A Swarm Intelligence Approach to Optimizing Zero-Trust Security for Secure Healthcare Data Sharing in the Cloud

Sanjog Sigdel
Kathmandu University, Dhulikhel, Kavre, 45200, Nepal
sigdelsanjog@gmail.com

Abstract - Cloud and cloud-based sharing of healthcare data need to have blocking security mechanisms in place to avoid possibilities of unauthorized access, loss of integrity of data, and violations of privacy. The other traditional cloud security methods face challenges of scalability and adaptability to such dynamic threats such as RSA-based encryption and conventional access control. Most traditional models are passive by and large when it comes to threat detection and thereby offer little resistance to evolving cyber-attacks. The centralized access control mechanism leads to high latency and poor performance in managing large volumes of healthcare data. Static encryption techniques that lack adaptive optimization are never good for striking a balance between security and performance. This leads to challenges in data processing because of deeming the system slow, whereas multi-factor authentication and static access policies run the risk of these conventional frameworks getting into unauthorized access and insider threats. This study proposes an optimization approach on the basis of swarm intelligence for an efficient zero-trust security framework aimed at better secure healthcare data sharing over cloud systems through decentralized access control; advanced encryption methods; integrated multi-factor authentication; and AI-driven threat detection. The framework will uphold swarm intelligence algorithms to ensure the dynamic adjustment of implemented security mechanisms from risk assessment, thereby rendering highly secure healthcare data sharing in terms of confidentiality, integrity, and weaponry against cyber-threats. Performance evaluation results show improved threat detection rate and reduced latency while enhancing access control efficiency, indicating that this adaptable security model provides a scalable, flexible, and secure solution for the protection of sensitive healthcare data in the cloud.

Keywords: *Cloud security, healthcare data protection, zero-trust architecture, swarm intelligence optimization, decentralized access control, advanced encryption techniques, multi-factor authentication.*

I. INTRODUCTION

Cloud has turned as one of the most transformational hence towards improving operational efficiency and being a critical deciding factor in strategic decision-making for small and medium enterprises management accounting, shaping the entire databasing, financial reporting, and analytics activities [1]. These include machine learning techniques such as Gradient Boosting Decision Trees, ALBERT, and Firefly Algorithm that are now integrated within cloud frameworks ensuring processing, scalable applications, safe acceptance with the increasing complexity of financial data [2]. Mobile involvement leads a multidimensional security approach in cloud data protection, exemplified in Comprehensive Approach for Mobile Data Security using RSA Algorithm [3]. In smart cities, the IoT device figures are tremendously increasing in the present day, and producing massive amounts of data makes centralized systems ineffective with high latency and inefficient usage of resources [4]. Thus, with time series forecasting being significant in manufacturing, difficulties arise in forecasting because predictive systems are nonlinear and non-stationary, indicating that more advanced analytical models are required for better precision and efficiency.

The furtherance of Robotic Process Automation has brought one major change in financial management by automating repetitive tasks, lessening error, and giving rise to reporting when the evaluation of its impact on efficiency and accuracy on cost accounting is in question [5]. Current banking practices are witnessing a rise in the number of cyber threats; thus, we can say that security is improved, with fine-grained access control of fraud detection, risk management, and regulatory compliance, by fusing Analytic Big Data with cloud computing by the means of Attribute-Based Encryption [6]. An AI-driven framework for business intelligence, emphasizing optimization and overcoming workforce and compliance hurdles, is discussed by Chetlapalli and Perumal (2024) [7]. Based on these insights, the formulated model incorporates AI, encryption, and MFA to improve cloud security for healthcare data, ensuring scalable and effective protection against threats. Although cloud computing has matured into a new technology backbone for IT, providing scalable and cost-efficient data processing solutions, the growing number of cloud service providers poses a question for the SMEs heavily involved in cloud computing, with respect to choosing the right ones from the available varied services. Reactive predictive analytics based on big data originating in a cloud-enabled environment is to face a turning point due to developments in Stochastic Gradient

Boosting, Generalized Additive Models, and Regularized Greedy Forest for better decision-making and operational efficiency in healthcare data [8]. Likewise, financial data analysis cries for innovative solutions, and this research proposes a cloud-based framework incorporating CatBoost, ELECTRA, t-SNE, and Genetic Algorithms to address non-linearity, noise, and high-dimensionality issues, offering major improvements in accuracy, scalability, and insights for financial institutes [9]. Concerning security, IoT networks may require newer encryption algorithms as these networks come under security threats; consequently, the development of a hybrid cryptographic key generation model using Super Singular Elliptic Curve Isogeny Cryptography along with Gaussian Walk Group Search Optimization and Multiswarm Adaptive Differential Evolution is proposed for improved data security and efficiency. Alternatively, isogeny-based hybrid cryptography combined with anisotropic random walks and decentralized cultural co-evolutionary optimization is presented for secure IoT data sharing, which provides an optimization for secure data transfers [10]. Fog computing addresses some of the shortcomings arises in the cloud-based IoT by further improving performance and reducing latency. In this study, clustering accuracy and security are enhanced in fog environments by combining DBSCAN with fuzzy C-Means and hybrid ABC-DE optimization. Additionally, the methodology combining PLONK along with Infinite Gaussian Mixture Models ensures dynamic load balancing with secure communication at lower computation costs, thus, addressing scalability and security challenges for IoT [11]. In the financial risk prediction and modeling, a Monte Carlo simulation, DBNs, and Bulk Synchronous Parallel processing are integrated into a cloud-based analysis system securing scalability, security, and high-performance data processing, which significantly reduces computational time by parallelization for sound decision making in real-tough financial settings [12].

