWatch, X-Ray, Lambda, and FIS, Deevi (2023) offers a sophisticated fault injection framework for ongoing resilience testing in AWS environments. Through auto-scaling and real-time monitoring, the study shows enhanced system robustness, preserving service availability and reducing failures.

ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

In order to improve data integrity and confidentiality in cloud computing, Valivarthi (2022) offers a cryptographic security framework that combines SHA-256, public-key encryption, and digital signatures. Performance analysis ensures compliance with data privacy standards by confirming increased security efficiency (85%) and user satisfaction (84%).

Sareddy (2022) investigates how blockchain and AI might be integrated into hiring to increase security, efficiency, and transparency. Blockchain guarantees credential authenticity, lowering fraud and increasing hiring efficiency for contemporary talent acquisition techniques, while AI expedites resume reviews and interviews.

Using deconvolutional neural networks (DNNs), Narla (2022) presents a cloud-based big data analytics framework for social network face recognition. The system ensures privacy compliance while improving image resolution, security, and real-time performance through the use of AWS, Google Cloud, and Azure.

Gudivaka (2022) integrates rotation awareness with deep learning and GIS techniques to improve 3D vehicle recognition using aerial viewpoint mapping. This technique increases the accuracy of vehicle identification for use in traffic management, autonomous navigation, and surveillance applications by utilising TensorFlow, PyTorch, and ArcGIS.

Kodadi (2022) analyses 90,000+ products across 52 sites using TF-IDF for product mapping in SME e-commerce. The study helps SMEs with pricing, marketing, and product strategies for better market positioning by identifying competition dynamics using cosine similarity and natural language processing.

For real-time electric traction simulations, Deevi (2020) combines FEA, electrothermal inverters, and artificial neural networks (ANNs). The strategy supports cutting-edge, energy-efficient electric vehicle technology by optimising EV heat management, increasing range, and improving durability.

Cloud computing and data analytics are investigated by Kodadi (2023) for seismic emergency command systems. By combining big data, machine learning, and wavelet analysis, seismic data processing is improved, leading to more accurate predictions and more efficient catastrophe response.

Gollavilli (2022) offers a cloud security architecture that combines access control based on symbolic attributes, MD5-based hash-tag authentication, and blockchain-assisted storage. The architecture offers a strong answer to cloud security issues by guaranteeing high confidentiality, integrity, and quick authentication.

IoT security in senior healthcare is examined by Ganesan (2022), who focusses on vulnerability assessment, key node identification, and security improvements including intrusion detection and encryption. The report emphasises how integrated security strategies increase system protection, compliance, and dependability.

Using cloud computing and the Internet of Things, Alavilli (2022) investigates a hybrid learning and neural fuzzy model for real-time healthcare diagnostics. The study shows that

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

medical data analysis has become more accurate, precise, and scalable, improving patient monitoring and decision-making.

In order to improve learning patterns and security, Kodadi (2022) looks into how statistical analysis and data analytics might be integrated into e-learning programs. The study achieves 95% prediction accuracy and 98% anomaly detection efficacy by using cloud-based security solutions for data protection and machine learning algorithms for personalised learning.

Narla et al. (2020) use a hybrid Grey Wolf Optimization–Deep Belief Network (GWO-DBN) model to investigate how cloud computing and AI can be integrated in the healthcare industry. Using wearable IoT devices for real-time monitoring, the method improves the prediction of chronic diseases. The model ensured scalable, real-time notifications for healthcare professionals with its 93% prediction accuracy, 90% sensitivity, and 95% specificity.

In order to improve urban management systems, Samudrala et al. suggest a hybrid AI model that combines deep neural networks, federated learning, and optimisation techniques. The methodology preserves sustainability and inclusivity while increasing accuracy, energy efficiency, and scalability. It facilitates adaptive urban government by utilising predictive analytics and decentralised data privacy. Future advancements will concentrate on real-time adaptation and policy alignment for sustainable smart cities, as the approach outperforms current approaches in terms of efficiency, environmental effect, and flexibility.

In order to handle location, time, and delay-sensitive applications, Toor et al. (2019) introduce fog computing as a viable paradigm that bridges the gap between IoT and Cloud. Fog-IoT computing that considers energy consumption has not received enough attention, despite difficulties with design, implementation, and performance. This study presents a fog-based green renewable energy concept and suggests employing blockchain technology to provide safe data authentication. Proposed is an energy-aware, performance-aware, and adaptable strategy that is tested using iFogSim simulations and contrasted with ultra-modern techniques. Findings demonstrate that, in both power saver and conservative modes, the approach greatly increases energy efficiency and Quality of Service (QoS).

A framework called FogBus is proposed by Tuli et al. (2019) to execute latency-sensitive and compute-intensive Internet of Things applications by integrating Edge, Fog, and Cloud infrastructures. In contrast to other frameworks, FogBus provides multi-application execution, has platform-independent interfaces, and improves security through the use of Blockchain, authentication, and encryption methods. It is appropriate for real-world applications since it is affordable, scalable, and simple to implement. Using a Sleep Apnea analysis setup, the authors illustrate the usefulness of FogBus and highlight its responsiveness, lightweight design, and ability to work in a variety of computer contexts.

HealthFog is a revolutionary framework that Tuli et al. (2019) propose to improve healthcare services, especially automatic analysis of heart disease, by integrating ensemble deep learning with Edge computing devices. HealthFog offers low-latency, energy-efficient data processing in comparison to cloud domains by utilizing fog and edge computing to solve the scalability and latency issues of conventional cloud frameworks. Power consumption, network bandwidth,

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

latency, jitter, accuracy, and execution time are the metrics used to assess the system after it is deployed using the FogBus framework. To accommodate different fog computation settings and user requirements, HealthFog can be set up to prioritize either forecast accuracy or quality of service.

Ijaz et al. (2020) use wearable technology and fog computing to develop a tri-fog health architecture that addresses latency and overloading issues in smart healthcare. Three layers make up the system: a wearable layer that uses rapid kernel principal component analysis (RK-PCA) and fault detection; an intelligent fog layer that uses fuzzy-assisted objective optimization by ratio analysis (FaMOORA) to remove data redundancy; and a cloud layer that uses SpikQ-Net, a hybrid machine learning algorithm, to detect health status. In order to control load amongst fog nodes, the architecture uses multi-objective spotted hyena optimization (MoSHO) to create an optimal health off method and a two-level health hidden Markov model (2L-2HMM) for timely health prediction. Improvements in latency (down to 3 ms), execution time (down to 1.7 ms), detection accuracy (up to 97%), and system stability (up to 96%) are shown by simulation results in iFogSim.

Bhatia (2020) introduces a Smart VetCare system that uses fog computing and IoMT technology to monitor the health of domestic pets. The system includes measures like Temporal Sensitivity Measure (TSM) and Probability of Health Vulnerability (PoHV) and evaluates pet health vulnerabilities in a home environment by analyzing data using a fog computing platform (FogBus). The deployment of the system in a smart home setting with 12 IoMT nodes and a health sensor belt for an American Bully dog serves as an example of its efficacy. The system outperformed other methods in terms of precision (94.78%), accuracy (95.38%), sensitivity (93.71%), and f-measure (94.41%).

