International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 03 Mar. 2025, pp: 600-606 www.ijaem.net ISSN: 2395-5252

Secure Cloud Storage and Authentication for Health Insurance Data

Bhavya Kadiyala[1], Chaitanya Vasamsetty[2], Rajani Priya Nippatla[3], Subramanyam Boyapati[4], Sunil Kumar Alavilli[5], Purandhar. N[6, *]

[1]*Parkland Health, Texas, USA*
[2]*Elevance Health, Georiga, USA*
[3]*Kellton Technologies Inc, Texas, USA*
[4]*American Express, Arizona, USA*
[5]*Sephora, California, USA*
[6]*Department of CSE (Artificial Intelligence) School of Computers Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh, India*

Date of Submission: 10-03-2025 Date of Acceptance: 20-03-2025

ABSTRACT:
Data privacy and security have emerged as crucial issues in the healthcare insurance environment, owing to increasing reliance on digital data. Protecting sensitive customer data would be a fundamental requirement for compliance and risk management against threats of unauthorized access. The study is to develop a secure cloud-based solution to encrypt health insurance policyholder data, implement authentication mechanisms, and safely store the data in cloud storage for future analysis.Initially,data collection whereby all data integral to insurance may be collected. The system gives strict access control via Zero Trust Authentication such that only authorized people can get access to the data. Next, high-level encryption of data using Elliptic Curve Cryptography takes place, after which the data is safely stored with the intent of scalable and efficient management in Cloud Storage. The outcomes proved that the cryptographic overhead is 30 units while achieving a very low cryptographic failure (5%). Moreover, the cloud computing latency has been optimized, wherein the response time enhances from 375 ms to 100 ms by the 10th time step, The contribution of this study lies in advancing an integrated approach for healthcare insurance data management that is complete, secure, and based on modern encryption and authentication techniques and provides an understanding of how cloud storage solutions could effectively manage sensitive data with high security.

Keywords: Healthcare Insurance, Data Security, Elliptic Curve Cryptography (ECC), Zero Trust Authentication, Cloud Storage.

I. INTRODUCTION

Cloud computing has totally transformed the way organizations use spaces for containing data, for managing data, and processing data[1]. The increased scalability and affordability accrue from the use of cloud computing technology for sensitive data such as health insurance information[2]. Store the sensitive data in a cloud-based environment to provide secure, centralized access and compliance with data protection legislation[3]. Integrate encryption techniques, such as ECC, and develop a strong security model such as Zero Trust to ensure confidentiality, integrity, and availability for data in cloud systems[4]. Cloud flexibilities also include real-time access to information and having disaster recovery solutions while reducing infrastructure costs[5]. Therefore, cloud computing is a critical element in the operations of any organization, for it helps any business in handling large amounts of sensitive data in this current digital era[6].

Healthcare has become increasingly dependent on the use of advanced technology - for the improvement of quality of patient care, the enhancement of operational efficiency in the workplace, and the effective security of data[7]. With the emergence of EHRs (Electronic Health Records), wearable devices, and telemedicine, health collects enormous amounts of data, which need proper secure and efficient management[8].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 03 Mar. 2025, pp: 600-606 www.ijaem.net ISSN: 2395-5252

With the use of artificial intelligence, machine learning, and cloud technology, healthcare could provide real-time data for analysis, treatment personalized, and more effective decision-making[9]. This, however, becomes a major challenge in terms of the privacy and security of sensitive medical information[10]. Progress in encryption, authentication mechanisms, and secure cloud storage can effectively protect patients' data and derive terms in compliance with such healthcare regulations as HIPAA and GDPR as to how health data is secured within a country's limits[11].

Numerous services are provided by the finance industry in the world economy such as banking, investment, insurance, and asset management[12]. The digital transformation of the sector would result in increased adoption of new technologies such as artificial intelligence, cloud computing, and blockchain to create operational efficiencies, enhance customer experiences, and ignite innovation across financial institutions[13]. Another critical consideration is that due to the increased use of data-driven decision-making, stringent security measures have to be in place to ensure the protection of sensitive financial information[14]. Regulatory compliance and data privacy remain a big issue, while frameworks directly like GDPR and PCI-DSS guide financials in practicing complete transparency while also being safeguarded against any imaginable threats from cybercriminals[15]. Thus, with the dynamics in technology, financial institutions are set to improve and broaden their very own operational strategies, and in so doing, they create room for the opportunity and the scope to increase challenges[16].