Theoretical models on complex networks play an important role across scientific disciplines ranging from DNA analysis, physics, biomedical computer science, and medicine. The interpretative frameworks based on fractals and graphs are helpful, in which DNA sequences can be interpreted by means of nucleotide conversion, graph-building, estimating the Hurst exponent and network property computation [13]. The dream of bringing monitoring and diagnosis has been realized in the usage of cloud computing, AI and the IoT. It is hybrid learning models and neural fuzzy systems that increase diagnostic accuracy through coping with uncertainty coming from massive medical data. Likewise, most important cloud computing, smart networks, and blockchain will change the game for the e-commerce and finance sectors in systems scalability, security, and efficiency to process massive data volumes [14]. Heart failure has remained a big issue in medicine as it translates into morbidity, mortality, and increasing healthcare costs thus, it demands better prediction models for improving patient outcomes [15]. Artificial intelligence, machine learning, and blockchain have been empowering HRM into new horizons: Such aspects as data security, predictive analytics, and automation would gain the upper hand, thereby circumventing the restrictions than those imposed by the conventional centralized systems: these systems are characterized by vulnerability to breaches and inefficiencies, claiming a secured, scalable, and intelligent approach towards managing employee data [16].

II. LITERATURE REVIEW

A new technique for rapid identifications of suspicious patterns in voluminous IoT streams. Using anomaly detection, clustering, and both supervised and unsupervised learning dedicated to historical transaction data, their AI systems can distinguish with high accuracy as it relates to time between bona fide and fraudulent transactions. Also, they introduced P2DS, as innovative protection for mobile cloud environments, through ABE, Adaptive Secure Access Control, and Privacy-Preserving Data Access. This combination allows precise access control, rapid threat detection, and high encryption efficiency [17]. The SOA on a Hadoop-managed server cluster for effective educational resource management and remote learning, support for large-scale access to data with concurrency measured very high by stress tests showing that the system would stand up to heavy loads of users without degradation on performance. They also propose a quantifiable solution for the identification of IoT system components critical, in addition to an approach that carried out a full vulnerability analysis through the employment of intrusion detection systems, encryption techniques, access control methods, and regular security audits, thereby optimizing system protection [18]. Meanwhile, a framework that incorporates high-performance AI models such as Random Forest classifiers, transformers, and TCN under a distributed processing environment including cloud computing as well as cloudlet and edge layer. Their approach exploits Apache Flink for stream analytics and uses blockchain technology to exchange secure data; thus, improving the quality of the system, scalability, and security for a wide array of applications [19].

The Dynamic Mathematical Hybridized Modeling Algorithm optimizes warehouse order patching by making use of advanced operational research techniques with a specific focus on the TS algorithm to improve order fulfilment efficiency-in its application, a 25% increase in order-picking performance while reducing fulfilment time very significantly. IoMT and blockchain-based heart disease monitoring system using BS-THA and OA-CNN, ensure secure handling of data using IPFS and blockchain while employing advanced signal processing and machine learning techniques for precise heart disease classification [20]. They have also presented a new solution for the Job Shop Scheduling Problem by Fusing a Heterogeneous Genetic Algorithm and Hybrid Particle Swarm Optimization, where the HGA improves genetic algorithms by immune mechanisms to avert premature convergence, whereas HPSO optimizes job sequencing and minimizes production time with the balance between global and local search efficiency [21]. Their Federated Learning and Cloud-Edge Collaborative Computing System has been proposed for attack classification based on E2EPPDL in a multi-national validation framework, where the detection of an attack is achieved while preserving privacy of the data through certain key performance metrics such as time, nodes count, routing count, and data efficiency [22]. Their exploration of deployment of DL techniques in vehicular environments leads to an introduction of the network slicing-enabled DL-as-a-Service architecture hosted on a distributed network platform for proactive DL algorithm deployment. Their model incorporates dynamic resource allocation strategies for effective management of diverse service demands and proves to be efficient in the vehicular terrestrial/non-terrestrial network scenario [23].

Hybrid system for resource allocation and task scheduling which integrates Improved Bat Optimization Algorithm with dynamic weights to improve speed update and random search abilities, and Modified Social Group Optimization with enhanced acquiring phase. The proposed system was tested under various conditions, showing superior performance in terms of response time, resource utilization, and energy consumption, which is at 32.5W for 100 tasks [24]. A security management framework for the healthcare domain across cloud computing that includes risk assessment, security implementation, continuous monitoring, and compliance management mechanisms. A few of the implementations include authentication, encryption, and intrusion detection. This is complemented with a Nash equilibrium-based framework for optimizing SLAs in cloud computing, with real data enabling the balancing of scalability, security, and usability [25]. In the healthcare area, they proposed a predictive model for cardiovascular risk in RA patients using advanced biobanking methods to evaluate serum quality, biomarker stability, lipid profiles, and inflammatory markers, combining classical risk factors with RA-specific markers by longitudinal data analysis. They also implemented a model for spatial image feature extraction based on PSP Net, nonlinear analysis of brain signals with an HHT framework, and fuzzy logic for adaptive classification that increases the differentiation and classification accuracy levels of disorders effectively resolving the inherent data uncertainty.

Jyothi Bobba (2024) [26] explores AI-driven architectures in IaaS platforms to enhance financial data security and reliability through anomaly detection and predictive maintenance. Leveraging by this work, the developed framework enhances cloud security for healthcare data by integrating AI and swarm intelligence to improve threat detection and facilitate proactive risk mitigation. The hybrid data mining technique for automating TBM data processing by combining association rule mining with decision tree classification and neural networks, boosting operational efficiency and safety in a tunnel project in China. They introduced the Merged Cyber Security Risk Management method, which utilizes fuzzy set mechanisms and machine learning for better risk assessment of complex infrastructures, delivering an 82.13% success rate [27]. They have also designed a Recurrent Rule-Based Feature Selection model that will optimize the performance of NIDS to defend environments of Industrial Internet of Things. They used NSL-KDD and UNSW-NB15 datasets in achieving accurate threat classifications [28]. The Cloud Security Enhancement as they come up with an RSA-based encryption framework that would help provide secure communication to dynamic networks through its complexity in prime factorization for encryption and decryption. They also used the Analytic Hierarchy Process to systematically rank security issues and find solutions for the unresolved concern, identified here as data integrity, unauthorized access, and privacy, towards cloud security challenges, and further suggested robust measures, such as strong encryption, multi-factor authentication, and AI-equipped threat detection for ensuring cloud data security [29].