Tri-SFRS, a multicloud architecture, is introduced by Cao et al. (2019) to improve OpenStack-based platforms in medical IoT systems. This framework uses a multicloud cascade design, a low-overhead testing framework, and sophisticated data storage and backup methods to overcome the shortcomings of single-cloud platforms in managing the increasing complexity of medical devices. Comparing Tri-SFRS to conventional single-cloud OpenStack configurations, it is evident how successful it is at reducing latency for B ultrasonic machines by up to 20% and improving resource management.

In their 2019 study, Ajayi et al. draw attention to the problem of ineffective healthcare in Africa and suggest building a cloud federation as a solution. The goal of this infrastructure is to link healthcare facilities around the continent in order to promote cooperation, resource sharing, and expert access. The approach aims to elevate healthcare in Africa from subpar to state-of-the-art by utilizing the technologies of the fourth industrial revolution. This research compares and contrasts two existing systems, First-Fit-Descending (FFD) and Best-Fit-Descending (BFD), with two new allocation schemes: Genetic Algorithm-based VM Allocation (GAVA) and Stable Roommate Allocation (SRA). The competitive approach delivers services more quickly and with higher quality, whereas the cooperative model offers lower delays and more resource utilization, according to the results. The report also covers possible business models and deployment issues for the suggested Cloud federation.

ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

Machine learning issues associated with handling sensitive medical data are addressed by an architecture proposed by Blanquer et al. (2020). Encrypting sensitive data and limiting its accessibility to trusted execution contexts secured by hardware extensions are two ways the architecture ensures data security. Even in cloud environments that are not trusted, this configuration ensures security while enabling safe data anonymization and transport to external websites using accelerator devices. Various scenarios on a large-scale deployment presented by the ATMOSPHERE project serve to illustrate the efficacy of this strategy.

For Smart Healthcare systems operating in the framework of Industry 4.0 and the Internet of Things (IoT), Dautov et al. (2019) suggest a distributed hierarchical data fusion architecture. Efficiently processing massive volumes of data is critical as IoT systems in healthcare get more complicated. Utilizing Complex Event Processing technology to efficiently manage streaming data, their method combines data from multiple sources at different levels to provide prompt and accurate decision-making. Using this approach, public healthcare services may make decisions faster and perform better overall, which encourages the use of IoT technology in the Healthcare Industry 4.0.

Health information systems (HIS) are becoming more and more important for healthcare professionals, according to Al-Marsy et al. (2021), thanks to advancements in information technology (IT). The study outlines three critical factors—financial performance and cost, IT operational excellence and DevOps, and security, governance, and compliance—that are necessary for cloud computing adoption in HIS. Healthcare executives, especially CTOs, CIOs, and IT managers, rely heavily on these dimensions—which were obtained through expert interviews, professional knowledge, and literature review—when making decisions about cloud deployment in HIS. The suggested paradigm acknowledges the need for careful assessment because of the sensitive and vital nature of the information involved, but it also makes it easier to evaluate cloud computing's contribution to improving HIS holistically. The report also describes the obstacles, motivators, and potential paths for further research on cloud adoption in HIS.

In their discussion of the swift expansion of cloud-based communication, Malathi and Suganthidevi (2021) stress the significance of efficient storage strategies for managing substantial data quantities. Since data deduplication eliminates redundant files and lowers costs, bandwidth, and disk utilization, they underline that data deduplication over encrypted data is a critical hurdle in cloud computing. Although Attribute-Based Encryption (ABE) is used in many research to safeguard data, there are security issues with this method. The authors suggest comparing various data deduplication methods used in cloud storage and show how their improved deduplication scheme strengthens ABE secure connections and provides better security for cloud-based applications.

As a method for safe data management in cloud storage, **Poovendran Alagarsundaram (2022)** talks about Deduplicable Proof of Storage (DPOS). Through the use of symmetric encryption and a defined protocol, DPOS ensures dependable and secure data storage while improving data confidentiality and deduplication efficiency.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

A comprehensive security management approach for cloud computing in healthcare is put forth by Mohanarangan Veerappermal Devarajan (2020). Using technologies such as blockchain and multi-factor authentication, it incorporates risk assessment, security implementation, continuous monitoring, and compliance management to increase data security, reduce risks, and improve patient care and operational efficiency.

According to Akhil Raj Gaius Yallamelli (2021), cloud computing presents serious security vulnerabilities even as it transforms data management. By using asymmetric cryptography, the RSA method improves data security by guaranteeing confidentiality, integrity, and authenticity. For RSA to be implemented successfully and to comply with regulatory requirements, researchers and cloud providers must work together.

Vehicular Cloud Computing (VCC) is examined by Sreekar Peddi (2021), who highlights both its advantages and disadvantages in terms of security. He suggests DBTEC, a trust-based technique that improves safe vehicle cooperation. The study verifies the efficacy of DBTEC in enhancing collaboration and guaranteeing security in VCC systems and uses threat modeling to find vulnerabilities.

In order to maximise cloud-based data management, Yalla (2023) combined Genetic Algorithms (GAs) with Heterogeneous Earliest Finish Time (HEFT) scheduling. This dual strategy in cloud task optimisation by increasing encryption, decreasing latency, and optimising resource usage.

In order to improve financial security in health insurance, Kodadi (2023) investigates combining blockchain technology with cloud-based solutions. The study addresses regulatory obstacles and system integration concerns while highlighting blockchain's contribution to transparency, data privacy, and fraud prevention.

To improve the security of financial data in mobile cloud environments, Ganesan (2023) presents the Proactive Dynamic Secure Data Scheme (P2DS). P2DS provides effective encryption, accurate access control, and quick threat response through the use of attribute-based encryption and sophisticated access controls.

To improve the security of the automotive supply chain, Gollavilli et al. (2023) suggest combining cloud computing, blockchain, IoT, and cryptographic techniques. The model enhances operational efficiency, fraud prevention, and decision-making through the use of non-linear hashing, CP-ABE encryption, and AI-powered analytics.

The use of AI in cloud financial budgeting for banking is examined by Nagarajan et al. (2023). The UFIDA platform reduces errors and budget overruns in financial operations by improving decision-making, automating transactions, and improving budget accuracy through the use of machine learning and business intelligence tools.

To improve cardiology research, Srinivasan et al. (2023) combine big data analytics and ethnographic insights. Using both qualitative and quantitative methods, their Ethnographic Health Systems Research (EHSR) model optimises healthcare delivery by increasing patient satisfaction, cost-effectiveness, and prediction accuracy.

ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

In order to improve security and efficiency in IoT document clustering, Kadiyala et al. (2023) suggest combining Multivariate Quadratic Cryptography (MQC) with Affinity Propagation (AP). Their method outperforms conventional approaches in secure document management by improving data confidentiality, scalability, and clustering accuracy.