The layout of the paper appears as follows. section 2, Literature review on healthcare data security, authentication techniques, and encryption methods. section 3, proposed methodology in detail in, including details of the data collection process, zero-trust authentication, ECC-based encryption, and cloud storage integration. section 4, discuss the results Finally, the paper concludes in Section 5.

II. LITERATURE SURVEY

This study examines the effects of cloud computing on the management accounting processes of SMEs. Different methodologies such as Content Analysis, Partial Least Squares Structural Equation Modeling (PLS-SEM) and Classification and Regression Trees (CART) were put together in assessing the role of cloud computing in enhancing financial data management, operational efficiency, and decision making[17]. The findings indicate that cloud-based accounting solutions are usable for real-time data access for compliance and strategic decision making.

Going now to JSP, a new hybrid approach is proposed that combines HGA and HPSO. The HGA modifies the basic Genetic Algorithm using immune mechanism concepts to overcome premature convergence, and HPSO integrates the PSO with genetic operators in issues concerning the ordering of jobs and production times[18]. This hybridization optimizes costs and scheduling efficiency, outperforming protocols.

The present project deals with the time series data forecast in the manufacturing system and all the problems of the non-linearity and non-stationarity associated with it. In particular, present work hybridizes the temporal ARIMA linear model for time series with a non-linear Bi-directional GRU (Bi-GRU) model interested in error correction [19]. The hybridization of the two models tested on six real-world time series showed improved performance in all three-error metrics: MSE, MAE, and MAPE. This shows that the method proposed here is more accurate to improve forecasting accuracy compared to the existing methods.

Mayo and Cleveland Clinics case study demonstrates that possible threats and vulnerabilities can be identified to ensure data confidentiality through the use of encryption and intrusion detection[20]. In this light, data security and compliance with regulatory requirements have been proved along with improved patient care.

The present research proposes a new hybrid approach for enhancing workload forecasting in intelligent cloud computing systems using Backpropagation neural network algorithm and game theory[21]. Through this introduction, optimization of resource allocation and service delivery are accomplished through a mutual Service Level Agreement (SLAs) to cloud users and service providers at Nash equilibrium. Real data experimentation has proved its efficacy in strengthening cloud operation. Now, the methodology is scalable, secure, and easy to use; thus, applicable in many domains for enhanced cloud resource management.

The second phase of our study investigates advanced artificial intelligence-based fraud investigations in the IoT sector. The major distinction between legitimate and fraudulent activity is primarily performed through supervised

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 03 Mar. 2025, pp: 600-606 www.ijaem.net ISSN: 2395-5252

and unsupervised learning methods applied to historical transaction data through AI systems[22]. The study aims to assess the main techniques, datasets, and evaluation metrics for adaptive learning so that retraining of models is done frequently for improved automation responses.

The research proposes an intelligent education management platform utilizing cloud computing and AI capable of enhancing educational service delivery through intelligent automation and personalized learning. Built on service-oriented architecture (SOA) and deployed within a Hadoop-managed server cluster such that high processing efficiency and scalable data management assured[23]. Great data access and high concurrency create enabling environments for effective resource management and remote learning. Nonetheless, the entire approach does not provide a very rich understanding regarding certain aspects.

CFMSiC, Cognition in the Financial Management Systems in the Cloud, defines a new subclass of intelligent financial management systems using cognitive techniques for financial data management and reference to semantic analysis. These systems expand traditional financial services by overlaying an adjustable advanced information-sharing protocol aimed at solving a key trust issue concerning confidential data protection among trusted groups of clients[24]. CFMSiC deals, therefore, with an intuitive secure and strategic financial data management mechanism, backed by a mechanism for innovative sharing and encryption over cloud-based systems.

2.1. Problem Statement

The study describes some major improvements, such as an 84.7% reduction in personnel across subsidiaries, with the average number of employees per subsidiary dropping from 23 to 3.5 over a period of nine years and an almost three times increase in financial assets from 23 billion yuan to 68.55 billion yuan[25]. Cloud computing technology plays a crucial role in reducing investment costs, achieving high reliability standards, and supporting modular expansion.The research thereby goes ahead to seek opportunities in intelligent forecasting and evaluation technologies to effect the growth for digital transformation within the financial sector of data management[26].