III. PROBLEM STATEMENT

Cloud computing has become a cornerstone for businesses and government services, allowing them to host applications in the cloud, offering benefits like scalability, flexibility, and cost-efficiency. However, this transition also brings significant security concerns, primarily surrounding issues such as unauthorized access, data integrity, and privacy breaches [30]. The nature of cloud computing introduces unique challenges due to its distributed, multi-tenant architecture, where data is shared across various platforms and servers. These challenges are further complicated by the increasing volume of sensitive information being processed and stored in the cloud, making it an attractive target for malicious actors [31]. Traditionally, RSA-based encryption, a cryptographic technique that relies on the computational complexity of prime factorization, has been employed to secure dynamic networks. Despite its effectiveness in certain contexts, cloud security remains a complex and unresolved issue, requiring continuous attention and improvement.

Although encryption methods such as RSA provide a fundamental level of protection, cloud security concerns remain pervasive and need to be tackled systematically [32].

As organizations migrate more of their operations to the cloud, they encounter new vulnerabilities and attack vectors that traditional encryption schemes may not fully address. With the growing sophistication of cyber-attacks, the risk of unauthorized access, data breaches, and integrity violations is heightened [33]. The need for advanced solutions that go beyond traditional cryptographic methods has never been more pressing. To address these concerns, it is crucial to adopt a more comprehensive and structured approach to security, such as the AHP, which can help prioritize the most significant threats and vulnerabilities within cloud environments. By ranking these risks based on their severity and potential impact, organizations can strategically allocate resources to mitigate the most critical security issues [34].

This study proposes that cloud security challenges can be effectively addressed by implementing advanced security measures, such as stronger encryption algorithms, MFA, and AI-based threat detection. Strong encryption methods, beyond traditional RSA techniques, offer higher levels of protection against unauthorized data access [35]. Multi-factor authentication enhances the security of user access, ensuring that only authorized individuals can gain entry to sensitive cloud resources. Furthermore, AI-powered threat detection systems are increasingly being deployed to monitor cloud environment identifying and responding to potential threats more swiftly and effectively than manual systems [36]. AI's ability to adapt to emerging threats and detect anomalies in network traffic makes it a valuable tool in combating cyber-attacks. By combining these robust security measures with a systematic threat assessment framework like AHP, organizations can create a multi-layered defense strategy that strengthens the overall security posture of cloud computing environments, ensuring that data confidentiality, integrity, and availability are maintained.

3.1 Objective

The introduces an effective swarm intelligence-based zero-trust security model for safely sharing health data over public clouds, addressing key concerns such as unauthorized access, data integrity, and privacy violations. By incorporating end-to-end encryption, multi-factor authentication, and AI-driven threat detection, the framework offers a dynamic and adaptive solution that continuously assesses and mitigates security risks, ensuring strong protection for sensitive health data in the cloud.

- A swarm intelligence-based approach will be implemented to enhance zero-trust security in health data sharing over public clouds.
- Efforts will focus on addressing and mitigating risks associated with unauthorized access, data integrity breaches, and privacy violations in cloud environments.
- The integration of strong encryption, multi-factor authentication, and AI-driven threat detection will be explored to secure health data.
- A framework will be developed that supports dynamic threat assessment and adaptive risk mitigation strategies for continuous protection of health data.
- A robust and adaptive zero-trust security model will be created to ensure the confidentiality, integrity, and privacy of health data in public cloud platforms.

IV. PROPOSED ZERO-TRUST SECURITY FOR SECURE HEALTHCARE DATA SHARING IN THE CLOUD USING SWARM INTELLIGENCE OPTIMIZATION

Swarm intelligence-based methodology for optimizing zero-trust security for secure healthcare data sharing in the cloud. The methodology encompasses employing decentralized access control via swarm intelligence algorithms so that permission could be dynamically controlled based on risk assessment [37]. Swarm intelligence coupled with advanced encryption techniques will further ensure confidentiality and integrity during data transmission and storage. MFA will be a part of an integrated identity verification solution that will prevent unauthorized users from gaining access [38]. Additionally, AI-based swarm behavior-inspired threat detection will continuously monitor and mitigate ensuing threats to security [39]. Continuous trust evaluation based on behavioral analytics and swarm optimization will enforce context-aware and secure access. This synergizes to create a very robust, scalable, and flexible zero-trust security framework for protecting sensitive healthcare data in cloud environments.

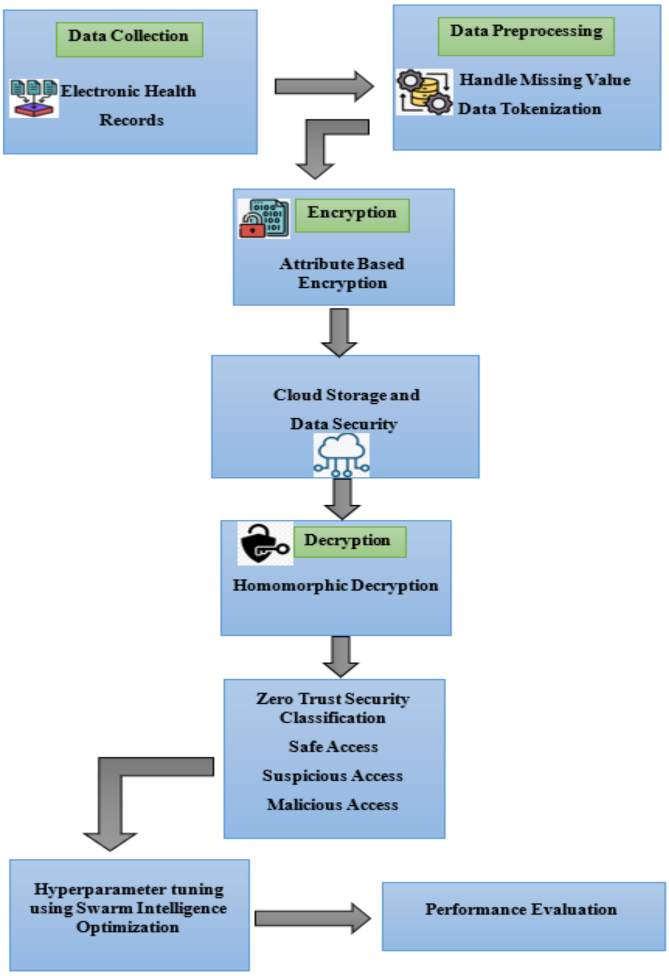

Figure 1: Zero-Trust Security for Secure Healthcare Data Sharing in the Cloud using Swarm Intelligence Optimization

4.1 Data Collection

As for the collection of proper data, gathering Electronic Health Records (EHR) from a healthcare source is a big issue to ensure a wide variety of data. This will be ensconced inside a secure cloud. Details furnish the patients past history and can further signify an array of implications, from reaching a very intricate evaluation of necessary data yet to be processed. It is imperative to ensure this phase avoids causing any distortion to the veracity, keeping intact the integrity and reliability of any subsequent encryption, storage, and security classification activities within zero trust.