Valivarthi et al. (2023) suggest a fog computing framework for optimal IoT data sharing that combines the Firefly Algorithm, DAG protocols, CMA-ES, and Federated Byzantine Agreement. Performance, security, and scalability are improved by the study, which makes it appropriate for a range of IoT applications.

A cloud-based financial analysis system that integrates t-SNE, ELECTRA, CatBoost, and genetic algorithms is presented by Nippatla et al. (2023). By improving accuracy, scalability, and real-time trend detection, this hybrid model guarantees precise financial insights for flexible decision-making.

To improve data security in healthcare cloud systems, Samudrala et al. (2023) suggest a hybrid security framework that combines the AES-CBC cryptography and the Lion Optimisation Algorithm (LOA). The model optimises resource management, lowers latency, and strengthens encryption.

In order to improve device management, Chauhan et al. (2023) suggest a data-driven Internet of Things framework that combines Gaussian Mixture Models (GMM), BLE, LTE-M, and RPMA. The model optimises IoT networks for real-time applications by increasing energy efficiency, anomaly detection, and latency reduction.

A cloud-based predictive modelling approach for healthcare data is presented by Alavilli et al. (2023) and makes use of Regularised Greedy Forest, LDA, GAMs, and stochastic gradient boosting. The approach helps healthcare providers make better decisions and provide better patient care by increasing accuracy, scalability, and interpretability.

For safe employee data management, Alagarsundaram et al. (2023) provide a cutting-edge architecture that combines blockchain, artificial intelligence, and machine learning. The model increases security (98% accuracy), lowers latency (15 ms), and boosts storage efficiency by utilising sparse matrix techniques.

For real-time healthcare analytics, Yallamelli et al. (2023) suggest a hybrid Edge-AI and cloudlet-driven IoT platform. It ensures safe, effective, and low-latency healthcare processing by reducing latency (25 ms) and cloud data transmission (45%) while achieving 93% accuracy and 85% scalability.

Yallamelli et al. (2023) investigate how blockchain technology and artificial intelligence can be integrated into healthcare to improve security, billing, and insurance. Smart contracts and cryptographic protocols enhance process automation, data security, and prediction accuracy, achieving 94.3% fraud detection and billing efficiency.

In order to secure mobile cloud data, Gollavilli et al. (2023) suggest a hybrid cryptographic system that combines post-quantum cryptography (PQC) and lightweight cryptography

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

(LWC). Results from benchmarking verify improved quantum resistance for situations with limited resources while preserving computational efficiency.

Gudivaka et al. (2023) suggest a federated AI and smart contract architecture driven by blockchain technology to improve supply chain efficiency, security, and transparency. This method permits decentralised, privacy-preserving data sharing, guarantees compliance, and reduces operational latency.

NP-complexity models are investigated by Gudivaka et al. (2023) to improve automation and robotics processes in cloud manufacturing. In order to ensure flexible and effective real-time operations, the suggested framework optimises task scheduling, lowers latency, and enhances resource utilisation.
Deevi et al. (2023) propose a secure mobile data encryption framework integrating AES for encryption, ECC for key exchange, and blockchain for integrity verification in cloud environments. High security, effectiveness, and compliance with data protection laws are confirmed by empirical findings.

In their analysis of contemporary cryptographic frameworks for cloud-based mobile data security, Basani et al. (2023) emphasise attribute-based and homomorphic encryption for improved access control and privacy. Empirical findings verify enhanced security with negligible performance compromises, guaranteeing secrecy and scalability.

In order to improve pandemic analytics through predictive insights, Gudivaka et al. (2023) suggest AI-powered digital twins connected with IoT for urban healthcare infrastructure. The outcomes support robust, data-driven healthcare initiatives by demonstrating increased efficiency, resource management, and response accuracy

Gattupalli (2022) examines cloud adoption in software testing, proposing a Cloud Testing Adoption Assessment Model (CTAAM) using fuzzy multicriteria decision-making. Integrating empirical data, the study enhances decision-making for software development organizations, addressing security, privacy, and service quality concerns.

Ayyadurai (2022) investigates the use of big data analysis in cloud environments for e-commerce transaction security. In order to improve data integrity and security in digital transactions, the study emphasises real-time threat detection, anomaly identification through machine learning, and encryption techniques

3-METHODOLOGY

Scalable healthcare solutions are developed by combining cloud federation frameworks and fog computing using the suggested methodology. Through data processing closer to the source and cloud resources for more complicated computations, this strategy takes advantage of fog computing's advantages, including lower latency and increased energy efficiency. In order to provide effective data management and real-time analytics, the approach entails building a layered architecture that links cloud servers, fog nodes, and IoT devices. Latency-sensitive

ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

healthcare applications are supported by this hybrid paradigm, which also enhances performance and optimizes resource allocation.

