Grenze International Journal of Engineering and Technology, June Issue

Comprehensive Survey and Design of a Secure and Intelligent Healthcare Fraud Detection Framework by Integrating Blockchain and Deep Learning

Anshika Negi[1] and Renuka Arora[2]
[1]Phd Student, Department of Computer Science and Engineering, Jagannath University, Bhadurgarh, India Faculty, Department of Information Technology, ADGIPS Delhi, India
Email: anshunegi2@gmail.com
[2]Department of Computer Science and Engineering Jagannath University Bhadurgarh , India
Email: renuka.arora@jagannathuniversityncr.ac.in

***Abstract*— The issue of Healthcare Fraud detection has gained prominence due to the emergence of sophisticated frauds in the virtual world. Recent works used BChain, Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) to build safe and smart identification systems. The current survey paper is a synthesis of other authors, exploring the techniques, frameworks, and performance comparison of other authors. The paper has distinguished the strengths and weaknesses of various methods by categorizing the current methods based on the technology applied in each method. Alongside this, it also determines some of the critical gaps in research and qualifies future directions regarding the evolution of adaptive, secure, and scalable fraud detection systems.**

***Keywords*— Blockchain, Deep Learning, Fraud Detection, Healthcare Sector.**

I. INTRODUCTION

The healthcare industry is augmented on digital technologies to control patient information, insurance claims, prescriptions, diagnostics, and billing systems. Nonetheless, the industry has also become susceptible to such serious challenges as the breach of data, insurance fraud, identity theft, and manipulation of health records due to this digital transformation. These not just destroy the trust between the patients but also result in huge financial losses and undermine healthcare systems in many countries across the globe [1].

Convenient methods of fraud detection and data management are usually not sophisticated enough to combat advance frauds and are not as transparent, which requires real-time monitoring. In that regard, the union of the Blockchain technology with Deep Learning is a transformative solution. Blockchain is a decentralized registry where changes cannot be altered to guarantee the invariable nature and openness of healthcare transactions. In the meantime, deep learning can notice complicated trends and abnormalities in vast quantities of medical data, thus removing the need to notice type of fraud or operating abnormalities in time [5].

The legacy fraud detection models are purely rule engine based and are designed by the domain experts. These processes identify the normal patients as abnormal because a normal patient is a violator of the established rules at times. Due to this, the fraudsters are awarded the opportunity and may seek to claim false superiority. This is why, all such procedures possess a lot of false positive rate [19].

Grenze ID: 01.GIJET.12.2.32_20

Health claims processing is a relevant factor on the medical and insurance industry, and ensures that the medical providers will be paid on time and patients will be able to undergo a hassle free reimbursement process. Nonetheless, the traditional approaches to claims processing are marred by lack of efficiency, human errors and corruption that make them very costly and time-consuming at the administrative level.

A. Example of Indian Healthcare Frauds

Ayushman Bharat Scheme Fraud: Through the flagship health insurance scheme of the government, Ayushman Bharat Pradhan Mantri Jan Arogya Yojana, there have been so many reports of fraudulent claims. This involves instances in which the hospitals overstated insurance claims and some states such as Haryana, Punjab, and Himachal Pradesh registered a high percentage of the false claims. The fraud is carried out when the private hospitals present the claims that are not admissible because of abuse, misuse, or wrong entries.

Pharmaceutical Firm Bank Fraud: The Directorate of Enforcement in Chennai conducted searches at locations linked to a pharmaceutical firm in a case involving a ₹637 crores bank fraud. The company and its promoters were accused of siphoning off bank funds through shell entities, rotating funds to inflate turnover, and illegally acquiring assets.

"Fake" Lab Test Allegations: The Aam Aadmi Party's Mohalla Clinics in Delhi have come under scrutiny for allegations of "fake" lab tests. The Central Bureau of Investigation (CBI) has also been involved in probing these allegations.

II. Comparative Analysis of Various Approaches for Fraud Detection in Healthcare Sector

To design secure and Intelligent Healthcare Fraud Detection Framework, the various approaches proposed in different research papers are being discussed.

