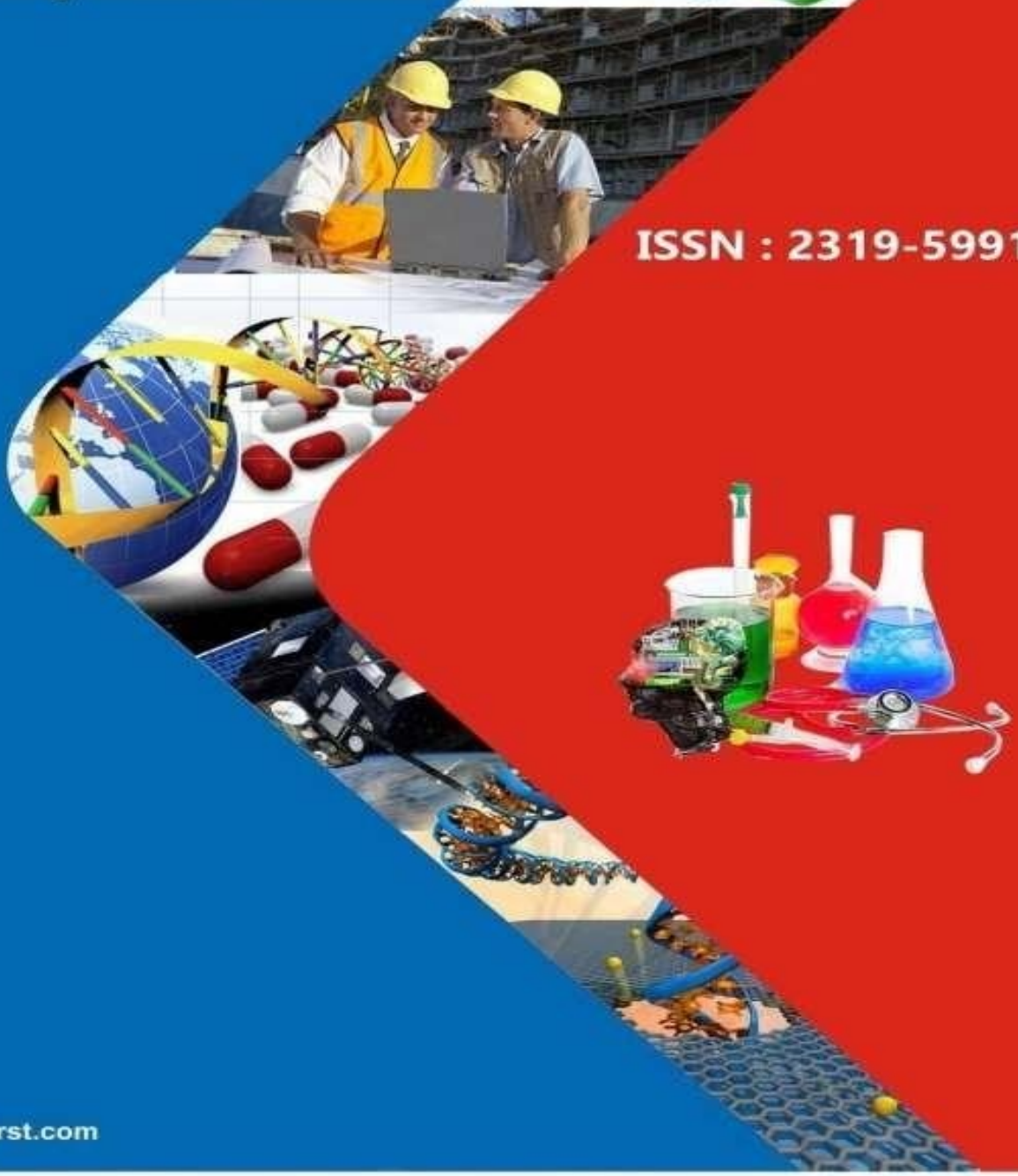
International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991



www.ijerst.com

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

ISSN 2319-5991 www.ijerst.com
Vol. 19, Issue 1, 2023

Leveraging Internet of Things (IoT) for Healthcare Monitoring and Cloud Integration

