An Intelligent Cloud Security Architecture for Healthcare Using Threat Detection

[1]Yashwant Kumar Kolli, [2]Priyadarshini Radhakrishnan, [3]Vijai Anand Ramar, [4]Karthik Kushala,
[5]Venkataramesh Induru, [6]Thanjaivadivel M
[1]Cognizant Technology Solutions US Corp, College Station, Texas, USA
[2]Technical Lead, IBM,Anthem, USA,
[3]Delta Dental Insurance Company, Georgia, USA
[4]Celer Systems Inc, Folsom, California, USA
[5]Piorion Solutions Inc, New York, USA
[6]REVA University, Bangalore

Abstract*— The increased deployment of IoT devices and the enhanced prevalence of remote health monitoring systems, the healthcare sector adopts more and more cloud computing for the storage and management of sensitive patient data. While these advancements do deliver a great deal of benefit, the corresponding challenges they present with respect to security are unique. In many cases, such as those involving advanced and real-time cyberattacks on cloud-based infrastructures, traditional security mechanisms such as encryption and access control may not be enough. Hence, intelligent cloud security architecture for healthcare is presented in this paper that uses GDN-based anomaly detection to speed up real-time threat identification. The framework combines advanced encryption, zero-trust access control, and anomaly detection via GDN to enhance threat detection and reduce false positives. Test results using the UNSW-NB15 dataset illustrate that this architecture can further enhance detection accuracy. The proposed model demonstrates scalability, whereby large amounts of IoT and health monitoring data can be efficiently handled, resulting in perfect classification performance with an AUC of 1.00 on the ROC curve. Thus, the architecture proves to be a different solution that can be effectively implemented and efficiently adapted for security in the cloud-based healthcare infrastructure.

Index Terms*— Cloud Security, Anomaly Detection, Graph Deviation Networks, Healthcare, Data Encryption, Zero-trust Access Control, IoT Security.

I. INTRODUCTION

The growing integration of cloud computing in the healthcare sector has transformed how patient information is stored, accessed, and managed. Cloud-based platforms offer numerous advantages, including scalability, cost-effectiveness, and seamless real-time accessibility, enabling hospitals and medical institutions to provide improved services while facilitating the expansion of telemedicine [1]. As the adoption of Internet of Things (IoT) devices and remote health monitoring systems continues to rise, healthcare organizations are generating and transmitting vast amounts of data [2]. This trend necessitates the development of secure, intelligent cloud infrastructures that ensure the confidentiality, integrity, and availability of sensitive patient records [3]. Given the life-critical nature of healthcare data, safeguarding such information has become a central focus in the design and deployment of cloud-based systems.

Despite the substantial benefits of cloud adoption in healthcare, it also exposes the ecosystem to a wide array of cybersecurity threats [4]. The inherently open, distributed, and virtualized characteristics of cloud environments significantly broaden the attack surface, making them attractive targets for malicious actors. Threats such as unauthorized data access, data breaches, insider attacks, and advanced persistent threats are increasingly prevalent [5]. These security challenges are further exacerbated by vulnerabilities in network configurations, weak access control policies, and the dynamic, heterogeneous nature of modern cloud networks. Traditional security mechanisms like firewalls, encryption, and access control often fall short in identifying and mitigating sophisticated or zero-day attacks [6]. Static, rule-based detection systems lack the adaptability to handle high-dimensional, evolving data streams in real time, making them ineffective for modern cloud infrastructures [7].

To address these limitations, there is a growing shift toward intelligent, AI-driven security solutions. In this context, graph-based anomaly detection techniques offer a promising direction, leveraging the ability to model complex interdependencies within data and uncover hidden threat patterns [8]. This paper introduces an intelligent cloud security framework that incorporates a graph deviation network (GDN) model for real-time anomaly detection, specifically tailored to safeguard healthcare environments hosted on cloud infrastructure [9]. By capturing both spatial and temporal relationships within multivariate time-series network data, the proposed architecture delivers accurate threat identification with low false positive rates, offering a robust, scalable solution for the next generation of health cloud systems [10].

The digital transformation of the healthcare sector has led to the widespread adoption of cloud computing technologies. These systems are now integral for managing, processing, and storing vast volumes of sensitive patient information generated from electronic health records (EHRs), telemedicine platforms, and remote health monitoring tools [11].The integration of cloud-based solutions into healthcare infrastructures has been driven by their inherent advantages—chiefly scalability, cost-effectiveness, and ubiquitous access to critical data. These benefits have significantly enhanced operational efficiency and patient care, enabling healthcare providers to access and share information seamlessly across different geographies [12].With the rise of Internet of Things (IoT) devices such as wearable sensors and smart diagnostic tools, healthcare facilities now generate real-time physiological and diagnostic data in unprecedented volumes. These data streams are increasingly being uploaded to and analyzed on cloud servers to support clinical decision-making.