The detailed description about various approaches for Fraud Detection in healthcare sector along with their pros and cons are shown in Table 1 as follows:

TABLE I: THE FOLLOWING TABLE PROVIDES VARIOUS PROS AND CONS OF THE APPROACHES FOR FRAUD DETECTION IN HEALTHCARE SECTOR

Ref	Author(s) / Year	Objectives	Methodology	Findings	Limitations
1	Mohammed et al. (2023)	Propose a fraud detection model using ML for Blockchain-based healthcare	Supervised machine learning integrated with Blockchain	Achieved high fraud detection accuracy in simulated networks	Limited to simulated data; lacks real-time system validation
2	Bello et al. (2024)	Develop a conceptual framework integrating ML and Blockchain for fraud detection	Conceptual modeling and design of ML-Blockchain integration	Real-time monitoring and prevention mechanisms presented	Lacks empirical validation; not tested in real healthcare systems
3	Amponsah et al. (2022)	Improve healthcare claim fraud detection using ML + Blockchain	Ensemble machine learning with decentralized data processing	Increased detection rates, reduced processing times	Data availability and interoperability remain concerns
4	Omidian (2024)	Explore synergy of AI and Blockchain in healthcare optimization	Review and theoretical integration of AI and Blockchain	Conceptual enhancement in transparency and diagnosis	Lacks implementation and quantifiable impact metrics
5	Zhang et al. (2022)	Detect medical insurance fraud using DL + Blockchain	Deep learning on Blockchain-verified insurance datasets	Improved fraud classification accuracy over baselines	Requires high computational resources; scalability issues
6	Ali et al. (2023)	Enhance security and scalability of healthcare via Blockchain + hybrid DL	Hybrid deep learning with Blockchain infrastructure	High performance in multi-layer security validation	Complex architecture and integration overhead
7	Datta et al. (2025)	Secure and transparent healthcare using energy-efficient Blockchain-AI model	AI-driven Blockchain with smart contracts and edge computing	Enhanced energy efficiency, security, transparency	Limited support for legacy systems; implementation cost
8	Kapadiya et al. (2022)	Analyze architecture for AI-Blockchain fraud detection in insurance	Analytical study of Blockchain-AI fusion with use-case discussion	Comprehensive model shows scalability and efficiency	Mostly theoretical; limited prototype testing

9	Prova (2024)	Apply ML to detect healthcare fraud	Traditional ML algorithms on insurance datasets	Noted significant anomaly detection with minimal errors	No Blockchain integration; privacy concerns persist
10	Rane et al. (2023)	Enhance financial security and transparency using AI + Blockchain	Blockchain-AI security model proposed for finance (with health relevance)	Proposes real-time fraud detection and secure transactions	Focused on finance; healthcare application is indirect
11	Kumar & Gupta (2023)	To assess the role of ML and DL in enhancing Blockchain-based fraud detection	Comparative study using ML and DL approaches in Blockchain environments	ML and DL improve fraud detection accuracy in Blockchain-based healthcare systems	Lack of real-time implementation and limited scalability evaluation
12	Narne (2024)	To explore ML techniques for health insurance fraud detection	Review of ML algorithms and real-world use cases	ML offers substantial potential in automating fraud detection	Insufficient evaluation of ethical and privacy concerns
13	Taher et al. (2024)	To design an ensemble learning and explainable AI model for Blockchain fraud detection	XAI-based ensemble model tested on Blockchain datasets	Enhanced interpretability and accuracy in detecting fraudulent Blockchain transactions	Dataset bias and overfitting concerns remain
14	Mackey et al. (2020)	To conceptualize a Blockchain framework for healthcare fraud prevention	Prototype-based Blockchain antifraud framework	Blockchain ensures auditability, traceability, and reduction of fraud	Prototype stage only; lacks empirical large-scale validation
15	Vijay Anand et al. (2025)	To design a secure Blockchain using federated learning and LSTM autoencoders	Federated learning with LSTM autoencoders applied in a Blockchain environment	High efficiency and data privacy achieved	Computational complexity and training overhead not addressed
16	Masud et al. (2024)	To integrate ML with Blockchain to secure financial transactions	Conceptual analysis with simulated fraud scenarios	Blockchain + ML improves transparency and detection	Limited real-world experimentation
17	Selvamuthu et al. (2024)	To streamline claims processing via Blockchain for fraud prevention	Blockchain-based health insurance framework with automated verification	Significant time reduction and fraud prevention achieved	Focused only on insurance; generalizability to other domains limited
18	Alzoubi (2024)	To evaluate synergy of AI and Blockchain for secure and efficient systems	Theoretical and practical review of security-enhancing use cases	Enhanced system security, data trust, and process transparency	Generalized approach; lacks domain-specific experimental results
19	Buvana & Gayathri (2025)	To protect healthcare data privacy using ECC and DL-based key tuning	ECC encryption integrated with DL for secure Blockchain storage	Improved privacy, security, and efficient key management	Complexity in integrating DL and ECC at scale
20	Jubiter (2025)	To detect real-time fraud in fintech via Blockchain and ML	Real-time analytics framework integrating ML with Blockchain	Quick fraud response and improved accuracy	Lack of healthcare-specific validation
21	Khan & Jilani (2024)	To enable privacy-enhanced heart disease prediction using DL and Blockchain	DL model for prediction with Blockchain-based secure transmission	Strong data security and high prediction accuracy	Needs broader testing on diverse datasets
22	Abbas et al. (2025)	To improve threat detection in healthcare Blockchain systems using ML	Network traffic analysis with ML for anomaly detection	Enhanced threat detection and network resilience	Limited validation in operational healthcare environments
23	Ranganatha & Mustafa (2025)	To enhance mobile transaction fraud detection via 3D QRNN and Blockchain	Bi-directional 3D QRNN model integrated with Blockchain	High detection accuracy with improved temporal feature learning	Focused only on mobile payments; lacks cross-domain validation