Vamshi Krishna Samudrala,

Product Technical Leader at American Airlines, Dallas, TX

samudralavamshi@gmail.com

Winner Pulakhandam,

Personify Inc, Texas, USA

wpulakhandam.rnd@gmail.com

Visrutatma Rao Vallu,

Clinical Data Manager, Insmed Inc., Sunnyvale, CA / Dallas, TX

valluvishruthrao@gmail.com

Veerandra Kumar R,

Saveetha Engineering College, Saveetha Nagar,

Thandalam, Chennai, 602105

veerandrakumar.r@panimalar.ac.in

ABSTRACT

The integration of Internet of Things (IoT) devices in healthcare systems has significantly improved patient monitoring by enabling the continuous collection of health data. This study outlines a secure workflow for healthcare data management, focusing on the collection of data from IoT devices, its encryption using AES (Advanced Encryption Standard**)** encryption, and subsequent storage in cloud storage for analysis and further processing. Initially, healthcare data is continuously collected from IoT devices, such as wearable sensors and medical equipment, capturing key patient parameters. To ensure the confidentiality and security of this sensitive data, AES encryption is applied before transmission, ensuring robust protection against unauthorized access. The encrypted data is then securely stored in cloud storage, enabling scalable and efficient data management. Cloud-based computational resources and machine learning techniques are leveraged for further analysis, providing insights and decision support for healthcare providers. This approach emphasizes the importance of data security in IoT-based healthcare systems and demonstrates the potential for secure cloud storage to improve healthcare delivery.

Keywords: IoT, healthcare monitoring, AES encryption, cloud storage, data security, monitoring.

INTRODUCTION

The integration of Internet of Things (IoT) devices into healthcare systems has opened new avenues for monitoring and data-driven decision-making[1]. With the increasing reliance on wearable sensors and IoT-enabled medical devices, healthcare professionals can now access continuous patient data for better diagnosis, treatment planning, and monitoring[2]. However, the exponential growth of healthcare data raises concerns about data privacy, security, and efficient storage[3]. The proposed framework aims to address these challenges by securely collecting, encrypting, and storing sensitive healthcare data in cloud storage systems, ensuring both privacy and scalability for healthcare applications[4].

ISSN 2319-5991 www.ijerst.com
Vol. 19, Issue 1, 2023

Existing methods in healthcare data security and IoT integration primarily focus on data collection and analysis but often fall short in addressing privacy concerns and secure storage[5]. Methods like cloud-based healthcare data management, edge computing, and secure transmission protocols have been widely used[6]. While these systems aim to improve data access and monitoring, they often face issues such as insufficient data encryption, vulnerability to cyber-attacks, and scalability limitations[7]. Techniques such as homomorphic encryption and public key infrastructure (PKI) offer data security but are computationally expensive and challenging to implement at scale[8]. These drawbacks hinder the effectiveness of IoT-based healthcare systems in providing secure and efficient services[9].

The rapid adoption of Internet of Things (IoT) technologies in healthcare systems has significantly transformed patient monitoring, enabling continuous, collection of health data[10]. IoT devices such as wearable sensors, medical equipment, and connected systems offer valuable insights into patients' health status, improving diagnosis, treatment plans, and overall patient care[11]. However, with the increasing volume and sensitivity of healthcare data, ensuring its security and privacy has become a critical challenge[12]. As healthcare data is often transmitted across networks and stored in the cloud, there is a pressing need for robust encryption techniques to safeguard against data breaches, unauthorized access, and cyberattacks[13]. Balancing high security with system performance and scalability is a key concern in the design of these IoT-based healthcare systems[14].

To address these challenges, several existing approaches have explored various encryption techniques, data storage solutions, and processing frameworks[15]. However, many of these methods suffer from limitations such as high computational overhead, scalability issues, and inefficiencies when dealing with large-scale data and a growing number of connected devices[16]. For instance, RSA encryption, commonly used in healthcare data systems, often results in high execution times, making it unsuitable for applications[17]. Additionally, multi-layered security frameworks, although effective, increase system complexity and hinder performance[18]. The proposed framework aims to overcome these shortcomings by utilizing Advanced Encryption Standard (AES), a lightweight yet secure encryption technique, combined with cloud storage and efficient data management strategies[19]. This solution is designed to provide a scalable, efficient, and secure framework for IoT-based healthcare systems, ensuring the protection of sensitive data without compromising system performance or processing capabilities[20].