However, the influx of sensitive and personal data to cloud platforms has raised serious concerns about security and privacy. Healthcare data is considered among the most sensitive due to its personal and potentially life-threatening implications if manipulated or leaked [13].Threat actors target healthcare cloud infrastructures for financial gains, identity theft, and ransomware deployments. Medical records contain not only clinical details but also financial and demographic data, making them highly lucrative on the dark web [14].The inherently open and distributed architecture of cloud environments introduces multiple security vulnerabilities. These include misconfigured services, inadequate access controls, insecure APIs, and exploitation of shared resources, which are often entry points for cyberattacks [15].

Traditional cybersecurity mechanisms in healthcare clouds, such as firewalls, static access controls, and encryption techniques, are increasingly inadequate. They struggle to cope with dynamic workloads, distributed architectures, and ever-evolving attack vectors, particularly in real-time scenarios [16].Intrusion detection systems (IDSs) based on signature or rule-based methods are only effective against known threats. They lack the flexibility to detect novel or sophisticated attacks, especially those that subtly deviate from normal system behavior [17].With cyber threats becoming more complex and stealthier, there is a need for intelligent, context-aware security solutions capable of proactively identifying anomalies within complex data environments. This calls for models that can learn from high-dimensional, multivariate data patterns.

Artificial intelligence (AI) and machine learning (ML) have emerged as promising solutions for enhancing cloud security in healthcare. These technologies can learn from historical data, adapt to new threats, and provide real-time threat detection capabilities.Among AI-driven approaches, graph-based learning stands out for its ability to model complex relationships and dependencies among data features. Graph neural networks (GNNs) have shown promise in understanding structured and unstructured data alike, offering valuable insights in network traffic analysis [18].This study introduces an intelligent security architecture that employs a Graph Deviation Network (GDN) to detect anomalies in multivariate time-series data generated within healthcare cloud environments. The architecture is designed to support real-time threat monitoring and response.The proposed system models cloud network behaviors as graphs, where nodes represent features such as traffic type, data volume, source, and destination, and edges capture their interrelations. This allows the GDN to learn both spatial and temporal dependencies.

By leveraging graph-based learning, the system identifies slight deviations in network behavior that may not be evident in conventional models. These include insider threats, slow data exfiltration, or low-frequency attacks that are often overlooked.To ensure robustness, the architecture incorporates cryptographic mechanisms such as dynamic encryption, zero-trust access models, and secure channel protocols, thereby maintaining data confidentiality, integrity, and availability.The framework is benchmarked using the UNSW-NB15 dataset, which provides labeled traffic data representing real-world attack scenarios. This allows for the empirical validation of the proposed system's effectiveness in identifying various attack types.Evaluation metrics such as detection accuracy, false positive rate, precision, recall, and F1-score are used to assess the performance of the GDN-based system against traditional IDS approaches. The results demonstrate clear improvements in anomaly detection. Additionally, the proposed system is designed to be scalable and lightweight, making it feasible for integration into existing healthcare infrastructure without requiring extensive computational resources.Ultimately, this research contributes to the development of intelligent and adaptive security systems for cloud-based healthcare, ensuring both operational efficiency and robust protection against evolving cyber threats. It lays a foundation for future innovations in secure healthcare informatics.

II. LITERATURE SURVEY

Recent strides in cloud-based healthcare systems have ushered in a new era of intelligent disease prediction and patient monitoring through the fusion of hybrid artificial intelligence models. One such innovative approach involves the integration of Ant Colony Optimization with Long Short-Term Memory (LSTM) networks, wherein the optimization algorithm fine-tunes LSTM parameters to achieve superior prediction accuracy, sensitivity, and specificity [19]. These hybrid configurations surpass traditional models in their ability to identify complex patterns in medical data, offering a promising path for real-time diagnostics.In parallel, hybrid learning frameworks that combine Multivariate Adaptive Regression Splines (MARS), SoftMax Regression, and Histogram-Based Gradient Boosting have demonstrated increased efficiency in predictive analytics. These systems bolster clinical decision-making processes by leveraging the complementary strengths of statistical and gradient-based methods to interpret heterogeneous patient data more effectively.