24	Alonge et al. (2021)	To examine ML fraud detection algorithms for data security	Survey and implementation of multiple ML fraud algorithms	Effective pattern recognition for fraud detection	Older data and algorithms may limit relevance to current tech
25	Pranto et al. (2022)	To propose a privacy-preserving fraud detection method combining Blockchain and ML	Adaptive incentive mechanism integrated with ML and Blockchain	Privacy is preserved while maintaining fraud detection efficiency	Simulation-based results; lacks live deployment data
26	Jena et al. (2024)	To create a Blockchain-based solution to trace fraudulent healthcare claims	Hyperledger Fabric-based tracing model	Improved traceability and prevention of false claims	Requires integration with external healthcare systems for wider use

A. Frequency of Themes across the Literature Review

The integrated approaches of machine learning and Blockchain turn out to be the dominant theme in the analysis of technological themes across the shows as it became the most explored stream in the literature. The second most frequent focus is deep learning combined with Blockchain which evidence the increasing interest in the application of advanced neural network models to detect frauds and improve the security of healthcare systems. Combining several AI methods with Blockchain as hybrid AI models are also seen on the list, which again show their applicability to develop flexible and resilient fraud detection models.

Reported Performance Outcomes in Studies.

The overall results of the studied performance aggregates indicate that the most significant benefits of the use of systems are the accuracy and security, supplemented by an increased interest in privacy-preserving solutions.

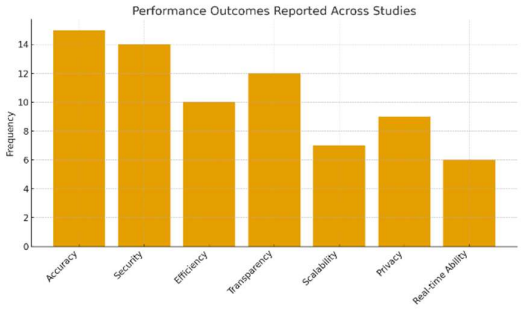

Figure 1: Performance Outcomes of various studies

III. Proposed Architecture

According to the Literature Study a proposed model combines deep learning and Blockchain technology to improve the detection of fraud and guarantee transparent and secure data management in the healthcare systems. It starts with Data Input Layer, which stores such healthcare records as insurance claims, billing data, patient histories, and EHRs. At the same time, this raw data is delivered to the Deep Learning-Based Fraud Detection Layer where sophisticated models like LSTM, CNN, or Autoencoders can be used to detect anomalies and suspicious patterns that are signs of fraud. Fraud alerts or scores in detector are the outputs of this layer [2].

The results are then forwarded to the Blockchain-Based Secure Data Management Layer whereby the authenticated data is stored in a decentralized and immutable ledger. This layer guarantees that the records are unchanged, reliable and untouched by applying smart contract to implement rules that are automatic and designed to prohibit suspicious activities or limit unauthorized access. The Blockchain is such that the transactions, and results in the detection of fraud can be traced, verified and also not manipulated [28].