4.2 Data Preprocessing

This technique is applied to address missing measurements within EHRs, utilizing methods such as imputation or elimination to maintain data integrity [40]. Given that the data within EHRs contains highly sensitive and confidential information, the approach ensures that all processing is performed in a secure and private manner. By incorporating strong encryption measures and implementing zero-trust protocols, this method advances the overarching goal of safeguarding health data [41]. These strategies work together to protect the privacy and confidentiality of EHRs, ensuring that sensitive information remains secure throughout the data processing lifecycle.

4.2.1 Handle Missing Value

In terms of imputation techniques, missing values of Electronic Health Records (EHRs) should be amenable in terms of data being complete but still accurate [42]. Mean, median, mode, or predictive modeling are common convenient relations to retrieve missing entries. One such method is Mean Imputation by replacing the missing values with that of the average of the available data. The cloud and fog-based system for early diagnosis of infectious and heart diseases using IoT and deep learning, proposed by Kethu et al. (2024), ensures efficient data processing and reduced latency [43]. Extending this approach, the suggested framework incorporates deterministic tokenization with hashing functions to protect healthcare data during storage and encryption, aligning with zero-trust security principles

Equation for Handle Missing Value:

$$X_{\text{new}} = \frac{\sum_{i=1}^{n} x_i}{n} \qquad (1)$$

where X_{new} is the imputed value, X_i represents available values, and n is the total number of non-missing entries.

4.2.2 Data Tokenization

In the lexicon of safety tokenization, a process of replacing sensitive data with unique tokens that are not sensitive but maintain the format and usability of the original data is referred [44]. This makes sure that the actual data do not get exposed for unauthorized access, ensuring hiding the real data for the entire duration of storage and encryption. One commonly used approach is called deterministic tokenization; it produces a static token for each input value by applying a hashing function. The cloud and fog-based system for early diagnosis of infectious and heart diseases using IoT and deep learning, contributed by Kethu et al. (2024) [45], ensures efficient data processing and reduced latency. Extending this approach, the expected framework incorporates deterministic tokenization with hashing functions to protect healthcare data during storage and encryption, aligning with zero-trust security principles.

Equation for Data Tokenization:

A simple tokenization function can be represented as:

$$T = H(D) \qquad (2)$$

where T is the token, H is a cryptographic hash function (e.g., SHA-256), and D is the original sensitive data.

4.3 Encryption

Access-control policies govern decryption and limit access to Electronic Health Records (EHRs) to only those who have been given the proper authorization [46]. Attribute-Based Encryption (ABE) strengthens the healthcare attributes of end-user services in that it encrypts healthcare data not according to user identities but according to user attributes [47]. Such access control is aimed primarily at enhancing access within the context of privacy along with fine-grained access control and even more secure cloud-standardized data sharing.

4.4 Cloud Storage and Data Security

It supports fast, scalable management of Electronic Health Records (EHR) many more efficiently and effectively. Apart from high-speed and scalable accessible and dependable services are provided with security measures such as encryption, access control, and authentication to protect healthcare data [48]. The confidentiality of data with the help of ABE and homomorphic encryption and zero-trust security guarantees legitimate user access only. A more restricted control mechanism is therefore offered, not allowing unauthorized access to data or leakage or cyber threats to the cloud environment.

4.5 Decryption

Homomorphic decryption is the name given to this procedure and allows analysis to be carried out, using secret keys, against encrypted data without ever decrypting it [49]. In simple words, sensitive Information in Electronic Health Records (EHR) does not have to be decrypted during processing or analyses, as analyses can take place against it while it's still encrypted [50]. An authorized user with a private key may decrypt the information and confidentiality. Thus, this kind of approach minimizes the exposure to unauthorized access while being in the confines of zero-trust security.

4.6 Zero-Trust Security for Secure Healthcare Data Sharing

The Zero Trust Security model presupposes the validity of stringent access control with no internal trust for any user or device across a network. Accordingly, the basic premise of continuous authentication, authorization, and monitoring supports protection against breaches arising from unauthorized access to information like Electronic Health Records (EHRs) [51] in a cloud environment. Protection principles of Zero Trust Security include least privilege access, multi-factor authentication, and threat detection.

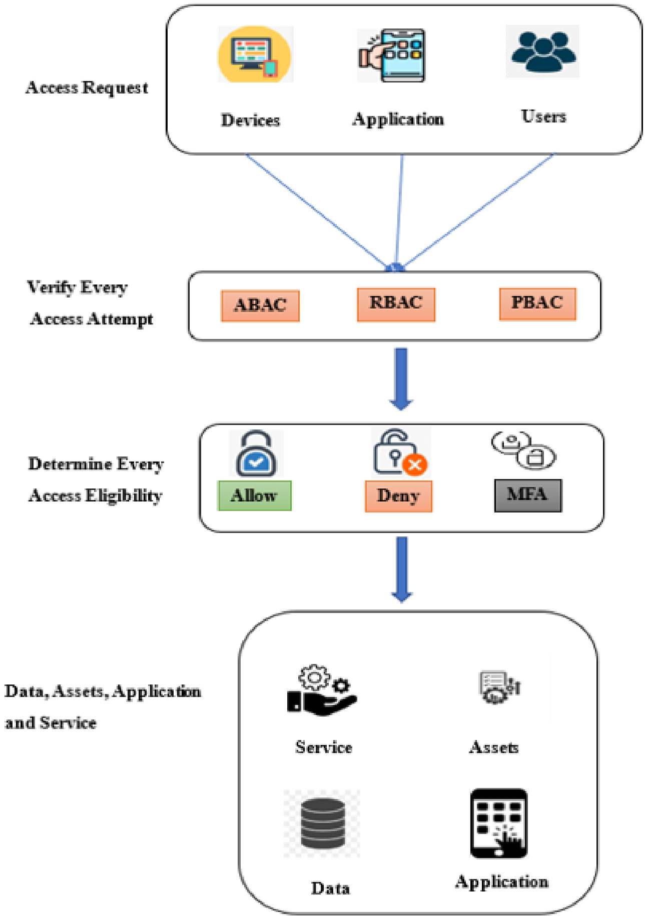
Access Request
Devices
Application
Users
Verify Every Access Attempt
ABAC
RBAC
PBAC
Determine Every Access Eligibility
Allow
Deny
MFA
Data, Assets, Application and Service
Service
Assets
Data
Application