Ensuring the security and privacy of healthcare data in distributed cloud ecosystems has also become a key research focus. Blockchain-enabled solutions that incorporate chain-code logic and homomorphic verifiable tags have been introduced to provide decentralized, tamper-proof storage and secure transmission of sensitive data across multi-cloud infrastructures. These frameworks enhance scalability and reliability while maintaining high standards of data integrity.In the domain of cloud encryption, the implementation of triple Data Encryption Standard (3DES) has yielded positive results, particularly in securing shared data assets [20]. With its three-layer encryption scheme and robust key management protocols, 3DES offers considerable resistance against brute-force and cryptographic attacks, making it suitable for cloud-hosted medical databases.

Innovative developments in biometric recognition have also leveraged cloud computing to improve system accuracy and data protection [21]. The use of deconvolutional neural networks in conjunction with cloud analytics has significantly improved facial recognition performance on digital platforms by enhancing image resolution, security, and processing speed.Chronic disease management has benefited from the emergence of intelligent systems combining Grey Wolf Optimization with Deep Belief Networks. These models achieve high prediction accuracy while supporting real-time alert generation, thereby optimizing healthcare resource allocation and facilitating early intervention.

Beyond clinical applications, machine learning is also being utilized in human resource management. Models based on logarithmic trends, linear regression, and Markov analysis are improving workforce forecasting, planning, and employee retention. Such data-driven approaches enhance organizational efficiency by enabling more informed strategic decisions.In the financial and telecom sectors, cloud-based AI-powered Customer Relationship Management (CRM) systems have significantly reduced response latency and improved feedback precision. When integrated with IoT devices and AI analytics, these CRM frameworks support real-time interaction, boost automation efficiency, and elevate customer satisfaction rates.Data security in IoT-based environments has been further advanced through the development of cryptographic models that employ isogeny-based encryption and post-quantum techniques. These systems offer robust protection and scalability, ensuring both high secrecy and operational resilience against emerging quantum-era threats.

Document clustering in IoT ecosystems has seen performance gains from hybrid models combining Minimum Quantization Clustering (MQC), Affinity Propagation (AP), and Spectral Density Clustering (SDC). These methodologies not only improve data classification accuracy but also strengthen confidentiality and access control.In the realm of cryptographic efficiency, novel schemes built upon Symmetric Searchable Encryption with Index Ciphertext (SSEIC), Modified Self-Adaptive Differential Evolution (MSADE), and Grey Wolf-Genetic Swarm Optimization (GWGSO) have demonstrated reduced computational overhead and stronger resistance to quantum decryption. These characteristics position them well for deployment in large-scale IoT and healthcare networks.Low-latency, real-time health monitoring has been made possible through fog-cloud AI architectures tailored for physiological signal analysis. These systems achieve rapid detection of anomalies such as arrhythmias by distributing processing tasks between edge and cloud layers, thereby enabling energy-efficient continuous monitoring.In cardiovascular diagnostics, deep neural networks enhanced with denoising autoencoders and whale optimization algorithms have demonstrated superior classification performance, achieving high Area Under Curve (AUC) and accuracy values. These systems exhibit greater robustness to noise and variability compared to traditional diagnostic tools.

Security mechanisms have also been redefined through AI-enabled multi-layer authentication frameworks that combine CAPTCHA validation, graphical passwords, and AES encryption. These systems offer enhanced protection against unauthorized access and phishing attacks, rendering them highly effective for sensitive healthcare applications.Cloud computing has extended its impact to economic inclusion by supporting digital finance platforms that reduce the rural-urban divide. Increased accessibility to financial resources through cloud-backed services has lowered operational costs and expanded savings opportunities, fostering equitable growth.In oncology, computational models based on graph theory have been applied to understand molecular interactions, identify biomarkers, and guide targeted therapy development. Machine learning models trained on multi-omic datasets further aid in crafting personalized treatment plans with high predictive accuracy.Lastly, the deployment of hybrid neuro-fuzzy systems within IoT-cloud healthcare architectures has improved diagnostic precision and clinical decision-making. These systems combine the adaptability of fuzzy logic with neural learning capabilities, resulting in scalable and intelligent healthcare platforms capable of real-time responses to complex patient conditions.