Lastly, there is a User Interface Layer that offers the healthcare stakeholders to interoperate with the system. It is on this interface that users are able to see flagged records and get access to past transaction logs and confirm the authenticity of the information stored on the Blockchain. When these elements are integrated, it is possible to have smooth data flow, detecting fraud in real-time, and a high level of security, as well as enhanced transparency, which is why the proposed model is a complex solution to the long-standing problem of healthcare fraud and data manipulations [8].

The suggested model is a combined framework where the use of the Blockchain technology is combined with the deep learning algorithms to improve the detection of the fraud, data integrity, and transparency in the healthcare

systems [6]. The model is made to overcome the shortcomings of the current systems through the integration of the decentralized security and immutability of the Blockchain with the smartly anomaly detection features of the deep learning [20].

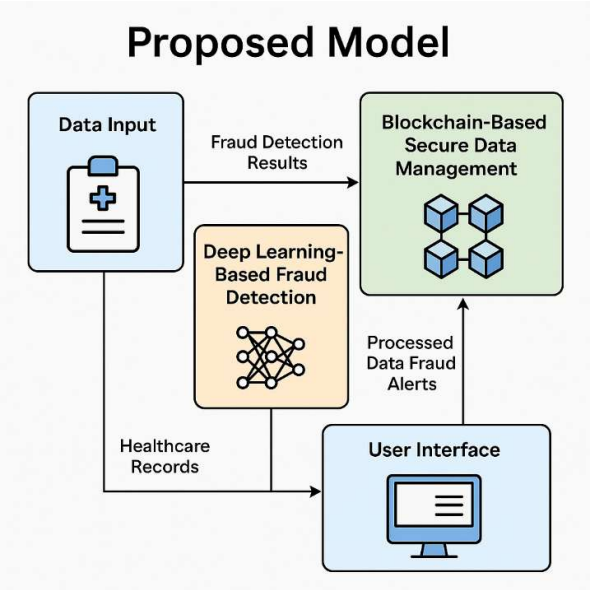

Figure 2. Proposed Architecture based on the basis of various studies

A. Core Components of the Proposed Model

Data Input Layer: Data of the health is obtained through the EHR systems in the form of insurance claims, billing information, patient history, and diagnostics. This data is pre-processed, de-identified and formatted to be analyzed.

Deep Learning-based Fraud Detection Layer: This layer will use sophisticated deep learning models (i.e., LSTM, CNN, or Autoencoders) that are being trained on labeled health datasets. The model identifies fraud acts using anomalies and trends in the records of patients and claim histories. Outputs are the scores of chances of fraud or flags of anomaly [13].

Secure Data Management Layer: Permission Blockchain (e.g., Hyper ledger Fabric) is implemented to store healthcare records and logs of the transactions. Smart contracts are used to automate access permission, verify claims and audit. In order to ascertain data progression that is identified to be fraud, they are time stamped and archived permanently [12].

Integration & Communication Layer: It guarantees the high-quality real-time communication between the deep learning engine and Blockchain ledger. Middleware/APIs facilitate connectivity, exchange of information between the AI module and Blockchain backend [19].

It has User Interface Layer: a dashboard displayed on the web or mobile assists the healthcare provider, the insurer, and regulators to see the processed data and the fraud alerts, access immutable records, and follow any analytics and reports [22].

IV. Conclusion and Discussion

The current paper is a very detailed overview of current healthcare fraud detection techniques with the focus on the replacement of manual audits and rule-based tools with more sophisticated and data-driven analytics that are based on machine learning. Current ML solutions can leverage and analyze masses of claims, patient, and provider data to identify suspicious patterns with a remarkably high level of precision, but major issues stay, especially the imbalance in data and inability to explain deep learning models. Blockchain provides good data integrity and resistant records keeping with no effect when it comes to identifying intricate fraud patterns[30]. Due to the constraints of privacy, in many cases, studies use simulated or anonymized Medicare/Medicaid datasets, using a variety of supervised machine learning, such as Random Forest and SVM, or unsupervised anomaly detection algorithms, down to deep learning models, like Graph Neural Networks. The literature marks

hybrid frameworks, integrating the secure, transparent data infrastructure of Blockchain with the off-chain ML and deep learning analytics, as the most viable approach to consider, and allow the reliable, as well as, the most efficient fraud detection.