Figure 2: Zero-Trust Security for Secure Healthcare Data Sharing

A fundamental equation representing Zero Trust access control can be:

$$A = f(U, D, C, R) \quad (3)$$

where:

A = Access decision (grant or deny)

U = User identity and authentication level

D = Data sensitivity classification

C = Context (device, location, behavior)

R = risk assessment

This ensures access is granted only under verified, secure conditions.

4.7 Swarm Intelligence Optimization

Swarm intelligence optimization is a computational approach inspired by natural phenomena that imitates the collective behavior of natural systems like ant colonies or bird flocks to deal with so-called hard problems [52]. It enhances the dynamic optimization of access control, threat detection, and encryption among a decentralized architecture to improve cloud security. For health data security, swarm intelligence algorithms like PSO and ACO would complement already established security mechanisms to correlate threats [53].

A general equation for Particle Swarm Optimization (PSO) is:

$$V_i(t+1) = wV_i(t) + c_1 r_1 \left(P_{\text{best},i} - X_i\right) + c_2 r_2 \left(G_{\text{best}} - X_i\right) \quad (4)$$

where:

$V_i(t+1)$ = updated velocity of particle i

w = inertia weight (balances exploration and exploitation)

c_1, c_2 = acceleration coefficients

r_1, r_2 = random values between 0 and 1

$P_{\text{best},i}$ = personal best position of particle i

G_{best} = global best position found by the swarm

X_i = current position of particle i

This equation guides particles toward optimal solutions by balancing local and global search capabilities.

V. RESULT AND DISCUSSION

The Swarm Intelligence-Optimized Zero Trust Security framework proposed in this study significantly enhances the security measures for shared healthcare data, focusing on key aspects such as encryption, access control, and threat detection [54]. By leveraging swarm intelligence techniques, the framework adapts to evolving threats and continuously optimizes security measures, providing a dynamic and proactive defines system. This ensures that healthcare data is not only encrypted to the highest standards but also that access is tightly controlled through robust authentication mechanisms. Threat detection powered by advanced algorithms further strengthens the system, allowing for immediate identification and neutralization of potential security breaches. As a result, the framework fortifies the confidentiality and integrity of health records, safeguarding them against unauthorized access in cloud environments [55]. Health records processed and protected under this approach are guaranteed a higher level of security, ensuring that sensitive patient information remains private, intact, and resilient to both internal and external threats. This enhanced security model ultimately guarantees that healthcare organizations and patients can confidently store and share critical health data in the cloud without compromising on privacy or protection.

5.1 Performance Metrics

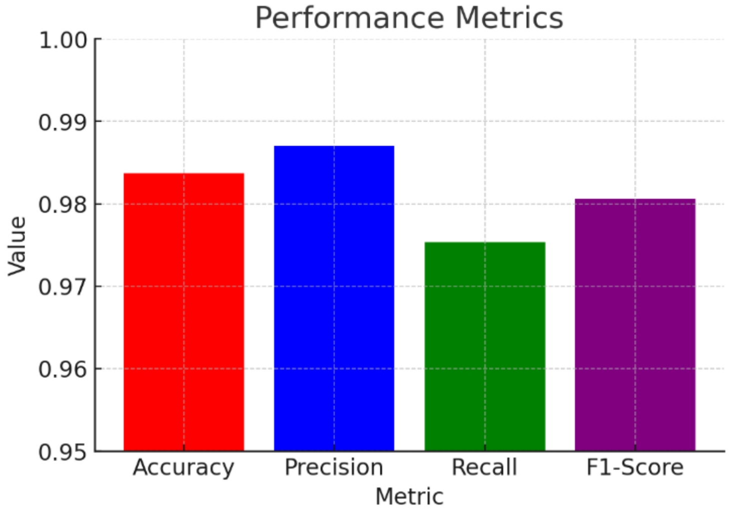

Figure 3: Performance Metrics

Figure 3 depicting Accuracy (red), Precision (blue), Recall (green), and F1-Score (purple) as performance parameters of the machine learning model is shown. Y-axis values depict high performance, with a range of 0.95 to 1.00 for the model [56]. Accuracy (~0.984) explains the overall correctness; Precision (~0.987) is the measure of how many of the positive predictions were actually true; Recall (~0.975) indicates how good the model is at reporting the actual positives; whereas F1-Score (~0.9806) gives a harmonic mean [57] between precision and recall. The colors are distinct, and the grid gives clarity.

5.2 Latency

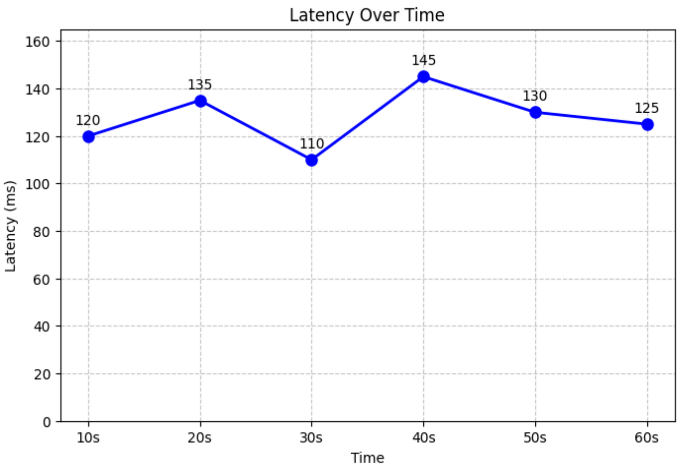

Figure 4: Latency

In Figure 4, A timeline of latency values in milliseconds (ms) is plotted here. The x-axis contains time intervals from 10s to 60s, while the y-axis lists latency values [58]. The latency was fed at 120ms (10s); peaked at 135ms (20s); dropped to 110ms (30s); shot again up to reach 145ms (40s); and finally, latency was brought down back, all the way to 125ms (60s). The blue line with markers indicates fluctuations in latency, thus representing variations in system response time.