III. METHODOLOGY

The system is intended to be an integrated strength in health care insurance data security as shown in figure 1. From the Data Collection, data will be assembled to generate that relevant insurance data down into Authentication via Zero Trust, thus ensuring strict access to that data. Afterward data will be encrypted using ECC and stored within Cloud Storage, thus ensuring high security and higher efficiency in its management.

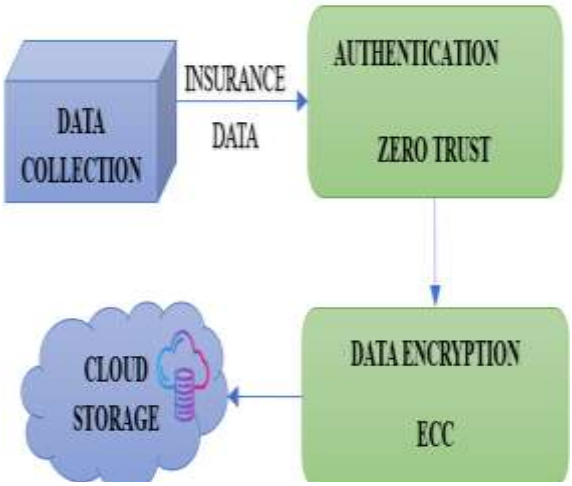

Figure 1: Secure Healthcare Insurance Data Management and Storage

3.1. Data Collection

Healthcare data collection usually involves the gathering of relevant data from insured lives. Primarily, it collects some sensitive attributes which include the following - customer demographics, health conditions, policy-related attributes, and also historical claims data. These data are very relevant in the analysis of the general behaviour of insured customers as regards their future probabilities of interest in other insurance products. It is also analysed to ensure completeness and accuracy before further processing. Data collection is the preliminary step for secure handling, encryption, and the final storage of the data in cloud-based systems.

3.2. Authentication using Zero Trust

Every user and device requesting admission to sensitive health insurance data are authenticated on a continuous basis regardless of user location or the network being used. Access to such data requires that Zero Trust computing asserts that trust is never assumed but rather requested access authenticated through various access factors, such as identity, device health, and contextual data. The authentication is accomplished through both the identity verification and Multi-Factor Authentication (MFA) and by assessing the security posture of the device. The access decision

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 03 Mar. 2025, pp: 600-606 www.ijaem.net ISSN: 2395-5252

is made dynamically with respect of the risk level shown in Equation (1) and (2).

$$P(\text{ Access }) = f(\text{ User Authentication , Device Security , Contextual Data }) \quad (1)$$

Were, User Authentication-the level of trust based on the user's authentication factors, Device Security-the measure of the device's security posture including antivirus status, operating system patches and security configurations, Contextual Data-geographical location of the user or device requesting access.

$$\text{Trust Level} = \frac{\text{User Credential Score} + \text{Device Health Score} + \text{Risk Factor}}{3} \quad (2)$$

Were, User Credential Score is the Strength with which authentication mechanism is used, Device Health Score the overall security status of the device, Risk score based on whether the access attempt comes from a trusted or risky location.

3.3. Data Encryption using Elliptic Curve Cryptography

Elliptic Curve Cryptography or in short ECC is the modern and complete method of cryptography that is used for encrypting sensitive data, especially in the case of healthcare insurance, where the security of data is of utmost importance. In ECC, elliptic curves play a significant role in generating public keys and private key pairs by using properties of mathematics over finite fields involving elliptical curves, which act as the fundamental URL to the secure transmission and storage of data. The ECC must be considered for encryption of health insurance data since it assures higher encryption standards with smaller key sizes comparatively lesser computational overhead for encryption as compared to its counterparts like RSA-type of encryptions which require large key sizes for the same strength of encryption. In this encryption system, the data is transformed into points on the elliptic curve, which can only be decrypted by authorized entities holding the valid private key. ECC is able to provide high-security levels with smaller key sizes which are important for environments that are resource limited such as mobile devices or embedded systems in healthcare applications. Confidential information in the data is not only stored but also transmitted over the public networks, thus under unauthorized access to sensitive customer information and breach of security as given in equation (3) and (4).

$$E(P) = k \cdot P \quad (3)$$

Were,E(P)is the point which is encrypted in the elliptic curve, k is the scalar (private key), P is the base point on the elliptic curve.

$$D(E(P)) = k^{-1} \cdot E(P) \quad (4)$$

Were, D(E(P))is the decrypted data, $k^{-1}$is the inverse of the private key (for decryption), E(P)is the encrypted data.