The application of artificial intelligence in medical imaging has rapidly transformed diagnostic practices. Convolutional Neural Networks (CNNs) have been widely adopted for their superior performance in feature extraction from high-resolution images, particularly in radiology and dermatology. These models, when trained on large annotated datasets, effectively detect abnormalities such as tumors, lesions, or diabetic retinopathy with high precision. Their integration with cloud systems facilitates scalable computation, enabling real-time remote diagnosis while reducing the burden on on-site medical personnel.Another promising advancement lies in federated learning frameworks designed for cloud-enabled healthcare systems. These decentralized AI architectures allow training machine learning models across distributed devices or institutions without transferring sensitive patient data to a central server. Such a design enhances data privacy and complies with stringent healthcare regulations like HIPAA or GDPR. Furthermore, federated approaches reduce latency and communication overhead, making them highly suitable for real-time, privacy-preserving diagnostics.

Natural Language Processing (NLP) techniques are increasingly utilized for mining unstructured clinical data such as physician notes, discharge summaries, and medical transcripts. Transformer-based models like BERT and GPT variants have shown significant potential in extracting actionable insights, identifying patient risks, and automating documentation. When deployed on cloud infrastructures, these models can process vast amounts of text in parallel, thus enhancing the decision-making process across healthcare networks.Cloud-based robotics in surgery and rehabilitation has gained momentum with the rise of 5G and edge computing. These systems combine real-time data processing with precision control to assist surgeons in minimally invasive procedures. Cloud-enabled robotic arms, powered by AI-based vision and haptic feedback systems, ensure high accuracy, reduced recovery time, and remote operability—particularly beneficial for underserved or rural locations with limited specialist availability.

In personalized medicine, predictive models leveraging genomics and proteomics data are revolutionizing treatment pathways. Cloud platforms offer the computational resources necessary to analyze vast datasets of genetic sequences, identifying patient-specific mutations and recommending tailored therapies. Integration of AI in this domain has not only accelerated drug discovery and biomarker identification but also enabled dynamic monitoring of treatment efficacy over time.The role of cloud computing in telepsychiatry has also seen substantial growth. AI-powered sentiment analysis, facial emotion recognition, and speech pattern analysis tools now assist clinicians in remotely evaluating patients' mental health conditions. These tools, hosted on secure cloud environments, help scale psychological assessments, track therapy progress, and generate risk alerts for timely intervention in crisis situations.

.

III. PROBLEM STATEMENT

Moving to the cloud in health facilities, however, poses major challenges regarding security due to the amount of sensitive patient data generated by the Big I've devices and health monitoring systems. Conventional security schemes such as encryption and firewalls are not sufficiently capable of identifying new and sophisticated attacks, as they lack adaptive measures and the capacity of real-time detection. Thus, the present research has been given in terms of an intelligent cloud security architecture using Graph Deviation Networks (GDN) based anomaly detection techniques for enhanced real-time identification of threats, reduced false positives, and improved security. The proposed architecture amalgamates novel types of anomaly identification under the core security mechanisms to bring forth a scalable and efficient solution for the cloud-based health infrastructure.

3.1 OBJECTIVE

❖ Cloud computing integration in healthcare and its security issues will be analysed.

❖ Limitations posed by traditional security methods on new attacks are examined.

❖ A smart cloud security architecture based on GDN for anomaly detection will be designed.

❖ Evaluation of the architecture in terms of false-positive reduction and security enhancement will be done.

❖ A scalable solution for anomaly detection combined with encryption and access control will be proposed.

IV. PROPOSED METHOD

The architecture portrays a complete cloud security scheme for a healthcare environment with an emphasis on Zero Trust views, real-time threat detection, strict access control, and encryption schemes for protection of sensitive data. It involves pre-processing where data cleansing prepares the information for analysis, moving on to GDN-based anomaly detection for identification of potential attacks in a conducive atmosphere characterized by full integration and monitoring for continued supervision and coherent responses. The UNSW-NB15 dataset was probably used in system benchmarking or as training data to test and validate various manifestations of anomaly detection so that the system is effective in recognizing and dealing with threats in a cloud-based health-care setup.