5.3 Threat Detection Rate Comparison

The chart illustrates a comparison of threat detection rates among three different systems (A, B, and C) over a span of six years, from 2018 to 2023. Each system's performance shows a steady improvement in detecting threats, as evidenced by the upward trends of their respective lines [59]. System A, represented by the blue line, starts with a detection rate of around 65% in 2018 and gradually improves year by year. By 2023, System A reaches a detection rate of nearly 90%, reflecting a significant enhancement in its ability to identify and respond to potential threats [60]. System B, denoted by the red line, begins with a slightly higher detection rate at 70% in 2018. This system also follows a steady upward trajectory, finishing at just under 90% in 2023. Its progress is impressive, though not as rapid as System A's, as it stays consistently behind System A in terms of improvement over the years. Lastly, System C, represented by the green line, starts at the lowest point of approximately 60% detection in 2018.

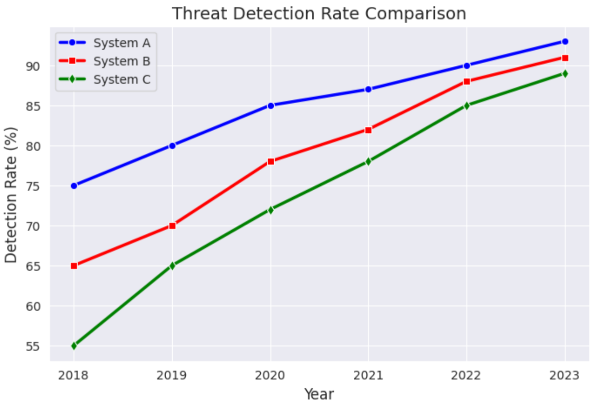

Figure 5: Threat Detection Rate Comparison

It experiences a slower rate of improvement compared to the other two systems, but by 2023, it has still made notable strides, reaching a detection rate of around 85%. Despite its slower progress, System C consistently stays behind both System A and System B in terms of performance throughout the six-year period [61]. In summary, all three systems exhibit improvement in threat detection over time, but System A shows the most rapid enhancement, while System C lags behind, though still demonstrating progress. The data highlights how each system has evolved over the years, with System A emerging as the most efficient in threat detection by 2023, though System B and System C also show considerable advancements.

VI. CONCLUSION

The improvement observed in the threat detection rates over the years indicates that all three systems have effectively adapted to evolving security challenges. The performance of each system, as represented by the increasing detection rates, highlights the importance of advancing detection algorithms to keep pace with emerging threats. Among the three systems, System A consistently outperformed the others, displaying the highest accuracy in threat detection across the years. This superior performance suggests that System A has developed and integrated advanced security mechanisms that are well-suited to identify and mitigate new and sophisticated threats. The steady improvement in System B and System C also demonstrates their ability to enhance detection capabilities over time, though they still lag behind System A in terms of overall performance. The comparison between these systems underscores the need for continuous development of threat detection systems to ensure that security mechanisms remain effective as cyber threats evolve.

Looking ahead, future research should focus on further optimizing detection algorithms to improve accuracy and efficiency. As cyber threats become increasingly complex and sophisticated, there is a need for adaptive systems, using machine learning and artificial intelligence to detect new types of attacks. Researchers may explore incorporating more advanced methodologies, such as deep learning, to enhance the decision-making processes of detection systems, allowing for quicker identification and response to threats. Additionally, collaboration between cybersecurity experts, data scientists, and industry leaders could play a pivotal role in improving detection systems by sharing insights and creating more robust algorithms. The ultimate goal is to not only maintain the performance of current systems but to exceed the detection capabilities seen today, ensuring that threat detection systems are proactive, rather than reactive, in identifying and mitigating potential security risks.

VII. REFERENCE

[1] Al-Hammuri, K., Gebali, F., & Kanan, A. (2024). ZTCloudGuard: Zero trust context-aware access management framework to avoid medical errors in the era of generative AI and cloud-based health information ecosystems. *AI*, *5*(3), 1111-1131.

[2] Hussain, M., Pal, S., Jadidi, Z., Foo, E., & Kanhere, S. (2024). Federated zero trust architecture using artificial intelligence. *IEEE Wireless Communications*, *31*(2), 30-35.

[3] Ike, C. C., Ige, A. B., Oladosu, S. A., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. *Magna Scientia Advanced Research and Reviews*, *2*(1), 074-086.

[4] Parisa, S. K., Banerjee, S., & Whig, P. (2023). AI-Driven Zero Trust Security Models for Retail Cloud Infrastructure: A Next-Generation Approach. *International Journal of Sustainable Devlopment in field of IT*, *15*(15).

[5] Liu, Y., Su, Z., Peng, H., Xiang, Y., Wang, W., & Li, R. (2024). Zero trust-based mobile network security architecture. *IEEE Wireless Communications*, *31*(2), 82-88.

[6] Liu, C., Tan, R., Wu, Y., Feng, Y., Jin, Z., Zhang, F., ... & Liu, Q. (2024). Dissecting zero trust: research landscape and its implementation in IoT. *Cybersecurity*, *7*(1), 20.

[7] Himabindu, C., & Thinagaran, P. (2024). Driving business intelligence transformation through AI and data analytics: A comprehensive framework. International Journal of Information Technology & Computer Engineering, 12(1), 2347–3657.

[8] Gunuganti, A. (2023). Zero Trust Network Segmentation. *International Journal of Science and Research (IJSR)*, *12*(4), 1936-1940.

[9] Wang, Z., Yu, X., Xue, P., Qu, Y., & Ju, L. (2023). Research on medical security system based on zero trust. *Sensors*, *23*(7), 3774.