3.4. Cloud Storage

Storing vital information in the cloud has become increasingly important in the management of private data. This practice is chiefly evident in the health insurance industry, where the secure storage of patient and customer information is most important. Cloud storage is a highly reliable, scalable, and cost-effective option for storing and accessing massive sensitive healthcare insurance data. It helps the authorized users easily retrieve data and protects data against unauthorized access and breaches, which is vital when handling personally identifiable information (PII) and other confidential health-related data.

Cloud storage offers access to encrypted data without compromising security. It provides access to authorized individuals to encrypted data stored in the cloud. Access is secured through user authentication such as multi-factor authentication (MFA) and role-based access control (RBAC). In addition, it makes possible the integration of different cloud storage solutions into other systems to facilitate smooth continuous workflow for real-time access, backup, and synchronization of data.

Cloud providers do this by offering built-in encryption during rest and for moving data into and out of the cloud. Such provisions ensure that data is protected while in a cloud storage environment and during any internal or external movement across networks. This end-to-end encryption protects classified data from unauthorized use while also representing a way to comply with many of the world's laws regarding the protection of data-including GDPR and HIPAA. Such protocols of encryption are fundamentally linked to the security of most data, ensuring confidentiality and integrity in records, preventing leakage of data or its unauthorized modification.

IV. RESULT

This outcome analyses the performance of secure data processing in financial terms in terms of time taken to encrypt data, scalability and the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 03 Mar. 2025, pp: 600-606 www.ijaem.net ISSN: 2395-5252

latency observed with the work already completed. These findings lend credence to the assertions of the proposed methodology regarding security in the management of such financial data.

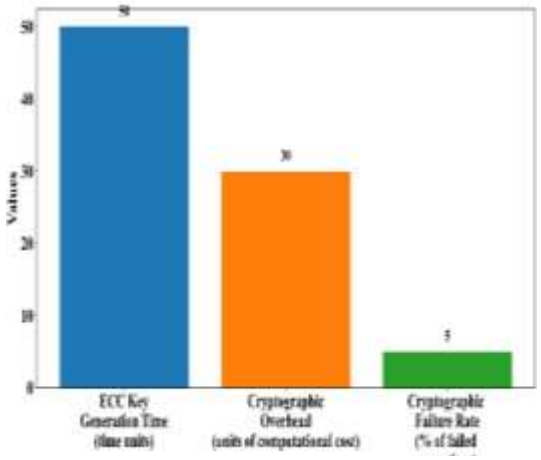

Figure 2: Encryption Time

Figure 2 states what it is, namely the performance ratings of elliptic curve cryptography for three major aspects - Of these, ECC Key Generation Time tends to be the most resource-consuming process at 50-time units. The Cryptographic Overhead, which describes the computational cost that incurs while performing ECC operations, stands at 30 units. In all, the last measure, Cryptographic Failures Rate, denotes the ratio of failed cryptographic operations to all cryptographic operations, being low at 5%. It indicates the trade-offs involved in ECC high key generation timings and computation cost maintaining against low failure rates.

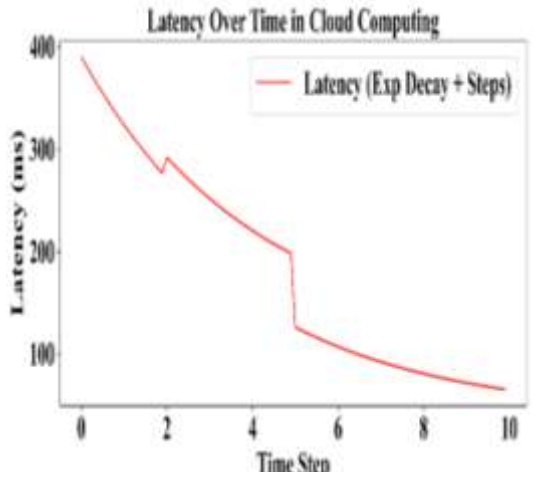

Figure 3: Latency Reduction Over Time in Cloud

Figure 3 indicates the reduction of latency based on time steps. Initially, at time step 0, latency was about 375 ms, and this began decreasing gradually throughout the early time steps. The graph follows an exponential decay trend, wherein there is a very significant reduction in latency during the first few time steps before gradually trending towards lesser reductions. By time step 10, latency becomes stable at around 100 ms, showing that performance and response time of the system continued improving over time. This latency trending is represented by the red line labelled Latency.