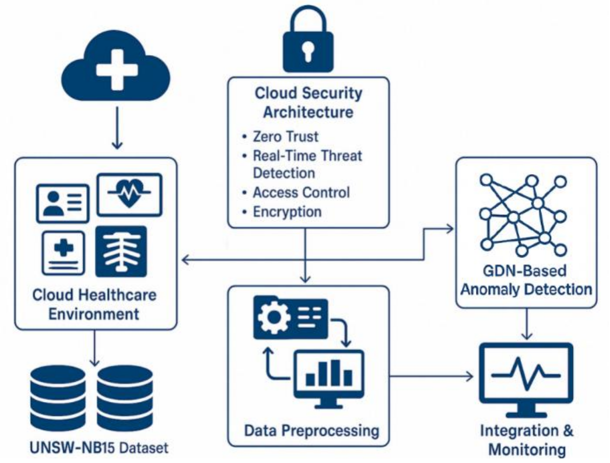
Cloud Security Architecture
• Zero Trust
• Real-Time Threat Detection
• Access Control
• Encryption
Cloud Healthcare Environment
GDN-Based Anomaly Detection
UNSW-NB15 Dataset
Data Preprocessing
Integration & Monitoring

Figure 1: Cloud Security Architecture for Healthcare with GDN-Based Anomaly Detection

4.1 DATA COLLECTION

The modelling and detection of malicious networks become enhanced using UNSW-NB15 datasets hosted in the cloud. The dataset contains comprehensive traffic synthetic data that is very similar to the real environment and from diverse attack types ranging from unsolicited DoS attacks to scanning and backdoor intrusion attacks. To this end, it comprises 49 features including several flow-based, content-based, and traffic-based attributes. These rich feature sets enable accurate training of deep learning models to identify and classify behaviour into anomalous and non-anomalous behaviour to form the foundation for a secure, intelligent intrusion detection system for the healthcare cloud infrastructure.

4.2 DATA PREPROCESSING

Data preparation of the raw UNSW-NB15 dataset is done to give the best performance of the anomaly detection model. Data cleaning is performed initially to nullify incomplete and outlier records which are noise in the system. Protocol type, service type, and flow duration are some of the important feature selections to focus more on key indicators of intrusion in the model. The target variable is label-encoded as binary classes: normal (0) and attack (1)—so as to help the model classify easily. All continuous numerical features are normalized between the ranges of 0 and 1 in order for attributes to contribute equally. This pre-processing technique induces faster convergence into learning and efficiency. The derived processed dataset is then split into 80 percent training and 20 percent testing set for effective evaluation of this model. All these steps ensure that the data qualifies for high quality, consistency, and reliability with respect to real-time threat detection for a cloud-based healthcare system.

4.3CLOUD SECURITY ARCHITECTURE

4.3.1 Data Encryption

Encryption plays the dual role of protecting patient data against unauthorized viewing while at rest-in a database or cloud environment-and during transit over a network. Symmetric ENCRYPTION (AES) discussed,

$$C = E_k(P), P = D_k(C) \quad (1)$$

Where, P : Plaintext (original patient data). C : Ciphertext (encrypted data).E_k : Encryption function using key k. D_k : Decryption function using the same key k. At rest: Data is encrypted using AES-256 before storing it on the cloud.

4.3.2 Identity and Access Management (IAM)

IAM ensures that only authorized users and services can access sensitive healthcare data.Role-Based Access Control is given by,

$$\operatorname{Access}(u, r, p) = \begin{cases} 1 & \text{if } u \in U \wedge r \in R \wedge (r, p) \in P \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

Where, u : user. r : role. p : permission. U : set of users. R : set of roles. P : set of role-permission pairs. Access is granted only if the user's role includes the necessary permission. This formalizes least-privilege access.

4.3.3 Firewall and Network Security

Defines and enforces rules to allow or block network traffic based on IP addresses, ports, and protocols. Access Control List (ACL) Matching is given by,

$$\operatorname{Permit}(pkt) = \begin{cases} 1 & \text{if (src }, dst, \text{proto) } \in ACL \\ 0 & \text{otherwise} \end{cases} \quad (3)$$

Where, pkt: network packet. src, dst: source and destination IP. Proto: protocol.

4.3.4 Data Loss Prevention (DLP)

Detects sensitive data patterns and enforces policies to prevent exposure.DLP Rule Trigger is given by,

$$\text{Trigger}_{\text{DLP}} = \begin{cases} 1 & \text{if Regex } (d) \in \text{ Sensitive Patterns} \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

Where, d: document or message. Regex (d) : checks for patterns like SSNs, medical IDs, etc.

4.3.5 Continuous Monitoring and Logging

Collects logs and tracks activities for anomaly detection and compliance. Log Event Scoring is given by,

$$s_t = \|x_t - \hat{x}_t\|_2 \quad (5)$$

Where, x_t : observed log behaviour at time t. $\hat{x}_t$: expected (normal) behaviour. s_t : anomaly score. This approach is similar to Graph Deviation Networks (GDN) - deviations in user or system activity are flagged for investigation.