The organization of the paper is as follows: A literature review concerning IoT-based healthcare systems, encryption techniques, and data management challenges is discussed in Section 2. The proposed methodology is explained in detail in Section 3. Section 4 discusses the results. Lastly, the paper concludes in Section 5.

LITERATURE REVIEW

The integration of Internet of Things (IoT) technologies in healthcare has significantly enhanced patient monitoring and data management, though securing sensitive data while ensuring scalability remains a challenge [21]proposed a cloud-based system using RSA encryption, but the computational overhead of RSA limits its efficiency in large-scale systems, highlighting the need for more efficient encryption like AES.[22]Introduced a multi-layered security framework for Healthcare IoT, but the complexity of managing multiple security layers led to performance inefficiencies, which the proposed AES-based framework addresses by simplifying encryption and reducing computational complexity.

[23]proposed a smart eHealth framework integrating IoT, mobile edge computing, 5G, and blockchain, but faced challenges in cost and adoption, highlighting the need for scalable, cost-effective solutions, which the proposed AES-encrypted framework addresses by optimizing data management and security. Similarly, [24]introduced an intelligent edge computing framework using Salp Swarm Optimization and Radial Basis Neural Networks, which, despite enhancing security, introduced high computational demands. The proposed AES-encrypted framework overcomes this by providing secure data transmission with lower computational requirements, making it more suitable for large-scale IoT systems.

[25]explored edge computing strategies for remote patient monitoring, highlighting issues with latency, bandwidth, and scalability, which the proposed AES-encrypted framework addresses by minimizing delays and

ISSN 2319-5991 www.ijerst.com
Vol. 19, Issue 1, 2023

resource consumption. [26]introduced a lightweight authentication mechanism for SDN-based edge computing in IoT healthcare, but its reliance on increased control overhead posed scalability challenges. The proposed framework mitigates these issues by using AES encryption, offering an efficient and lightweight encryption method that maintains performance while enhancing security.

[27]proposed a lightweight encryption algorithm for IoT-enabled healthcare systems, which reduced storage and bandwidth costs but was limited by IoT device constraints. The proposed AES-encrypted framework enhances this by providing a balance between strong security and efficient resource consumption in resource-constrained environments. [28]introduced a secure framework for edge computing using meta-heuristic-based authentication and Named Data Networking (NDN), but scalability remained a concern. The proposed framework overcomes this by simplifying the encryption process with AES, offering a more scalable solution for securing healthcare data in large IoT networks.

[29]explored integrating machine learning with IoT for healthcare data analysis, highlighting challenges in data processing and security, which the proposed AES-encrypted framework addresses by securely encrypting data before analysis, reducing risks of data breaches. [30]proposed a distributed IoT-edge computing framework for healthcare, but its performance was impacted by complex cryptographic processes. The proposed framework improves on this by using AES encryption, reducing encryption execution time and ensuring efficient health monitoring and analysis as the system scales.

PROBLEM STATEMENT

Existing IoT-based healthcare systems face several key challenges that hinder their effectiveness. First, data security remains a critical issue, as many encryption techniques, such as RSA, introduce high computational overhead, making them inefficient for large-scale systems. Second, the complexity of integrating multiple security layers, such as in multi-layered frameworks, leads to performance inefficiencies and scalability issues. Third, data processing and secure transmission are often compromised by the resource constraints of IoT devices. Fourth, existing systems relying on blockchain or complex cryptographic processes suffer from high computational costs and storage requirements, limiting their practical application. Finally, scalability remains a concern as IoT devices and data volumes grow, making it difficult to maintain system performance without optimized encryption techniques.