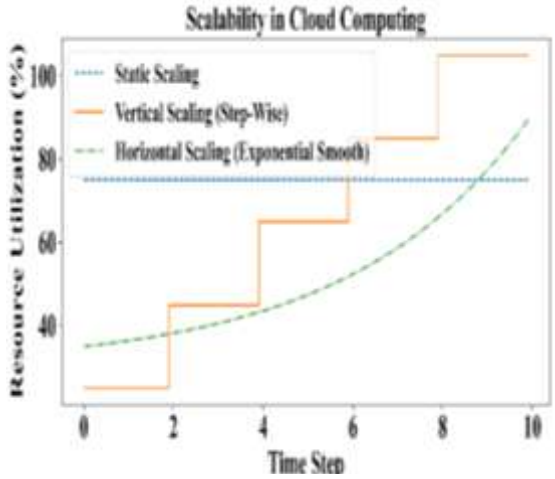

Figure 4: Resource Utilization and Scalability in Cloud

Figure 4 depicts the time variation in resource utilization behaviour adopted by different scaling methods. Static Scaling indicates constant 100% resource utilization which means resources are not adjusted over time. Vertical Scaling steps up resource utilization abruptly in increments, reaching 100% around time step 10. Horizontal Scaling smoothly and slowly increases resource utilization in an exponential fashion to (technically) reach 100%. The graph explains the various ways through which cloud systems can scale its resources according to increasing demands.

V. CONCLUSION

Secure healthcare insurance data managing methodology offers authenticating, encrypting, and cloud storage techniques. Results indicate that in ECC, the key generation time is 50-time units, the cryptographic overhead is 30 units, and the cryptographic failure rate is very low at 5%. Latency reduction in cloud computing is observed, in which response times decrease from 375 ms to 100 ms by time step 10. Resource utilization shows a gradual increase with horizontal scaling, while vertical scaling shows sudden increases. Future enhancements could focus on

optimizing ECC key generation time and increasing the study on dynamic scaling methods that will allow the handling of larger volumes of data more efficiently.

REFERENCES

[1]. A. R. G. Yallamelli, "Cloud Computing And Management Accounting In Smes: Insights From Content Analysis, Pls- Sem, And Classification And Regression Trees," Int. J. Eng., vol. 11, no. 3.

[2]. 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.

[3]. R. K. M. K. Yalla, A. R. G. Yallamelli, and V. Mamidala, "A Distributed Computing Approach to IoT Data Processing: Edge, Fog, and Cloud Analytics Framework," Int. J. Inf. Technol. Comput. Eng., vol. 10, no. 1, pp. 79–94, Jan. 2022.

[4]. A. R. G. Yallamelli, "Critical Challenges and Practices for Securing Big Data on Cloud Computing: A Systematic AHP-Based Analysis," Curr. Sci., 2021.

[5]. M. V. Devarajan, M. Al-Farouni, R. Srikanteswara, R. Rana Veer Samara Sihman Bharattej, and P. M. Kumar, "Decision Support Method and Risk Analysis Based on Merged-Cyber Security Risk Management," in 2024 Second International Conference on Data Science and Information System (ICDSIS), May 2024, pp. 1–4. doi: 10.1109/ICDSIS61070.2024.10594070.

[6]. T. Ganesan, R. R. Al-Fatlawy, S. Srinath, S. Aluvala, and R. L. Kumar, "Dynamic Resource Allocation-Enabled Distributed Learning as a Service for Vehicular Networks," in 2024 Second International Conference on Data Science and Information System (ICDSIS), May 2024, pp. 1–4. doi: 10.1109/ICDSIS61070.2024.10594602.

[7]. A. R. G. Yallamelli and M. V. Devarajan, "Hybrid Edge-Ai And Cloudlet-Driven Iot Framework For Real-Time Healthcare," vol. 7, no. 1, 2023.