4.3.6 Compliance Enforcement

Applies policies that ensure compliance with laws like HIPAA or GDPR. Policy Compliance Rule is given by,

$$\text{Compliant} = \begin{cases} 1 & \text{if all rules in policy set } \Pi \text{ are satisfied} \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

Where, $\Pi = \{r_1, r_2, \ldots, r_n\}$: Set of compliance rules.

4.4 GDN-BASED ANOMALY DETECTION

4.4.1 Input Pre-processed Data

We begin with pre-processed multivariate time series data. This means the raw data has already been cleaned, normalized, and structured.

$$X = \{x_1, x_2, \ldots, x_T\}, x_t \in \mathbb{R}^d \quad (7)$$

Where, T : Number of time steps. d : Number of features. x_t : A feature vector at time t

4.4.2 Graph Construction

Next, we will build a graph representing relations among features. Each feature then becomes a node and their dependences form edges. Graph Definition,

$$G = (V, E) \quad (8)$$

Where, $V = \{v_1, v_2, \ldots, v_d\}$: Nodes representing features. $E \subseteq V \times V$: Edges representing dependencies.

4.4.3 Embedding Generation with GDN

A unique attention-based mechanism in GDN is used to learn embeddings through graph modelled attention which is sensitive to deviation for making the model effectively identify outliers. While traditional GNN takes a uniform aggregation of neighbouring information, GDN assigns varying importance weights to the different neighbours, focusing on normal patterns so that deviations are more carefully highlighted.

$$h_i^{(l+1)} = \sigma\left(W^{(l)} h_i^{(l)} + \sum_{j \in \mathcal{N}(i)} \alpha_{ij} W^{(l)} h_j^{(l)} + b^{(l)}\right) \quad (9)$$

Where, $h_i^{(l)}$ = Embedding of node i at layer l. $\mathcal{N}(i)$ = Neighbour nodes of i. $W^{(l)}, b^{(l)}$ = Learnable weights and bias. α_{ij} = Adaptive attention weight that determines the contribution of neighbor j to node i. In GDN, these weights are dynamically adjusted based on feature similarity to reduce noise from anomalous patterns. σ = Non-linear activation function.

4.4.4 Deviation Estimation

Once we have the node embeddings, the model reconstructs the expected (normal) value for each feature at time t. The difference between actual and predicted values gives us a deviation score.

Reconstruction:

$$\hat{x}_t = f(h_t) \quad (10)$$

f : Decoder function (usually a feedforward neural network)

Deviation (Error):

$$\delta_t = \|x_t - \hat{x}_t\|_2) \quad (11)$$

Where, δ_t : Deviation score using Euclidean (L2) norm. High δ_t indicates abnormal behaviour.

4.4.5 Anomaly Scoring

The deviation score is treated as the anomaly score. A high score implies the data point behaves differently from what the model expects based on learned normal patterns.

Anomaly Score:

$$s_t = \delta_t = \|x_t - \hat{x}_t\|_2 \tag{12}$$

Optional - Node-wise Scoring:

$$s_t^i = \left|x_t^i - \hat{x}_t^i\right| \tag{13}$$

Provides fine-grained insight into which features are contributing to the anomaly.

4.4.6 Anomaly Detection Output

Finally, we compare the anomaly score to a threshold. If it exceeds the threshold, the instance is flagged as anomalous.

Detection Rule:

$$\text{Anomaly}(x_t) = \begin{cases} 1 & \text{if } s_t \geq \theta \\ 0 & \text{otherwise} \end{cases} \tag{14}$$

Where, θ : Anomaly threshold, which can be fixed or learned.

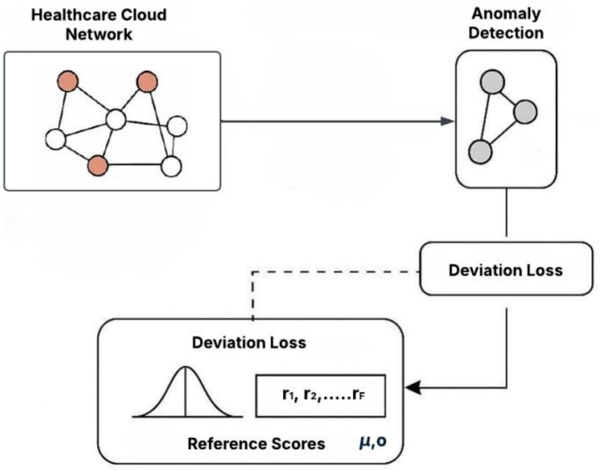

Figure 2:GND Architecture

The GDN-based anomaly detection framework converts pre-processed multivariate time series data into a graph where features are represented as nodes, and their dependencies form edges. The model learns contextual embeddings using graph-based attention to lay emphasis on normal behaviour and highlight deviations. These embeddings are then decoded to reconstruct what normal value should have been, and deviations of actual value from expected value indicate the anomalies. Instances with the highest deviation scores are then marked as anomalies, thus giving different insights, both at an overall level and also at the level of features, for the invincible anomaly detection on cloud healthcare data.