REFERENCES

[1] Mohammed, M. A., Boujelben, M., & Abid, M. (2023). A novel approach for fraud detection in Blockchain-based healthcare networks using machine learning. Future Internet, 15(8), 250.

[2] Bello, H. O., Idemudia, C., & Iyelolu, T. V. (2024). Integrating machine learning and Blockchain: Conceptual frameworks for real-time fraud detection and prevention. World Journal of Advanced Research and Reviews, 23(1), 056-068

[3] Amponsah, A. A., Adekoya, A. F., & Weyori, B. A. (2022). A novel fraud detection and prevention method for healthcare claim processing using machine learning and Blockchain technology. Decision Analytics Journal, 4, 100122.

[4] Omidian, H. (2024). Synergizing Blockchain and artificial intelligence to enhance healthcare. Drug Discovery Today, 29(9), 104111.

[5] Zhang, G., Zhang, X., Bilal, M., Dou, W., Xu, X., & Rodrigues, J. J. (2022). Identifying fraud in medical insurance based on Blockchain and deep learning. Future Generation Computer Systems, 130, 140-154.

[6] Ali, A., Ali, H., Saeed, A., Ahmed Khan, A., Tin, T. T., Assam, M., ... & Mohamed, H. G. (2023). Blockchain-powered healthcare systems: enhancing scalability and security with hybrid deep learning. Sensors, 23(18), 7740.

[7] Datta, S., Namasudra, S., Moparthi, N. R., Kumari, S., & Crespo, R. G. (2025). Transforming Healthcare With Artificial Intelligence and Blockchain: A Secure, Transparent and Energy-Efficient Approach. Expert Systems, 42(8), e70101.

[8] Kapadiya, K., Patel, U., Gupta, R., Alshehri, M. D., Tanwar, S., Sharma, G., & Bokoro, P. N. (2022). Blockchain and AI-empowered healthcare insurance fraud detection: an analysis, architecture, and future prospects. Ieee Access, 10, 79606-79627.

[9] Prova, N. N. I. (2024, August). Healthcare fraud detection using machine learning. In 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) (pp. 1119-1123). IEEE.

[10] Rane, N., Choudhary, S., & Rane, J. (2023). Blockchain and Artificial Intelligence (AI) integration for revolutionizing security and transparency in finance. Available at SSRN 4644253.

[11] Kumar, Y., & Gupta, S. (2023). Effectiveness of machine and deep learning for Blockchain technology in fraud detection and prevention. In Blockchain Technology in Healthcare-Concepts, Methodologies, and Applications (pp. 214-236). Bentham Science Publishers.

[12] Narne, H. (2024). Machine Learning for Health Insurance Fraud Detection: Techniques, Insights, and Implementation Strategies. International Journal Of Research And Analytical Reviews.

[13] Taher, S. S., Ameen, S. Y., & Ahmed, J. A. (2024). Advanced fraud detection in Blockchain transactions: An ensemble learning and explainable ai approach. Engineering, Technology & Applied Science Research, 14(1), 12822-12830.

[14] Mackey, T. K., Miyachi, K., Fung, D., Qian, S., & Short, J. (2020). Combating health care fraud and abuse: Conceptualization and prototyping study of a Blockchain antifraud framework. Journal of medical Internet research, 22(9), e18623.

[15] Vijay Anand, R., Magesh, G., Alagiri, I., Brahmam, M. G., Balusamy, B., Selvan, C. P., ... & Soufiene, B. O. (2025). Design of an improved model using federated learning and LSTM autoencoders for secure and transparent Blockchain network transactions. Scientific Reports, 15(1), 1615.

[16] Masud, S. B., Rana, M. M., Sohag, H. J., Shikder, F., Faraji, M. R., & Hasan, M. M. (2024). Understanding the financial transaction security through Blockchain and machine learning for fraud detection in data privacy and security. Available at SSRN 5164958.

[17] Selvamuthu, C. M., Lavaraju, B., & Sundaram, A. (2024, October). A novel approach of streamlining claims processing and fraud prevention in health insurance through Blockchain technology. In 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 611-618). IEEE.

[18] Alzoubi, M. M. (2024). Investigating the synergy of Blockchain and AI: enhancing security, efficiency, and transparency. Journal of Cyber Security Technology, 1-29.