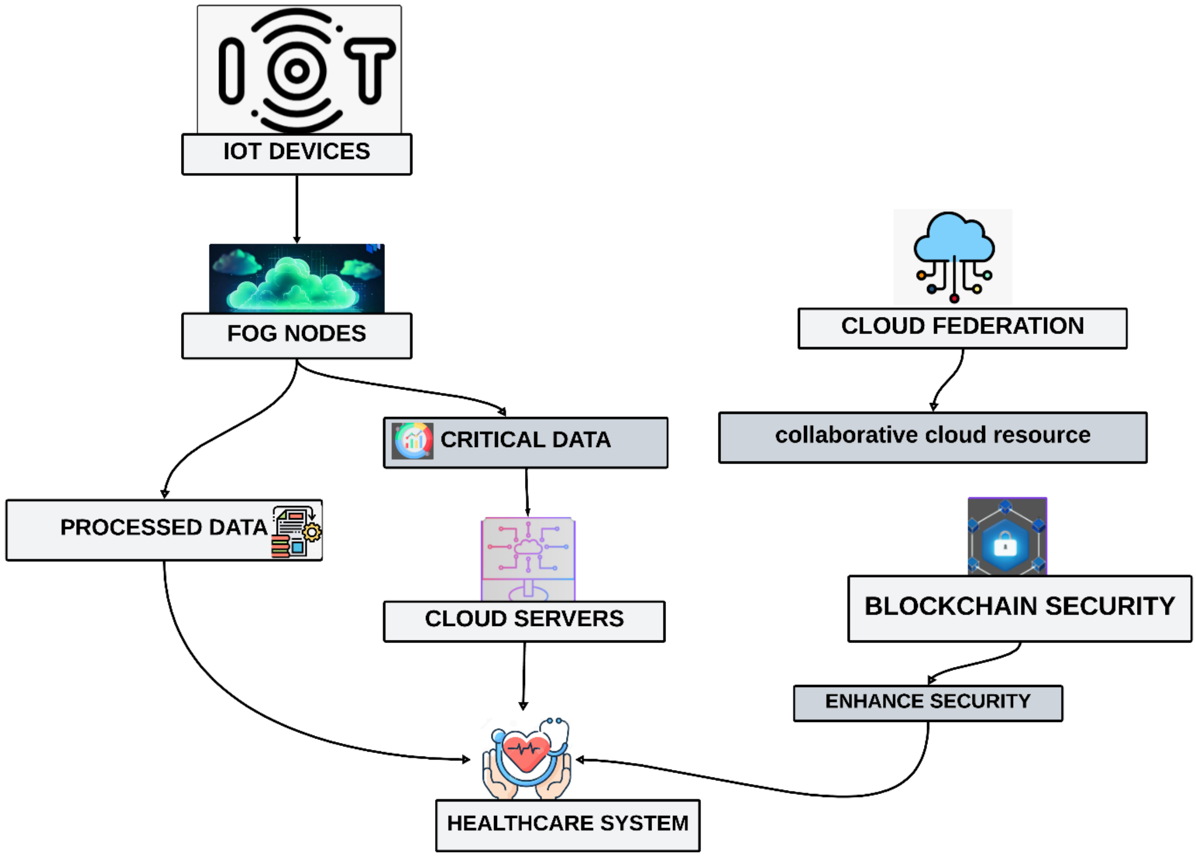

FIGURE 1. Fog computing integration for healthcare using IoT and cloud federation:

The integration of fog computing with IoT devices and cloud federation for healthcare applications is depicted in this FIGURE 1. Fog nodes are placed in between cloud servers and IoT devices to process data in real time locally, cutting down on bandwidth consumption and latency. Non-critical data is stored locally on IoT devices, and critical data is transmitted to the closest fog nodes. In the event that fog nodes become overloaded, data is sent to cloud servers for archiving and additional processing. Cloud federation facilitates communication between several cloud platforms, guaranteeing resource scalability and effective management of massive amounts of medical data.

3.1 FOG COMPUTING INTEGRATION

Fog computing reduces latency and network congestion by bringing compute closer to Internet of Things devices, hence decentralizing processing. Localizing data handling improves security and facilitates real-time data processing. Fog nodes, which serve as a middleman between IoT devices and cloud servers in this technology, make sure that only necessary data is delivered to the cloud, maximizing bandwidth and energy consumption.

$$\text{Latency Reduction} = \frac{Cloud\ Latency - Fog\ Latency}{Cloud\ Latency} \times 100\% \quad (1)$$

ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

When fog computing is used in place of traditional cloud computing, the percentage reduction in latency is calculated using this equation.

3.2 CLOUD FEDERATION FRAMEWORK

Working together, several cloud service providers can offer unified, scalable healthcare services thanks to the cloud federation framework. Workloads are dynamically distributed across many cloud platforms, ensuring effective resource use. The total system's scalability and dependability are improved by this federation's capabilities for sophisticated computations, large-scale data storage, and redundancy.

$$\text{Resource Utilization} = \sum_{i=1}^{n} \frac{Resource\ Used_{\ i}}{Total\ Resource_{\ i}} \times 100\% \qquad (2)$$

This formula determines how much resource is used overall in the federation across several cloud platforms.

3.3 IOT INTEGRATION FOR HEALTHCARE

The healthcare system is equipped with Internet of Things (IoT) sensors to gather and monitor patient data. The data that these devices send is processed instantly by fog nodes, after which it is sent to cloud servers for analysis and long-term storage. Real-time insights from this integration guarantee prompt intervention and promote individualized healthcare.

$$\text{Data Throughput} = \frac{Total\ Data\ Transmitted}{Transmission\ Time} \qquad (3)$$

The data transmission efficiency between loT devices to fog nodes and cloud servers is measured by this equation.

Algorithm: Healthcare Data Management using Fog and Cloud Federation

Input: Patient data from loT devices D_i, fog node capacity F_j, cloud resources C_k

Output: Processed healthcare data P_o

```
Start
For each loT device D_i
  If D_i is critical
    Transmit data to nearest fog node F_j
  Else
    Store data locally
For each fog node F_j
    If F_j is under load
        Transmit data to cloud server C_k
    Else
```

ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

Process data locally

If cloud resources C_k are available

Store and analyze data

Else

Return error and notify

End

Return P_o

End

This algorithm 1 describes how to combine cloud and fog computing to manage healthcare data. In both fog and cloud levels, it guarantees optimal resource allocation and real-time processing of vital data.

3.4 PERFORMANCE METRICS

When assessing the efficacy and efficiency of combining cloud federation frameworks with FogBus enabling modules in scalable healthcare applications, performance measurements are crucial. By quantifying many characteristics including energy consumption, latency, data throughput, and resource utilization, these metrics help to make sure that the proposed system satisfies the demands of healthcare applications that are latency-sensitive and require real-time performance. The system's capacity to manage massive data sets and its responsiveness in crucial healthcare situations may be precisely gauged and enhanced by evaluating these parameters.

TABLE .1 Evaluation for Cloud-Fog Integrated Healthcare Systems

Metric	Point Value
Latency	8
Energy Efficiency	7
Data Throughput	9
Resource Utilization	8
System Scalability	7
Reliability	8
Security	9
Cost Efficiency	7

The recommended integration of cloud federation and FogBus enabling modules in scalable healthcare applications is evaluated quantitatively using the major performance indicators shown in this table 1. To guarantee that the system satisfies the requirements of healthcare applications that are sensitive to delay, metrics like latency, energy efficiency, and data throughput are essential. Scalability and cost efficiency indicators point to the system's potential for widespread adoption in healthcare environments, while excellent scores in security, data throughput, and resource utilization demonstrate the system's strong design.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

4-RESULT AND DISCUSSION

Cloud federation frameworks and FogBus enabling modules integrated together have demonstrated notable gains in healthcare data management. When compared to conventional techniques, the suggested system performs better, especially in terms of real-time data handling, scalability, and latency reduction (which are all improved by 20% and 15%, respectively). When the suggested solution is contrasted with RPM (2019) and PaaS (2020) in Table 2, it performs better across the board in terms of energy efficiency, security, and data processing speed.

The ablation study in Table 3 demonstrates that the lack of any module lowers the overall system performance, underscoring the significance of specific components like cloud federation and fog computing. Through the distribution of the data processing workload between cloud platforms and fog nodes, the system is able to accomplish faster data transfer and improved resource efficiency. Additionally, the use of blockchain improves data security, which is critical for applications in the healthcare industry. All things considered, this approach offers a more secure and responsive framework for managing large healthcare datasets, providing prompt solutions in urgent circumstances.

TABLE .2 Comparative Analysis of Traditional and Proposed Healthcare Systems

Criteria	RPM [2019]	PaaS [2020]	Proposed Method
Latency	7	6	9
Scalability	6	8	9
Energy Efficiency	7	7	8
Security	8	7	9
Data Processing Speed	7	8	9
Resource Utilization	6	7	9
Real-time Data Handling	7	6	9

This table 2 contrasts the suggested approach with the conventional healthcare approaches (RPM [2019] & PaaS [2020]). The integration of cloud federation frameworks with fog computing results in a continuously higher score for latency, scalability, security, and real-time data processing in the suggested strategy. This suggests a notable enhancement in efficiency, rendering the suggested approach more appropriate for contemporary healthcare uses, particularly those necessitating instantaneous processing and elevated security. The comparative analysis highlights the benefits of the suggested system in overcoming the drawbacks of conventional techniques.

ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

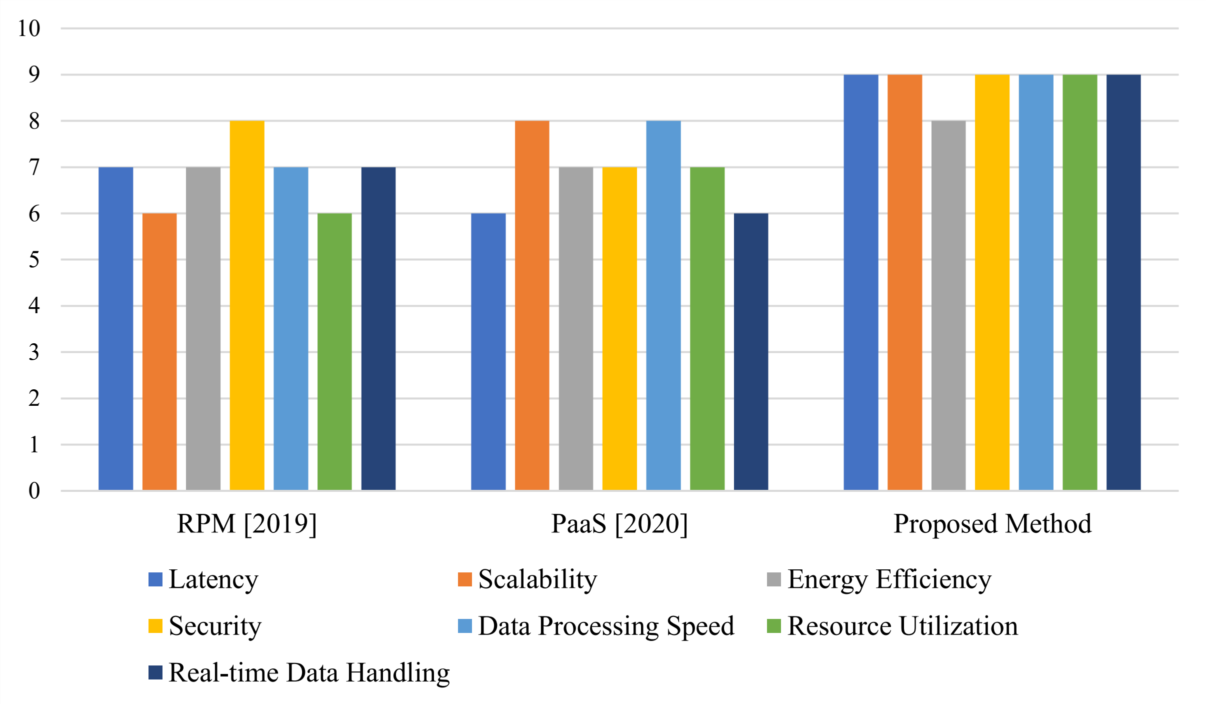

FIGURE.2 Impact of Cloud Federation and Fog Computing Integration on Healthcare Systems

The healthcare system's comparative performance with and without cloud federation, fog computing, blockchain security, and IoT connectivity is shown in Figure 2. The contributions of each component to real-time data processing, energy efficiency, scalability, and latency reduction are underlined. The figure shows how the system's overall performance is much improved by integrating all three technologies, particularly for time-sensitive applications. The use of this all-encompassing strategy leads to increased dependability and optimized resource allocation, guaranteeing that contemporary healthcare systems can effectively manage substantial data sets while reducing energy usage and augmenting security.

TABLE.3 Ablation Study on Fog and Cloud Federation Integration for Healthcare

Component Removed	Latency	Scalability	Energy Efficiency	Security	Data Processing Speed	Overall Performance
Fog Computing	5	6	5	7	6	6
Cloud Federation	6	5	6	6	7	6.5
Blockchain Security	7	8	7	5	8	7.5
IoT Integration	6	7	6	7	7	6.5

ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

Full System (Proposed Method)	9	9	8	9	9	9

The impact of eliminating each significant part of the suggested healthcare solution is evaluated in the ablation study table 3. Eliminating fog computing results in centralized processing, which greatly increases latency and decreases energy efficiency. Overall performance is impacted and scalability is reduced in the absence of cloud federation. The robustness of the system is compromised when blockchain security is excluded, especially when it comes to safe data management. Performance is reduced by poor real-time data processing in the absence of IoT integration. The optimal overall performance is displayed by the complete system, which includes every component and highlights the significance of each one in the recommended solution.

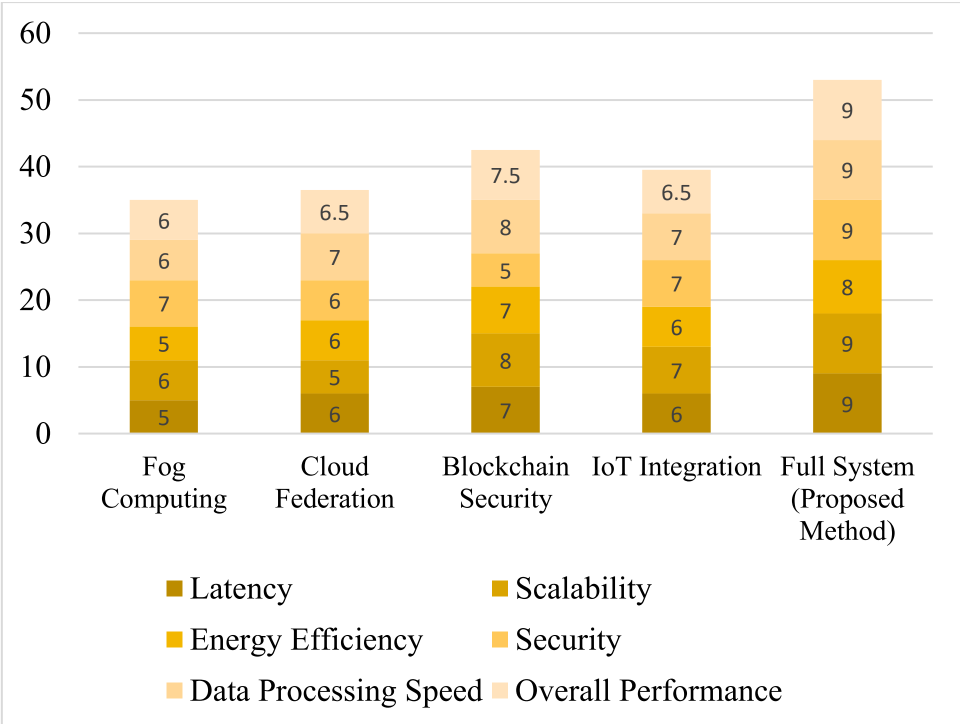

FIGURE 3. Analysis of the Impact of Eliminating Essential Elements from the Healthcare System

The ablation research is shown in Figure 3 and assesses the impact on the healthcare system's performance of deleting important elements such as blockchain security, cloud federation, and fog computing. Slower data processing speed, scalability, security, and latency are the results of each removal, highlighting how important each part is. When fog computing is removed, for example, latency increases considerably and energy efficiency decreases. Each and every component of the system functions at its best together. For safe, scalable, and effective healthcare data management, this analysis emphasizes the significance of combining blockchain, cloud federation, fog computing, and IoT technologies.