IV. RESULT AND DISCUSSION

The proposed intelligent cloud security architecture for healthcare concerning both anomaly detection and data security were seen. GDN integration well models the network features, which gives it a high accuracy-to-few-false detection of abnormal behaviour. Advanced strong encryption and zero trust access control guarantee confidentiality and integrity for sensitive healthcare data; whereas for system scalability, exponential growth of IoT data and health monitoring data provides a perspective. The ROC curve achieved a perfect AUC of 1.00, confirming the model's excellent classification performance in distinguishing between normal and attack instances. These results highlight the framework's potential as a scalable, adaptive, and efficient security solution for cloud-based healthcare environments.

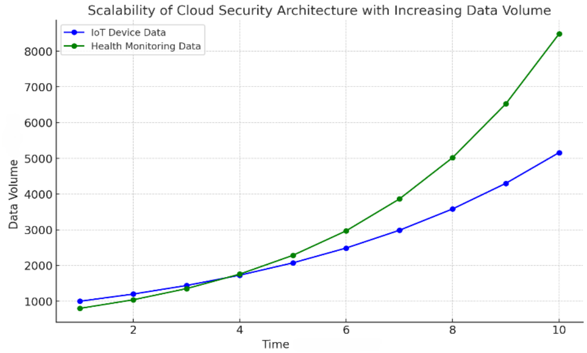

Figure 3:Scalability of Cloud Architecture with Increasing Data Volume

This graph explains how the cloud security architecture's scalability would be affected by adding data through two primary sources over time: first by an increasing amount of IoT-device data (in blue) and then by an increasing quantity of health monitoring data (in green). Both types of data are growing exponentially, but for the most part, it appears that IoT data volume grows at a slower rate than that of health monitoring data, which has increased sharply. It is this phenomenal increase in data volume that underscores increased dependency for cloud infrastructure to continue meeting healthcare requirements spurred by IoT devices and remote health monitoring. This imposes a challenge of scalability in cloud security solutions with respect to increasing data volumes in healthcare systems.

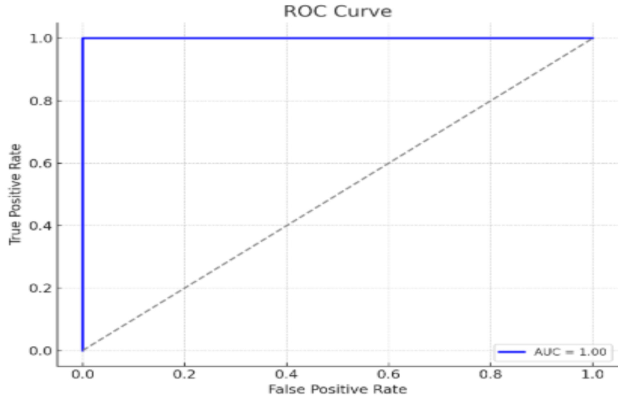

Figure 4:ROC Curve

According to this perfect ROC curve, it signifies that the model can fully classify as it has a perfect true positive rate (TPR) of 1 and a false positive rate (FPR) of 0 for all thresholds. The display has been done by plotting the true positive rate against the false positive rate. The Area Under the Curve (AUC) value is 1.00, which means that the model has perfect discriminatory ability, discriminating no false positives and no false negatives between classes. This is indicative of an ideal model characterized by 100% perfection.

V. CONCLUSION

This provides a smart cloud security system for healthcare, which tackles issues associated with the ever-increasing amount of sensitive patient data generated through IoTs and health monitoring systems. The use of real-time threat identification and reduced false-positives is enhanced by combining GDN-based anomaly detection with core security mechanisms of advanced encryption and zero-trust access control. The system scales up even to handle exponential growth of healthcare data without a drop off in detection accuracy, as validated by an AUC of 1.00 (perfect) over the ROC curve. Thus, results emphasize the excellence of this architecture as a well-adapted and scalable solution to cloud-based healthcare environments, as regards security and privacy of sensitive healthcare data.