[19] Buvana, J., & Gayathri, R. (2025). Blockchain-driven Privacy-Preservation of Healthcare Insurance Data using Improved ECC based Encryption and Deep Learning based Key Tuning. Knowledge-Based Systems, 114078.

[20] Jubiter, F. (2025). Blockchain and Machine Learning Integration for Real-Time Fraud Detection in Fintech. International Journal of Emerging Trends in Computer Science and Information Technology, 539-548.

[21] Khan, A. R., & Jilani, A. K. (2024). Privacy-Enhanced Heart Disease Prediction in Cloud-Based Healthcare Systems: A Deep Learning Approach with Blockchain-Based Transmission. Fusion: Practice & Applications, 15(1).

[22] Abbas, R., Ogunsanya, V. A., Nwanyim, S. J., Afolabi, R., Kagame, R., Akinsola, A., & Clement, T. (2025). Leveraging Machine Learning to Strengthen Network Security and Improve Threat Detection in Blockchain for Healthcare systems. International Journal of Scientific and Management Research, 8(02), 147-165.

[23] Ranganatha, H. R., & Mustafa, A. S. (2025). Enhancing fraud detection efficiency in mobile transactions through the integration of bidirectional 3d Quasi-Recurrent Neural network and Blockchain technologies. Expert Systems with Applications, 260, 125179.

[24] Alonge, E. O., Eyo-Udo, N. L., Ubanadu, B. C., Daraojimba, A. I., Balogun, E. D., & Ogunsola, K. O. (2021). Enhancing data security with machine learning: A study on fraud detection algorithms. Journal of Data Security and Fraud Prevention, 7(2), 105-118.
[25] Pranto, T. H., Hasib, K. T. A. M., Rahman, T., Haque, A. B., Islam, A. N., & Rahman, R. M. (2022). Blockchain and machine learning for fraud detection: A privacy-preserving and adaptive incentive-based approach. Ieee Access, 10, 87115-87134.
[26] Jena, S. K., Kumar, B., Mohanty, B., Singhal, A., & Barik, R. C. (2024). An advanced Blockchain-based hyperledger fabric solution for tracing fraudulent claims in the healthcare industry. Decision Analytics Journal, 10, 100411.
[27] Irum Matloob; Shoab Ahmed Khan; Habib Ur Rahman (2020).Sequence Mining and Prediction-Based Healthcare Fraud Detection Methodology.IEEE (143256 - 143273)
[28] Ankita Ghosh; Sudip Diyasi; Dipankar Dey(2025). Enhancing Blockchain Transaction Security: A Hybrid Machine Learning Approach for Fraud Detection. International Journal on Smart & Sustainable Intelligent Computing Vol. 02, Iss. 01, S. No.002, pp.14-30.
[29] Hota, A., Biswas, A., Saha, S. et al. (2025). Blockchain and deep learning-based approach towards privacy preserving healthcare solutions. Multimed Tools Appl 84, 41583–41613 (2025).
[30] Matloob, I., Khan, S., Rukaiya, R. et al. Healthcare fraud detection using adaptive learning and deep learning techniques. Evolving Systems 16, 72 (2025).
[31] Raktim Dey; Ashutosh Roy; Jasmin Akter; Aashish Mishra and Malay Sarkar(2025).Journal of Computer Science and Technology Studies. ISSN:2709-104X.
[32] Arora, R.K and Badal,D., Subject Distribution using Data Mining, I J. of Research in Engineering and Technology, Volume 2, Issue 12
[33] Shobana J, Ch. Gangadhar, Rakesh Kumar Arora, P.N.Renjith, J. Bamini, Yugendra Devidas , E-commerce customer churn prevention using machine learning-based business intelligence strategy, Measurements:Sensors, Volume 27, June 2023 (DOI: 10.1016/j.measen.2023.100728) ISSN: 2665-9174
[34] Narayanan S., Arora, R.K., Gangwar S., Kandhasamy J., Ratheesh, Murali K, Ultra-low latency communication technique for augmented reality application in mobile edge computing, Int. J. of Engineering Systems Modelling and Simulation, Vol 15, Number 3,pp 97-105
[35] Jacob,V. , Tandon, A. , Jeevitha, S., Arora, R.K., Laddha, S., Salunkhe, S. , Portable Healthcare Computing and Clinical Decision Support System Enabled by Artificial Intelligence, Int. J. of Engineering Systems Modelling and Simulation, Vol 13, Number 3,pp 228-233