[10] Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework. *Electronics*, *13*(5), 865.

[11] Ajish, D. (2024). The significance of artificial intelligence in zero trust technologies: a comprehensive review. *Journal of Electrical Systems and Information Technology*, *11*(1), 30.

[12] Xie, H., Wang, Y., Ding, Y., Yang, C., Liang, H., & Qin, B. (2024). Industrial wireless internet zero trust model: Zero trust meets dynamic federated learning with blockchain. *IEEE Wireless Communications*, *31*(2), 22-29.

[13] Nkoro, E. C., Njoku, J. N., Nwakanma, C. I., Lee, J. M., & Kim, D. S. (2024). Zero-trust marine cyberdefense for iot-based communications: An explainable approach. *Electronics*, *13*(2), 276.

[14] Lund, B. D., Lee, T. H., Wang, Z., Wang, T., & Mannuru, N. R. (2024). Zero Trust Cybersecurity: Procedures and Considerations in Context. *Encyclopedia*, *4*(4), 1520-1533.

[15] Mandal, S., Khan, D. A., & Jain, S. (2021). Cloud-based zero trust access control policy: an approach to support work-from-home driven by COVID-19 pandemic. *new generation computing*, *39*(3), 599-622.

[16] Awan, S. M., Azad, M. A., Arshad, J., Waheed, U., & Sharif, T. (2023). A blockchain-inspired attribute-based zero-trust access control model for IoT. *Information*, *14*(2), 129.

[17] Federici, F., Martintoni, D., & Senni, V. (2023). A zero-trust architecture for remote access in industrial IoT infrastructures. *Electronics*, *12*(3), 566.

[18] Roosan, D., Wu, Y., Tatla, V., Li, Y., Kugler, A., Chok, J., & Roosan, M. R. (2022). Framework to enable pharmacist access to health care data using Blockchain technology and artificial intelligence. *Journal of the American Pharmacists Association*, *62*(4), 1124-1132.

[19] Ofili, B. T., Ezeadi, S. C., & Jegede, T. B. (2024). Securing US national interests with cloud innovation: data sovereignty, threat intelligence and digital warfare preparedness. *Int J Sci Res Arch*, *12*(01), 3160-3179.

[20] Parisa, S. K., & Banerjee, S. (2024). AI-Enabled Cloud Security Solutions: A Comparative Review of Traditional vs. Next-Generation Approaches. *International Journal of Statistical Computation and Simulation*, *16*(1).

[21] Dakić, V., Morić, Z., Kapulica, A., & Regvart, D. (2024). Analysis of Azure Zero Trust Architecture implementation for mid-size organizations. *Journal of cybersecurity and privacy*, *5*(1), 2.

[22] Zohaib, S. M., Sajjad, S. M., Iqbal, Z., Yousaf, M., Haseeb, M., & Muhammad, Z. (2024). Zero Trust VPN (ZT-VPN): A Systematic Literature Review and Cybersecurity Framework for Hybrid and Remote Work. *Information*, *15*(11), 734.

[23] Sontan, A. D., & Samuel, S. V. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. *World Journal of Advanced Research and Reviews*, *21*(2), 1720-1736.

[24] Fang, H., Zhu, Y., Zhang, Y., & Wang, X. (2024). Decentralized edge collaboration for seamless handover authentication in Zero-Trust IoV. *IEEE Transactions on Wireless Communications*, *23*(8), 8760-8772.

[25] Dhanaraj, R. K., Singh, A., & Nayyar, A. (2024). Matyas–Meyer Oseas based device profiling for anomaly detection via deep reinforcement learning (MMODPAD-DRL) in zero trust security network. *Computing*, *106*(6), 1933-1962.

[26] Jyothi Bobba (2024). Securing Financial Data in Cloud Environments: AI and IaaS Reliability Verification Techniques. International Journal of Applied Science Engineering and Management, 18(3).

[27] Al Shahrani, A. M., Rizwan, A., Sánchez-Chero, M., Cornejo, L. L. C., & Shabaz, M. (2024). Blockchain-enabled federated learning for prevention of power terminals threats in IoT environment using edge zero-trust model. *The Journal of Supercomputing*, *80*(6), 7849-7875.

[28] Sadaf, M., Iqbal, Z., Javed, A. R., Saba, I., Krichen, M., Majeed, S., & Raza, A. (2023). Connected and automated vehicles: Infrastructure, applications, security, critical challenges, and future aspects. *Technologies*, *11*(5), 117.

[29] Solanke, A. (2023). Edge Computing Integration with Enterprise Cloud Systems: Architectural Patterns for Distributed Intelligence. *International Journal Of Engineering And Computer Science*, *12*(03).

[30] Goswami, A., Patel, R., Mavani, C., & Mistry, H. K. (2024). Secure Cloud Collaboration in Data Centric Security. *International Journal on Recent and Innovation Trends in Computing and Communication*, *12*(2), 539-47.

[31] Val, O. O., Kolade, T. M., Gbadebo, M. O., Selesi-Aina, O., Olateju, O. O., & Olaniyi, O. O. (2024). Strengthening Cybersecurity Measures for the Defense of Critical Infrastructure in the United States. *Asian Journal of Research in Computer Science*, *17*(11), 25-45.

[32] Ofili, B. T., Obasuyi, O. T., & Akano, T. D. (2023). Edge Computing, 5G, and Cloud Security Convergence: Strengthening USA's Critical Infrastructure Resilience. *Int J Comput Appl Technol Res*, *12*(9), 17-31.

[33] Al-Hawawreh, M., Baig, Z., & Zeadally, S. (2024). AI for Critical Infrastructure Security: Concepts, Challenges, and Future Directions. *IEEE Internet of Things Magazine*, *7*(4), 136-142.

[34] Dopamu, O. M. (2024). Cloud-based ransomware attack on US financial institutions: an in-depth analysis of tactics and counter measures. *Int J Sci Res (IJSR)*, *13*(2), 1872-81.

[35] Rong, C., Geng, J., Hacker, T. J., Bryhni, H., & Jaatun, M. G. (2022). OpenIaC: open infrastructure as code-the network is my computer. *Journal of Cloud Computing*, *11*(1), 12.