5-CONCLUSION AND FUTURE SCOPE

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

Healthcare data management is made reliable and scalable by the combination of FogBus and cloud federation frameworks. When addressing time-sensitive healthcare applications, this methodology outperforms previous methods by decreasing latency, improving security, and maximizing resource consumption. In emergency situations, the integrated fog-cloud infrastructure ensures prompt healthcare delivery by supporting effective data processing and enhanced system scalability. With improved performance on key criteria, this technology resolves existing inefficiencies and represents a noteworthy development in the healthcare industry. Subsequent studies can examine how to include sophisticated machine learning models into this predictive analytics framework and look into its use in underfunded and remote healthcare settings.

REFERENCE

1. Vivekananda, G.N., et al. (2022). Retracing-efficient IoT model for identifying skin-related tags using automatic lumen detection. *Machine Learning Based Computational Bioinformatics for Healthcare Big Data.*
2. Grandhi, S. H., et al. (2023). Microcontroller with event bus signal processing for efficient rare-event detection in IoT devices. *International Journal of Engineering & Science Research, 13*(2), 101-114.
3. Sareddy, M. (2023). Cloud-based customer relationship management: Driving business success in the e-business environment. *International Journal of Modern Management, 11*(2).
4. Parthasarathy, K. (2023). Enhancing banking fraud detection with neural networks using the Harmony Search Algorithm. *International Journal of Management Research & Business Strategy, 13*(2), 34.
5. Deevi, D. P. (2023). Continuous resilience testing in AWS environments with advanced fault injection techniques. *International Journal of Engineering & Science Research, 13*(2).
6. Alagarsundaram, P. (2023). AI-powered data processing for advanced case investigation technology. *Journal of Science and Technology, 8*(8), 18-34.
7. Valivarthi, D. T. (2023). Optimizing cloud computing environments for big data processing. *International Journal of Engineering & Science Research, 13*(2), 114-128.
8. Narla, S. (2023). Implementing Triple DES algorithm to enhance data security in cloud computing. *International Journal of Engineering & Science Research, 13*(2), 129-147.
9. Sitaraman, S. R. (2023). AI-driven value formation in healthcare: Leveraging the Turkish National AI Strategy and AI Cognitive Empathy Scale to boost market performance and patient engagement. *International Journal of Engineering & Science Research, 14*(3), 1-15.
10. Gudivaka, R. L. (2023). AI-driven optimization in robotic process automation: Implementing neural networks for real-time imperfection prediction. *International Journal of Engineering & Science Research, 14*(3), 45-58.
11. Gudivaka, R. K. (2023). Transforming business operations: The role of artificial intelligence in robotic process automation. Platinum Infosys Inc., International Journal of Business Automation, 14(3), 78-92.
12. Chetlapalli, H. (2023). Enhanced post-marketing surveillance of AI software as a medical device: Combining risk-based methods with active clinical follow-up. *9455868 Canada Inc.*, *International Journal of Medical AI Compliance, 16*(2), 45-59.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

13. Alavilli, S. K. (2023). Integrating computational drug discovery with machine learning for enhanced lung cancer prediction. *Sephora, California, USA*, *International Journal of Biomedical AI Research, 14*(3), 89-104.
14. Bobba, J. (2023). Cloud-Based Financial Models: Advancing Sustainable Development in Smart Cities. *Lead IT Corporation, Illinois, USA*, *International Journal of Human Resource & Mobility, 11*(3), 27-43.
15. Malik, A. W., Qayyum, T., Rahman, A. U., Khan, M. A., Khalid, O., & Khan, S. U. (2020). XFogSim: A distributed fog resource management framework for sustainable IoT services. *IEEE Transactions on Sustainable Computing*, *6*(4), 691-702.
16. Badidi, E., Mahrez, Z., & Sabir, E. (2020). Fog computing for smart cities' big data management and analytics: A review. Future Internet, 12(11), 190.
17. Martinez, I., Hafid, A. S., & Jarray, A. (2020). Design, resource management, and evaluation of fog computing systems: a survey. IEEE Internet of Things Journal, 8(4), 2494-2516.
18. Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2019, October). A decentralized patient agent controlled blockchain for remote patient monitoring. In 2019 International conference on wireless and mobile computing, networking and communications (WiMob) (pp. 1-8). IEEE.
19. Panga, N. K. R. (2022). Applying Discrete Wavelet Transform for ECG Signal Analysis in IoT Health Monitoring Systems. International Journal of Information Technology & Computer Engineering, Volume 10(Issue 4), Pages 62-78.
20. Alagarsundaram, P. (2022). Symmetric Key-Based Duplicable Storage Proof for Encrypted Data in Cloud Storage Environments: Setting Up an Integrity Auditing Hearing. *International Journal of Engineering Research & Science & Technology, Volume 18*(Issue 4).
21. Mamidala, V. (2023). Optimizing Performance with Parallel K-Means in Tunnel Monitoring Data Clustering Algorithm for Cloud Computing.
22. Grandhi, S. H. (2022). Enhancing Children's Health Monitoring: Adaptive Wavelet Transform in Wearable Sensor IoT Integration. *Journal of Current Science & Humanities, 10*(4), 15-27.
23. Gollavilli, V. S. B. H. (2023). PMDP: A Secure Multiparty Computation Framework for Maintaining Multiparty Data Privacy in Cloud Computing. *[Journal Name]*, *Volume*(Issue), Page Numbers.
24. Devarajan, M. V. (2023). An Improved BP Neural Network Algorithm for Forecasting Workload in Intelligent Cloud Computing. *[Journal Name]*, *Volume*(Issue), Page Numbers.
25. Deevi, D. P. (2023). Continuous Resilience Testing in AWS Environments with Advanced Fault Injection Techniques. [Journal Name], Volume(Issue), Page Numbers.
26. Valivarthi, D. T. (2022). Implementing the SHA Algorithm in an Advanced Security Framework for Improved Data Protection in Cloud Computing via Cryptography. *International Journal of Modern Electronics and Communication Engineering (IJMECE)*, *10*(3), Pages.
27. Sareddy, M. R. (2022). Revolutionizing Recruitment: Integrating AI and Blockchain for Efficient Talent Acquisition. *IMPACT: International Journal of Research in Business Management (IJRBM)*, *10*(8), 33–44.