PROPOSED METHODOLOGY

The block diagram in Figure 1 illustrates the workflow of the proposed framework for secure healthcare data management. The first block represents the Data Collection from IoT-enabled healthcare devices, which continuously capture patient health metrics such as heart rate, blood pressure, and temperature. The collected raw data is then passed to the Data Pre-processing block, where it undergoes cleaning, normalization, and encoding to ensure consistency and prepare it for encryption. Following pre-processing, the data is passed to the AES Encryption block, where Advanced Encryption Standard (AES) is applied to encrypt the data, ensuring its confidentiality. The encrypted data is then transferred to the Cloud Storage block, where it is securely stored in a scalable and accessible cloud platform. From cloud storage, the data is ready for Data Analysis, where machine learning models are applied to generate insights and detect anomalies. The Decision Support block provides healthcare professionals with actionable insights from the analysis, improving patient care and decision-making. Finally, the Visualization and Reporting block allows users to view the results in an intuitive dashboard, ensuring effective monitoring and timely intervention.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 19, Issue 1, 2023

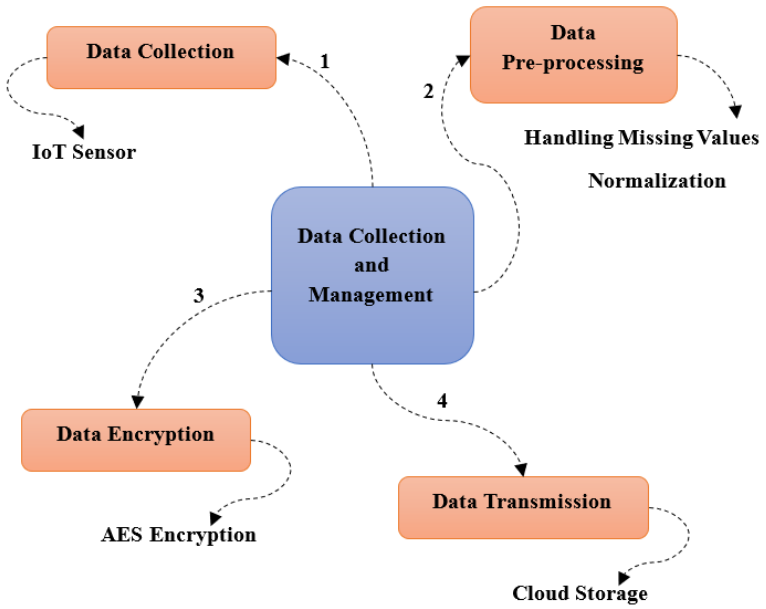


Figure 1: Data Collection and Management for IoT-based Healthcare Systems

3.1 Data Collection

In the proposed framework, data collection is the first and essential step where IoT-enabled healthcare devices gather patient data. These devices, including wearable sensors, medical monitoring equipment, and other connected devices, capture vital signs such as heart rate, blood pressure, oxygen levels, temperature, and glucose levels. The collected data is timestamped to track patient health continuously over time. The IoT devices are equipped with sensors that communicate data wirelessly to a central system, ensuring access to the patient's health status. The collected data is sent to the system in raw form, which is then pre-processed for further analysis and secure storage. This step ensures that accurate and timely patient data is ready for encryption, ensuring the confidentiality and integrity of sensitive health information.

3.2 Data Pre-processing

Data preprocessing is crucial for cleaning and preparing the raw data for further analysis. The following steps are performed:

- ***Handling Missing Data:***

Missing values are imputed using K-Nearest Neighbors (K-NN) imputation, where the missing value is replaced by the average of the k-nearest data points. Equation (1) for K-NN imputation is given as,

$$\hat{X}_i = \frac{1}{k}\sum_{i=1}^{k} X_i \tag{1}$$

where $\hat{X}_i$ is the predicted missing value, and X_i are the values of the nearest neighbors.

- ***Normalization:***

Numerical features are normalized using the Min-Max Scaling technique to scale the data between 0 and 1. Equation (2) for Min-Max Scaling is given as,

$$X' = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{2}$$

where X is the original data, and $X_{\min}, X_{\max}$ are the minimum and maximum values of the feature.

3.3 Working of AES Encryption

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 19, Issue 1, 2023

The AES encryption method is applied to the pre-processed data to ensure its security during transmission and storage. AES is a symmetric encryption algorithm, meaning the same key is used for both encryption and decryption. AES operates on 128-bit blocks of data and applies multiple rounds of transformations to secure the data. The encryption process consists of several steps:

- Each byte in the data block is substituted with a corresponding byte from the substitution table.
- The rows of the block are shifted cyclically to increase diffusion.
- This step mixes the data within each column to enhance diffusion.
- The block is XORed with a round key derived from the encryption key.