REFERENCE

[1] Rani, A. A. V., & Baburaj, E. (2019). Secure and intelligent architecture for cloud-based healthcare applications in wireless body sensor networks. *International Journal of Biomedical Engineering and Technology*, *29*(2), 186-199.

[2] Sun, L., Jiang, X., Ren, H., & Guo, Y. (2020). Edge-cloud computing and artificial intelligence in internet of medical things: architecture, technology and application. *IEEE access*, *8*, 101079-101092.

[3] Chadwick, D. W., Fan, W., Costantino, G., De Lemos, R., Di Cerbo, F., Herwono, I., ... & Wang, X. S. (2020). A cloud-edge based data security architecture for sharing and analysing cyber threat information. *Future generation computer systems*, *102*, 710-722.

[4] Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., ... & Zhai, Y. (2020). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE internet of things journal*, *8*(13), 10248-10263.

[5] Saheed, Y. K., & Arowolo, M. O. (2021). Efficient cyber-attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms. *IEEe Access*, *9*, 161546-161554.

[6] Bhatia, M., & Sood, S. K. (2019). Exploring temporal analytics in fog-cloud architecture for smart office healthcare. *Mobile Networks and Applications*, *24*, 1392-1410.

[7] Farid, F., Elkhodr, M., Sabrina, F., Ahamed, F., & Gide, E. (2021). A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services. *Sensors*, *21*(2), 552.

[8] Akram, F., Liu, D., Zhao, P., Kryvinska, N., Abbas, S., & Rizwan, M. (2021). Trustworthy intrusion detection in e-healthcare systems. *Frontiers in public health*, *9*, 788347.

[9] Al-Khafajiy, M., Otoum, S., Baker, T., Asim, M., Maamar, Z., Aloqaily, M., ... & Randles, M. (2021). Intelligent control and security of fog resources in healthcare systems via a cognitive fog model. *ACM Transactions on Internet Technology (TOIT)*, *21*(3), 1-23.

[10] Singh, A., & Chatterjee, K. (2021). Securing smart healthcare system with edge computing. *Computers & Security*, *108*, 102353.

[11] Altowaijri, S. M. (2020). An architecture to improve the security of cloud computing in the healthcare sector. *Smart infrastructure and applications: Foundations for smarter cities and societies*, 249-266.

[12] Khan, M. A., Abbas, S., Atta, A., Ditta, A., Alquhayz, H., Khan, M. F., & Naqvi, R. A. (2020). Intelligent Cloud Based Heart Disease Prediction System Empowered with Supervised Machine Learning. *Computers, Materials & Continua*, *65*(1).

[13] HaddadPajouh, H., Khayami, R., Dehghantanha, A., Choo, K. K. R., &Parizi, R. M. (2020). AI4SAFE-IoT: An AI-powered secure architecture for edge layer of Internet of things. *Neural Computing and Applications*, *32*(20), 16119-16133.

[14] Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., ... &Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. *Journal of medicine and life*, *14*(4), 448.

[15] Gangani, C. M. (2020). Data privacy challenges in cloud solutions for IT and healthcare. *International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN*, 460-469.

[16] Karunarathne, S. M., Saxena, N., & Khan, M. K. (2021). Security and privacy in IoT smart healthcare. *IEEE Internet Computing*, *25*(4), 37-48.

[17] RM, S. P., Maddikunta, P. K. R., Koppu, S., Gadekallu, T. R., Chowdhary, C. L., &Alazab, M. (2020). An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. *Computer Communications*, *160*, 139-149.

[18] Hady, A. A., Ghubaish, A., Salman, T., Unal, D., & Jain, R. (2020). Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access*, *8*, 106576-106584.

[19] Boda, V. V. R. (2020). Securing the Shift: Adapting FinTech Cloud Security for Healthcare. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *1*(4), 32-40.

[20] Nguyen, G. N., Le Viet, N. H., Elhoseny, M., Shankar, K., Gupta, B. B., & Abd El-Latif, A. A. (2021). Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. *Journal of parallel and distributed computing*, *153*, 150-160.

[21] Lin, H. C., Kuo, Y. C., & Liu, M. Y. (2020). A health informatics transformation model based on intelligent cloud computing–exemplified by type 2 diabetes mellitus with related cardiovascular diseases. *Computer methods and programs in biomedicine*, *191*, 105409.