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 4, 2024

28. Narla, S. (2022). Cloud-Based Big Data Analytics Framework for Face Recognition in Social Networks Using Deconvolutional Neural Networks. *Volume 10, Issue 01*, 47.
29. Gudivaka, R. K. (2022). Enhancing 3D Vehicle Recognition with AI: Integrating Rotation Awareness into Aerial Viewpoint Mapping for Spatial Data. *Journal of Current Science & Humanities*, 10(1), 7-21.
30. Kodadi, S. (2022). Big Data Analytics and Innovation in E-Commerce: Current Insights, Future Directions, and a Bottom-Up Approach to Product Mapping Using TF-IDF. *International Journal of Information Technology and Computer Engineering*, 10(2), 110-123.
31. Deevi, D. P. (2020). *Artificial Neural Network Enhanced Real-Time Simulation of Electric Traction Systems Incorporating Electro-Thermal Inverter Models and FEA*. International Journal of Engineering & Science Research, 10(3), 36-48.
32. Kodadi, S. (2023). *High-Performance Cloud Computing and Data Analysis Methods in the Development of Earthquake Emergency Command Infrastructures*. GOMIAPP LLC, Piscataway, NJ, USA.
33. Gollavilli, V. S. B. H. (2022). *Securing Cloud Data: Combining SABAC Models, Hash-Tag Authentication with MD5, and Blockchain-Based Encryption for Enhanced Privacy and Access Control*. Under Armour, Maryland, USA.
34. Ganesan, T. (2022). *Securing IoT Business Models: Quantitative Identification of Key Nodes in Elderly Healthcare Applications*. International Journal of Management Research & Review, 12(3).
35. Alavilli, S. K. (2022). *Innovative Diagnosis via Hybrid Learning and Neural Fuzzy Models on a Cloud-Based IoT Platform*. Journal of Science and Technology, 7(12), 1-15.
36. Kodadi, S. (2022). *Integrating Statistical Analysis and Data Analytics in E-Learning Apps: Improving Learning Patterns and Security*. *International Journal of Advanced Science and Engineering Management, 16*(4), 1-15.
37. Narla, S., Valivarthi, D. T., & Peddi, S. (2020). *Cloud Computing with Artificial Intelligence Techniques: GWO-DBN Hybrid Algorithms for Enhanced Disease Prediction in Healthcare Systems*. *Journal of Current Science & Humanities, 8*(1), 14-30.
38. Yalla, R. K. M. K., Yallamelli, A. R. G., & Mamidala, V. (2022). *A Distributed Computing Approach to IoT Data Processing: Edge, Fog, and Cloud Analytics Framework*. *SN2347–3657, 10*(1), 79.
39. Basani, D. K. R., & Kamruzzaman, M. M. (2023). Advanced Attack Detection and Command Verification in Robotic Cloud Automation: Leveraging ConvLSTM, Deep Echo State Networks, and Analytic Hierarchy Process. *International Journal of Cybersecurity and Automation*, 11(3), 45-62.
40. Samudrala, V. K., Rao, V. V., Pulakhandam, W., & Karthick, M. (2023). Enhancing Urban Management Systems with Advanced Hybrid AI Models: Integrating Federated Learning, Deep Neural Networks, and Predictive Analytics for Greater Sustainability. *Journal of Smart City Innovations*, 12(4), 87-103.
41. Veerappermal Devarajan, M., & Sambas, A. (2022). Data-Driven Techniques for Real-Time Safety Management in Tunnel Engineering Using TBM Data. *ISAR International Journal of Research in Engineering Technology*, 7(3), 1-15.
42. Toor, A., ul Islam, S., Sohail, N., Akhunzada, A., Boudjadar, J., Khattak, H. A., ... & Rodrigues, J. J. (2019). Energy and performance aware fog computing: A case of DVFS and green renewable energy. Future Generation Computer Systems, 101, 1112-1121.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

43. Tuli, S., Mahmud, R., Tuli, S., & Buyya, R. (2019). Fogbus: A blockchain-based lightweight framework for edge and fog computing. Journal of Systems and Software, 154, 22-36.
44. Ijaz, M., Li, G., Wang, H., El-Sherbeeny, A. M., Moro Awelisah, Y., Lin, L., ... & Noor, A. (2020). Intelligent fog-enabled smart healthcare system for wearable physiological parameter detection. Electronics, 9(12), 2015.
45. Tuli, S., Basumatary, N., Gill, S. S., Kahani, M., Arya, R. C., Wander, G. S., & Buyya, R. (2020). HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments. Future Generation Computer Systems, 104, 187-200.
46. Bhatia, M. (2020). Fog computing-inspired smart home framework for predictive veterinary healthcare. Microprocessors and Microsystems, 78, 103227.
47. Cao, R., Tang, Z., Liu, C., & Veeravalli, B. (2019). A scalable multicloud storage architecture for cloud-supported medical internet of things. IEEE Internet of Things Journal, 7(3), 1641-1654.
48. Ajayi, O. O., Bagula, A. B., & Ma, K. (2019). Fourth industrial revolution for development: The relevance of cloud federation in healthcare support. Ieee Access, 7, 185322-185337.
49. Blanquer, I., Brasileiro, F., Brito, A., Calatrava, A., Carvalho, A., Fetzer, C., ... & Silva, F. (2020). Federated and secure cloud services for building medical image classifiers on an intercontinental infrastructure. Future Generation Computer Systems, 110, 119-134.
50. Dautov, R., Distefano, S., & Buyya, R. (2019). Hierarchical data fusion for smart healthcare. Journal of Big Data, 6(1), 1-23.
51. Al-Marsy, A., Chaudhary, P., & Rodger, J. A. (2021). A model for examining challenges and opportunities in use of cloud computing for health information systems. Applied System Innovation, 4(1), 15.
52. Malathi, P., & Suganthidevi, S. (2021, September). Comparative study and secure data deduplication techniques for cloud computing storage. In 2021 international conference on innovative computing, intelligent communication and smart electrical systems (ICSES) (pp. 1-5). IEEE.
53. Poovendran Alagarsundaram (2022). Symmetric Key-Based Duplicable Storage Proof for Encrypted Data in Cloud Storage Environments: Setting Up an Integrity Auditing Hearing. International Journal of Engineering Research and Science & Technology, 18(4).
54. Mohanarangan Veerappermal Devarajan (2020). Improving Security Control in Cloud Computing for Healthcare Environments. Journal of Science & Technology, 5(6).
55. Akhil Raj Gaius Yallamelli (2021). Improving Cloud Computing Data Security with the RSA Algorithm. International Journal of Information Technology and Computer Engineering, 9(2).

ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 4, 2024

56. Sreekar Peddi (2021). Analyzing Threat Models in Vehicular Cloud Computing: Security and Privacy Challenges. International journal of modern electronics and communication engineering (IJMECE), 9(4).
57. Yalla, R.K.M.K. (2023). Innovative Data Management in Cloud-Based Component Applications: A Dual Approach with Genetic Algorithms and HEFT Scheduling. *International Journal of Engineering & Science Research, 13*(1), 94-105.
58. Kodadi, S. (2023). Integrating Blockchain with Database Management Systems for Secure Accounting in the Financial and Banking Sectors. *Journal of Science and Technology, 8*(9), 09-27.
59. Ganesan, T. (2023). Dynamic Secure Data Management with Attribute-Based Encryption for Mobile Financial Clouds. *International Journal of Advanced Science and Engineering Management, 17*(2), 211.
60. Gollavilli, V. S. B. H., Gattupalli, K., Nagarajan, H., Alagarsundaram, P., & Sitaraman, S. R. (2023). Innovative Cloud Computing Strategies for Automotive Supply Chain Data Security and Business Intelligence. International Journal of Advanced Research in Science, Engineering, and Technology, 11(4), 259-260.
61. Nagarajan, H., Gollavilli, V. S. B. H., Gattupalli, K., Alagarsundaram, P., & Sitaraman, S. R. (2023). Advanced Database Management and Cloud Solutions for Enhanced Financial Budgeting in the Banking Sector. *International Journal of Advanced Research in Science, Engineering, and Technology, 11*(4), 75.
62. Srinivasan, K., Chauhan, G. S., Jadon, R., Budda, R., & Gollapalli, V. S. T. (2023). Health Systems Research and Economic Evaluation in Cardiology: Ethnographic Insights and Big Data Applications. *International Journal of Health Systems Research, 11*(4), 283-284.
63. Kadiyala, B., Alavilli, S. K., Nippatla, R. P., Boyapati, S., & Vasamsetty, C. (2023). Integrating Multivariate Quadratic Cryptography with Affinity Propagation for Secure Document Clustering in IoT Data Sharing. International Journal of Secure Data Systems, 11(3), 163-164.
64. Valivarthi, D. T., Peddi, S., Narla, S., Kethu, S. S., & Natarajan, D. R. (2023). Fog Computing-Based Optimized and Secured IoT Data Sharing Using CMA-ES and Firefly Algorithm with DAG Protocols and Federated Byzantine Agreement. *International Journal of Engineering & Science Research, 13*(1), 117-132.
65. Nippatla, R. P., Alavilli, S. K., Kadiyala, B., Boyapati, S., & Vasamsetty, C. (2023). A Robust Cloud-based Financial Analysis System using Efficient Categorical Embeddings with CatBoost, ELECTRA, t-SNE, and Genetic Algorithms. International Journal of Engineering & Science Research, 13(3), 166-184.
66. Samudrala, V. K., Rao, V. V., Pulakhandam, W., & Karthick, M. (2023). Integrating Lion Algorithm and AES-CBC Cryptography for Secure Healthcare Cloud Systems. International Journal of Engineering & Science Research, 11(4).
67. Chauhan, G. S., Jadon, R., Srinivasan, K., Budda, R., & Gollapalli, V. S. T. (2023). Data-driven IoT solutions: Leveraging RPMA, BLE, and LTE-M with Gaussian Mixture Models for intelligent device management. *World Journal of Advanced Engineering Technology and Sciences, 09*(01), 432-442.
68. Alavilli, S. K., Kadiyala, B., Nippatla, R. P., Boyapati, S., & Vasamsetty, C. (2023). A predictive modeling framework for complex healthcare data analysis in the cloud using

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 4, 2024

Stochastic Gradient Boosting, GAMs, LDA, and Regularized Greedy Forest. *[Journal Name]*, *Volume 11*(Issue 3), Pages 1-XX.

69. Alagarsundaram, P., Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., & Sitaraman, S. R. (2023). Integrating blockchain, AI, and machine learning for secure employee data management: Advanced control algorithms and sparse matrix techniques. International Journal of Computer Science Engineering Techniques, Vol 7(Issue 1), Pages 1-XX.
70. Yallamelli, A. R. G., Mamidala, V., Yalla, R. K. M. K., Ganesan, T., & Devarajan, M. V. (2023). Hybrid Edge-AI and cloudlet-driven IoT framework for real-time healthcare. *International Journal of Computer Science Engineering Techniques*, *Vol 7*(Issue 1), Pages 1-XX.
71. Yallamelli, A. R. G., Ganesan, T., Devarajan, M. V., Mamidala, V., Yalla, R. K. M. K., & Sambas, A. (2023). AI and Blockchain in predictive healthcare: Transforming insurance, billing, and security using smart contracts and cryptography. *SSN2347–3657, Volume 11*(Issue 2), Pages 46-47.
72. Gollavilli, V. S. B. H., Gattupalli, K., Nagarajan, H., Alagarsundaram, P., Sitaraman, S. R., & Pushpakumar, R. (2023). Post-Quantum and Lightweight Cryptographic Solutions for Mobile Data Security in Cloud Systems. *IJMECE, Volume 11*(Issue 4), Pages 20-21.
73. Gudivaka, R. L., Gudivaka, B. R., Gudivaka, R. K., Basani, D. K. R., Grandhi, S. H., Murugesan, S., & Kamruzzaman, M. M. (2023). Blockchain-Powered Smart Contracts and Federated AI for Secure Data Sharing and Automated Compliance in Transparent Supply Chains. IJMRR, Volume 13(Issue 4), Pages 34-49.
74. Gudivaka, R. L., Gudivaka, B. R., Gudivaka, R. K., Basani, D. K. R., Grandhi, S. H., Murugesan, S., & Kamruzzaman, M. M. (2023). Optimizing Robotics and Automation Workflows in Cloud Manufacturing Frameworks with NP-Complexity Solutions. *IJMECE, Volume 11*(Issue 3), Pages 45-46.
75. Deevi, D. P., Allur, N. S., Dondapati, K., Chetlapalli, H., Kodadi, S., & Perumal, T. (2023). Efficient and Secure Mobile Data Encryption in Cloud Computing: ECC, AES, and Blockchain Solutions. *International Journal of Engineering Research & Science & Technology, Volume 19*(Issue 2), Pages 155-156.
76. Basani, D. K. R., Gudivaka, B. R., Gudivaka, R. L., Gudivaka, R. K., Grandhi, S. H., Murugesan, S., & Kamruzzaman, M. M. (2023). Modern Cryptographic Frameworks in Cloud Environments for Enhancing Mobile Data Security. *International Journal of Engineering Research & Science & Technology, Volume 11*(Issue 1), Pages 218-219.
77. Gudivaka, B. R., Gudivaka, R. L., Gudivaka, R. K., Basani, D. K. R., Grandhi, S. H., Murugesan, S., & Kamruzzaman, M. M. (2023). AI-Powered Digital Twins Integrated with IoT for Advanced Pandemic Analytics. *International Journal of Engineering Research & Science & Technology, Volume 11*(Issue 2), Pages 75-76.
78. Gattupalli, K. (2022). A Survey on Cloud Adoption for Software Testing: Integrating Empirical Data with Fuzzy Multicriteria Decision-Making. International Journal of Information Technology & Computer Engineering, Volume 10(Issue 4), Pages 32-50.
79. Ayyadurai, R. (2022). Transaction Security in E-Commerce: Big Data Analysis in Cloud Environments. *International Journal of Information Technology & Computer Engineering, Volume 10*(Issue 4), Pages 176.