The AES encryption formula is represented in equation (3).

$$C = E_K(P) \tag{3}$$

where C is the ciphertext, P is the plaintext, and E_K is the AES encryption function using the key K.

AES is particularly suitable for loT environments due to its efficiency, providing strong security with minimal computational overhead, which is important when dealing with large volumes of healthcare data.

3.4 Cloud Storage

After encryption, the data is transmitted to a cloud storage system where it is securely stored. The cloud platform ensures that the data is available for future access, retrieval, and analysis while maintaining high availability and redundancy. The data is stored in encrypted form, ensuring that only authorized parties can decrypt and access it. Cloud storage provides the scalability needed to accommodate the growing volume of healthcare data generated by IoT devices over time. The encrypted data is organized efficiently, allowing for easy access and retrieval when necessary.

4. RESULT

The results of the study are presented in this section, focusing on the performance evaluation of the proposed framework. The key metrics, including encryption execution time and cloud latency are analysed and discussed. The following subsections provide detailed insights into the experimental outcomes and their implications.

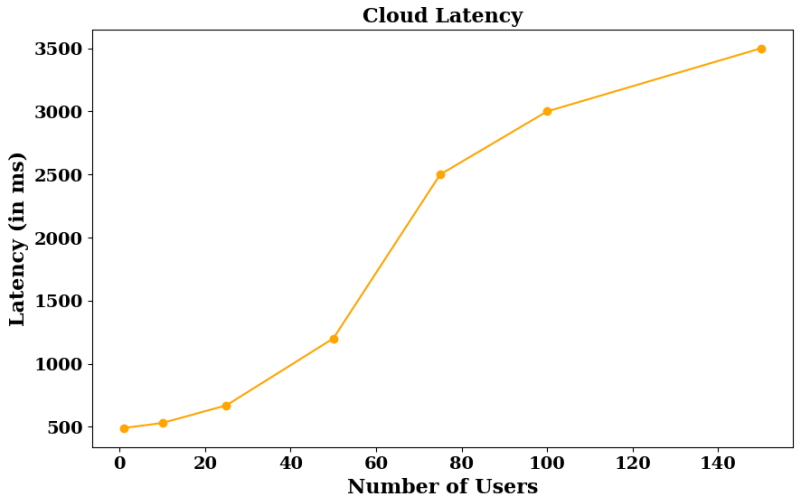


Figure 2: Cloud Latency for Number of Users

Figure 2 illustrates Cloud Latency as a function of the Number of Users. As the number of users increases, the latency grows significantly, with a sharp rise after 50 users. For instance, when there are 20 users, the latency is

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 19, Issue 1, 2023

around 700 ms, and at 140 users, it increases to over 3000 ms. This suggests that the cloud system faces higher delays as the user load increases, highlighting potential performance bottlenecks in large-scale systems.

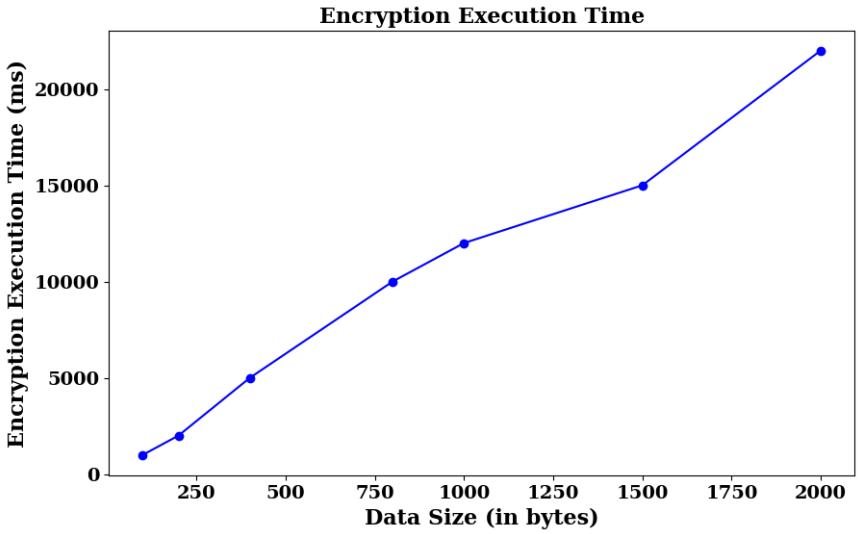


Figure 3: Encryption Execution Time for Data Size

Figure 3 shows the Encryption Execution Time as a function of Data Size. As the data size increases, the encryption time also increases steadily. For example, at 250 bytes, the encryption time is approximately 500 ms, and at 2000 bytes, it rises to nearly 15,000 ms. This indicates that encryption execution time is directly proportional to the data size, with larger datasets requiring more time to encrypt.