[8]. A. R. G. Yallamelli, "Improving Cloud Computing Data Security with the RSA Algorithm," vol. 9, no. 2, 2021.

[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]. T. Ganesan, "Integrating Artificial Intelligence And Cloud Computing For The Development Of A Smart Education Management Platform: Design, Implementation, And Performance Analysis," Int. J. Eng., vol. 11, no. 2.

[11]. M. V. Devarajan, S. Aluvala, V. Armoogum, S. Sureshkumar, and H. T. Manohara, "Intrusion Detection in Industrial Internet of Things Based on Recurrent Rule-Based Feature Selection," in 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON), Aug. 2024, pp. 1–4. doi: 10.1109/NMITCON62075.2024.10698962.

[12]. M. V. Devarajan, A. R. G. Yallamelli, V. Mamidala, R. K. M. K. Yalla, T. Ganesan, and A. Sambas, "IoT-based enterprise information management system for cost control and enterprise job-shop scheduling problem," Serv. Oriented Comput. Appl., Nov. 2024, doi: 10.1007/s11761-024-00438-3.

[13]. V. Mamidala, "Leveraging Robotic Process Automation (RPA) for Cost Accounting and Financial Systems Optimization — A Case Study of ABC Company," vol. 7, no. 6.

[14]. G. Thirusubramanian, "Machine Learning-Driven AI for Financial Fraud Detection in IoT Environments," Int. J. HRM Organ. Behav., vol. 8, no. 4, pp. 1–16, Oct. 2020.

[15]. V. Mamidala, "Optimizing Performance with Parallel K-Means in Tunnel Monitoring Data Clustering Algorithm for Cloud Computing," Int. J. Eng. Res. Sci. Technol., vol. 17, no. 4, pp. 34–49, Dec. 2021.

[16]. T. Ganesan, M. Almusawi, K. Sudhakar, B. R. Sathishkumar, and K. S. Kumar, "Resource Allocation and Task Scheduling in Cloud Computing Using Improved Bat and Modified Social Group Optimization," in 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON), Aug. 2024, pp. 1–5. doi: 10.1109/NMITCON62075.2024.10699250.

[17]. A. R. G. Yallamelli, "Cloud Computing And Management Accounting In Smes: Insights From Content Analysis, Pls- Sem, And Classification And Regression Trees," Int. J. Eng., vol. 11, no. 3.
[18]. M. V. Devarajan, A. R. G. Yallamelli, V. Mamidala, R. K. M. K. Yalla, T. Ganesan, and A. Sambas, "IoT-based enterprise information management system for cost control and enterprise job-shop scheduling problem," Serv. Oriented Comput. Appl., Nov. 2024, doi: 10.1007/s11761-024-00438-3.
[19]. S. Nelson, A. Raj Gaius Yallamelli, A. Alkhayyat, N. Naga Saranya, and S. M, "Hybrid Autoregressive Integrated Moving Average and Bi-directional Gated Recurrent Unit for Time Series Forecasting," in 2024 International Conference on Data Science and Network Security (ICDSNS), Jul. 2024, pp. 1–4. doi: 10.1109/ICDSNS62112.2024.10690898.
[20]. 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.
[21]. M. V. Devarajan and C. Solutions, "An Improved Bp Neural Network Algorithm For Forecasting Workload In Intelligent Cloud Computing," Vol. 10, No. 9726, 2022.
[22]. T. Ganesan, "Securing Iot Business Models: Quantitative Identification Of Key Nodes In Elderly Healthcare Applications," vol. 12, no. 3.
[23]. A. R. G. Yallamelli, "Wipro Ltd, Hyderabad, Telangana, India," vol. 7, no. 9726, 2019.
[24]. S. K. Alavilli, "Smart Networks And Cloud Technologies: Shaping The Next Generation Of E-Commerce And Finance," vol. 12, no. 4.
[25]. S. H. Grandhi, "Microcontroller With Event Bus Signal Processing For Efficient Rare-Event Detection In Iot Devices," Int. J. Eng., vol. 13, no. 2, 2023.
[26]. H. Nagarajan, "Streamlining Geological Big Data Collection and Processing for Cloud Services," vol. 9, no. 9726, 2021.