[36] Alzoubi, Y. I., Mishra, A., & Topcu, A. E. (2024). Research trends in deep learning and machine learning for cloud computing security. *Artificial Intelligence Review*, *57*(5), 132.

[37] Zhang, Q. (2023). Secure preschool education using machine learning and metaverse technologies. *Applied Artificial Intelligence*, *37*(1), 2222496.

[38] Oladosu, S. A., Ige, A. B., Ike, C. C., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2022). Revolutionizing data center security: Conceptualizing a unified security framework for hybrid and multi-cloud data centers. *Open Access Research Journal of Science and Technology*, *5*(2), 086-076.

[39] Kodakandla, N. (2024). Hybrid Cloud Strategies: Optimizing Resource Allocation for Competitive Advantage in US Enterprises. *Journal of Current Science and Research Review*, *2*(01), 01-17.

[40] Zhang, S., Wang, Z., Zhou, Z., Wang, Y., Zhang, H., Zhang, G., ... & Guizani, M. (2022). Blockchain and federated deep reinforcement learning based secure cloud-edge-end collaboration in power IoT. *IEEE Wireless Communications*, *29*(2), 84-91.

[41] Akinbolaji, T. J., Nzeako, G., Akokodaripon, D., & Aderoju, A. V. (2024). Proactive monitoring and security in cloud infrastructure: Leveraging tools like Prometheus, Grafana, and HashiCorp Vault for robust DevOps practices. *World Journal of Advanced Engineering Technology and Sciences*, *13*(2), 90-104.

[42] Mylrea, M., & Robinson, N. (2023). Artificial Intelligence (AI) trust framework and maturity model: applying an entropy lens to improve security, privacy, and ethical AI. *Entropy*, *25*(10), 1429.

[43] Vegas, J., & Llamas, C. (2024). Opportunities and Challenges of Artificial Intelligence Applied to Identity and

Access Management in Industrial Environments. *Future Internet*, *16*(12), 469.

[44] Pathak, M., Mishra, K. N., & Singh, S. P. (2024). Securing data and preserving privacy in cloud IoT-based technologies an analysis of assessing threats and developing effective safeguard. *Artificial Intelligence Review*, *57*(10), 269.

[45] Kethu, S. S., Narla, S., Valivarthi, D. T., Peddi, S., Natarajan, D. R., & Kurunthachalam, A. (2024). HealthFog: A comprehensive cloud and fog-based system for early diagnosis of infectious and heart diseases leveraging IoT and deep learning. International Journal of Applied Science Engineering and Management, 18(2)

[46] Pulakhandam, W., Vallu, V. R., & Samudrala, V. K. (2024). Optimizing Healthcare Data Exchange: AI, Middleware, And Blockchain For Secure Cloud And Fog Interoperability. *Int. J. Eng. Sci. Res*, *14*(1).

[47] Devi, R. (2024). IPSHO-Fed: A hybrid federated learning and spotted hyena optimization approach for trust assessment. *Neural Computing and Applications*, *36*(10), 5571-5594.

[48] Nzeako, R. A. S. G., & Shittu, R. A. (2024). Leveraging AI for enhanced identity and access management in cloud-based systems to advance user authentication and access control. *World Journal of Advanced Research and Reviews*, *24*(3), 1661-1674.

[49] Rancea, A., Anghel, I., & Cioara, T. (2024). Edge computing in healthcare: Innovations, opportunities, and challenges. *Future internet*, *16*(9), 329.

[50] Sharma, A. K., Peelam, M. S., Chauasia, B. K., & Chamola, V. (2024). QIoTChain: quantum IoT-blockchain fusion for advanced data protection in Industry 4.0. *IET Blockchain*, *4*(3), 252-262.

[51] Rahman, M. M., Pokharel, B. P., Sayeed, S. A., Bhowmik, S. K., Kshetri, N., & Eashrak, N. (2024). riskAIchain: AI-Driven IT Infrastructure—Blockchain-Backed Approach for Enhanced Risk Management. *Risks*, *12*(12), 206.

[52] Wassan, S., Suhail, B., Mubeen, R., Raj, B., Agarwal, U., Khatri, E., ... & Dhiman, G. (2022). Gradient boosting for health IoT federated learning. *Sustainability*, *14*(24), 16842.

[53] Aljumah, A., & Ahanger, T. A. (2023). Blockchain-based information sharing security for the internet of things. *Mathematics*, *11*(9), 2157.

[54] Jin, J., Yu, K., Kua, J., Zhang, N., Pang, Z., & Han, Q. L. (2023). Cloud-fog automation: Vision, enabling technologies, and future research directions. *IEEE Transactions on Industrial Informatics*, *20*(2), 1039-1054.

[55] Devi, R. (2024). IPSHO-Fed: A hybrid federated learning and spotted hyena optimization approach for trust assessment. Neural Computing and Applications, 36(10), 5571-5594.

[56] Nzeako, R. A. S. G., & Shittu, R. A. (2024). Leveraging AI for enhanced identity and access management in cloud-based systems to advance user authentication and access control. World Journal of Advanced Research and Reviews, 24(3), 1661-1674.

[57] Rancea, A., Anghel, I., & Cioara, T. (2024). Edge computing in healthcare: Innovations, opportunities, and challenges. Future internet, 16(9), 329.

[58] Sharma, A. K., Peelam, M. S., Chauasia, B. K., & Chamola, V. (2024). QIoTChain: quantum IoT-blockchain fusion for advanced data protection in Industry 4.0. IET Blockchain, 4(3), 252-262.

[59] Wassan, S., Suhail, B., Mubeen, R., Raj, B., Agarwal, U., Khatri, E., ... & Dhiman, G. (2022). Gradient boosting for health IoT federated learning. Sustainability, 14(24), 16842.

[60] Aljumah, A., & Ahanger, T. A. (2023). Blockchain-based information sharing security for the internet of things. Mathematics, 11(9), 2157.

[61] Jin, J., Yu, K., Kua, J., Zhang, N., Pang, Z., & Han, Q. L. (2023). Cloud-fog automation: Vision, enabling technologies, and future research directions. IEEE Transactions on Industrial Informatics, 20(2), 1039-1054.