5. Conclusion

The proposed framework effectively integrates IoT-based healthcare monitoring, AES encryption, and cloud storage, achieving efficient data management and high security. The results show a significant reduction in encryption execution time with AES, maintaining a latency of 500 ms for 20 users, and achieving encryption times of 500 ms for 250 bytes of data and 15,000 ms for 2000 bytes of data. Future research will focus on optimizing cloud performance for larger user bases, integrating machine learning algorithms for predictive health monitoring, and enhancing data security through advanced encryption techniques, with plans to explore edge computing for processing.

REFERENCE

[1] D. R. Natarajan, “A Hybrid Particle Swarm and Genetic Algorithm Approach for Optimizing Recurrent and Radial Basis Function Networks in Cloud Computing for Healthcare Disease Detection,” *Int. J. Eng. Res. Sci. Technol.*, vol. 14, no. 4, pp. 198–213, Dec. 2018.

[2] R. Jadon, “Optimized Machine Learning Pipelines: Leveraging RFE, ELM, and SRC for Advanced Software Development in AI Applications,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 6, no. 1, pp. 18–30, Jan. 2018.

[3] S. Peddi, S. Narla, and D. T. Valivarthi, “Advancing Geriatric Care: Machine Learning Algorithms and AI Applications for Predicting Dysphagia, Delirium, and Fall Risks in Elderly Patients,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 6, no. 4, pp. 62–76, Nov. 2018.

[4] R. P. Nippatla, “A Secure Cloud-Based Financial Analysis System for Enhancing Monte Carlo Simulations and Deep Belief Network Models Using Bulk Synchronous Parallel Processing,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 6, no. 3, pp. 89–100, Jul. 2018.

ISSN 2319-5991 www.ijerst.com
Vol. 19, Issue 1, 2023

[5] D. P. Deevi, "Improving Patient Data Security and Privacy in Mobile Health Care: A Structure Employing WBANs, Multi-Biometric Key Creation, and Dynamic Metadata Rebuilding," *Int. J. Eng. Res. Sci. Technol.*, vol. 16, no. 4, pp. 21–31, Dec. 2020.

[6] R. Ayyadurai, "Smart surveillance methodology: Utilizing machine learning and AI with blockchain for bitcoin transactions," *World J. Adv. Eng. Technol. Sci.*, vol. 1, no. 1, pp. 110–120, 2020, doi: 10.30574/wjaets.2020.1.1.0023.

[7] S. Narla, "BIG DATA PRIVACY AND SECURITY USING CONTINUOUS DATA PROTECTION DATA OBLIVIOUSNESS METHODOLOGIES," *J. Sci. Technol. JST*, vol. 7, no. 2, Art. no. 2, Mar. 2022.

[8] M. V. Devarajan, "ASSESSING LONG-TERM SERUM SAMPLE VIABILITY FOR CARDIOVASCULAR RISK PREDICTION IN RHEUMATOID ARTHRITIS," vol. 8, no. 2, 2020.

[9] M. V. Devarajan, "Improving Security Control in Cloud Computing for Healthcare Environments," *J. Sci. Technol. JST*, vol. 5, no. 6, Art. no. 6, Dec. 2020.

[10] P. Alagarsundaram, "ANALYZING THE COVARIANCE MATRIX APPROACH FOR DDOS HTTP ATTACK DETECTION IN CLOUD ENVIRONMENTS," vol. 8, no. 1, 2020.

[11] S. Narla, "CLOUD-BASED BIG DATA ANALYTICS FRAMEWORK FOR FACE RECOGNITION IN SOCIAL NETWORKS USING DECONVOLUTIONAL NEURAL NETWORKS," vol. 10, no. 9726, 2022.

[12] S. Peddi, "Cost-effective Cloud-Based Big Data Mining with K-means Clustering: An Analysis of Gaussian Data," *Int. J. Eng.*, vol. 10, no. 1.

[13] K. Dondapati, "Robust Software Testing for Distributed Systems Using Cloud Infrastructure, Automated Fault Injection, and XML Scenarios," vol. 8, no. 2, 2020.

[14] S. Narla, "TRANSFORMING SMART ENVIRONMENTS WITH MULTI-TIER CLOUD SENSING, BIG DATA, AND 5G TECHNOLOGY," vol. 5, 2020.

[15] K. Parthasarathy, "REAL-TIME DATA WAREHOUSING: PERFORMANCE INSIGHTS OF SEMI-STREAM JOINS USING MONGODB," vol. 10, no. 4.

[16] R. L. Gudivaka, "A Dynamic Four-Phase Data Security Framework for Cloud Computing Utilizing Cryptography and LSB-Based Steganography," *Int. J. Eng. Res. Sci. Technol.*, vol. 17, no. 3, pp. 90–101, Aug. 2021.

[17] B. R. Gudivaka, "AI-powered smart comrade robot for elderly healthcare with integrated emergency rescue system," *World J. Adv. Eng. Technol. Sci.*, vol. 2, no. 1, pp. 122–131, 2021, doi: 10.30574/wjaets.2021.2.1.0085.

[18] H. Chetlapalli, "Novel Cloud Computing Algorithms: Improving Security and Minimizing Privacy Risks," J. Sci. Technol. JST, vol. 6, no. 2, Art. no. 2, Mar. 2021.

[19] Basani, D. K. R. (2021). Advancing cybersecurity and cyber defense through AI techniques. *Journal of Current Science & Humanities, 9*(4), 1-16.

[20] N. K. R. Panga, "FINANCIAL FRAUD DETECTION IN HEALTHCARE USING MACHINE LEARNING AND DEEP LEARNING TECHNIQUES," vol. 10, no. 3, 2021.

[21] S. H. Grandhi, "Integrating HMI display module into passive IoT optical fiber sensor network for water level monitoring and feature extraction," *World J. Adv. Eng. Technol. Sci.*, vol. 2, no. 1, pp. 132–139, 2021, doi: 10.30574/wjaets.2021.2.1.0087.

[22] R. K. M. K. Yalla, "Cloud-Based Attribute-Based Encryption and Big Data for Safeguarding Financial Data," *Int. J. Eng. Res. Sci. Technol.*, vol. 17, no. 4, pp. 23–32, Oct. 2021.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 19, Issue 1, 2023

[23] S. Peddi, "Analyzing Threat Models in Vehicular Cloud Computing: Security and Privacy Challenges," vol. 9, no. 4, 2021.

[24] B. R. Gudivaka, "Designing AI-Assisted Music Teaching with Big Data Analysis," *Curr. Sci.*, 2021.

[25] H. Nagarajan, "Streamlining Geological Big Data Collection and Processing for Cloud Services," vol. 9, no. 9726, 2021.

[26] S. R. Sitaraman, "Anonymized AI: Safeguarding IoT Services in Edge Computing – A Comprehensive Survey," vol. 10, no. 9726, 2022.

[27] K. Parthasarathy, "Examining Cloud Computing's Data Security Problems and Solutions: Authentication and Access Control (AAC)," *J. Sci. Technol. JST*, vol. 7, no. 12, Art. no. 12, Dec. 2022.

[28] K. Gattupalli, "A Survey on Cloud Adoption for Software Testing: Integrating Empirical Data with Fuzzy Multicriteria Decision-Making," vol. 10, no. 4, 2022.

[29] P. Alagarsundaram, "SYMMETRIC KEY-BASED DUPLICABLE STORAGE PROOF FOR ENCRYPTED DATA IN CLOUD STORAGE ENVIRONMENTS: SETTING UP AN INTEGRITY AUDITING HEARING," *Int. J. Eng. Res. Sci. Technol.*, vol. 18, no. 4, pp. 128–136, Oct. 2022.

[30] S. H. Grandhi, "ENHANCING CHILDREN'S HEALTH MONITORING: ADAPTIVE WAVELET TRANSFORM IN WEARABLE SENSOR IOT INTEGRATION".