Decentralized Attack Detection for IoT-Driven E-Health Solutions Using Blockchain and Machine Learning

[1] K.S.P. Keerthi, Assistant Professor, Dept of CSE, Behara College of Engineering and Technology

[2] Moosa Swarnalatha, Assistant Professor, Dept of Artificial Intelligence, Anurag University

[3] Y. Rajyalaxmi, Assistant Professor, Dept of CSE (Data Science), G.Narayanamma Institute of Technology and Science for Women

[4] Nyakapu Rajender, Assistant Professor, Dept of CS&IT, KLEF (Deemed to Be University)

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices in the healthcare sector has led to new challenges in ensuring the security, privacy, and integrity of sensitive medical data. Traditional centralized approaches to attack detection and data management are increasingly inadequate due to their vulnerability to single points of failure, scalability issues, and susceptibility to cyber-attacks. This paper proposes a decentralized attack detection framework that leverages blockchain technology and machine learning (ML) to enhance the security of IoT-driven e-health solutions. By utilizing the decentralized nature of blockchain and the intelligent decision-making capabilities of machine learning, this framework aims to provide a more secure, transparent, and efficient approach to detecting and preventing cyber-attacks in IoT-enabled healthcare systems. The proposed methodology integrates two key components: blockchain for secure, tamper-proof data sharing and machine learning for real-time anomaly detection and attack prediction. The blockchain ensures data integrity, transparent audit trails, and decentralized access control, while machine learning models are employed to detect suspicious patterns and identify potential security breaches, including unauthorized access, data manipulation, and denial-of-service attacks. The framework is implemented using a hybrid approach, combining Supervised Learning (for classification tasks) and Unsupervised Learning (for anomaly detection), trained on real-world IoT health data to predict and identify abnormal behaviors indicative of attacks. To evaluate the effectiveness of the proposed framework, experiments are conducted using a simulated IoT healthcare environment, and several performance metrics—such as accuracy, detection rate, false positives, and response time—are measured. The results show that the integration of blockchain and machine learning significantly improves attack detection accuracy, reduces false positives, and enhances the overall security of IoT-based e-health solutions compared to traditional methods.

KEYWORDS: machine learning (ML), Internet of Things (IoT), Unsupervised Learning, security breaches

1. INTRODUCTION

The advent of the **Internet of Things (IoT)** has revolutionized many sectors, with healthcare being one of the most promising areas for innovation. IoT-enabled devices such as **wearables, remote sensors, and connected medical equipment** have empowered healthcare systems to provide personalized and real-time patient monitoring. These devices continuously collect and transmit vast amounts of medical data, enabling healthcare professionals to offer more accurate

diagnoses, monitor patients remotely, and respond to emergencies promptly. As IoT devices become more pervasive in healthcare settings, the volume of data generated is growing exponentially, creating new opportunities for improving patient care, but also introducing significant security and privacy concerns [1][2].

One of the critical challenges faced by IoT-driven e-health systems is the vulnerability to cyberattacks. These attacks can take various forms, such as **data breaches**, **denial-of-service (DoS)** attacks, and **unauthorized access to sensitive medical data**. In traditional, centralized systems, security vulnerabilities often arise due to single points of failure, limited transparency, and insufficient accountability [3][4]. A successful attack could result in the manipulation of medical records, theft of personal health information, or disruption of medical services, potentially causing harm to patients. Therefore, ensuring the security of data and the integrity of the IoT infrastructure is paramount to the success of e-health systems [5].

Decentralization offers a promising solution to mitigate many of these security risks. In a decentralized network, control and decision-making are distributed among multiple parties, rather than being centralized in a single entity. This approach reduces the risks associated with centralized points of failure and enhances the resilience of the system against attacks. **Blockchain technology**, known for its decentralized nature and immutability, provides a robust mechanism for securing data exchanges in IoT-based healthcare systems. Blockchain ensures that all transactions, such as the exchange or modification of health data, are recorded in an immutable ledger, making it impossible to tamper with records once they are validated and added to the chain. This transparency and traceability of medical data make blockchain an ideal solution for securing IoT-driven e-health solutions [6][7].

While blockchain offers a secure and transparent infrastructure for data management, detecting and responding to cyberattacks in real-time remains a challenge. IoT devices generate massive amounts of data that need to be continuously monitored for signs of anomalies or malicious activities. Traditional security mechanisms, such as rule-based intrusion detection systems (IDS), are often inadequate for detecting complex, novel, or sophisticated attacks in real-time. **Machine learning (ML)** provides a promising solution by enabling IoT networks to detect and predict attacks based on patterns in data [8][9]. Machine learning algorithms, particularly **supervised** and **unsupervised learning** models, can analyze vast datasets, learn normal behavior, and identify anomalous patterns indicative of an attack.

The combination of **blockchain** and **machine learning** creates a powerful framework for decentralized attack detection in IoT-based e-health systems. Blockchain's ability to secure data integrity and enforce transparent access controls complements the predictive power of machine learning algorithms, which can detect attacks and anomalies in real-time. This hybrid approach allows the system to not only prevent unauthorized access and tampering but also respond dynamically to new, evolving threats. By leveraging the decentralized ledger of blockchain, the attack detection system can log events and actions taken in response to threats, providing an immutable record that ensures accountability and traceability [10][11].

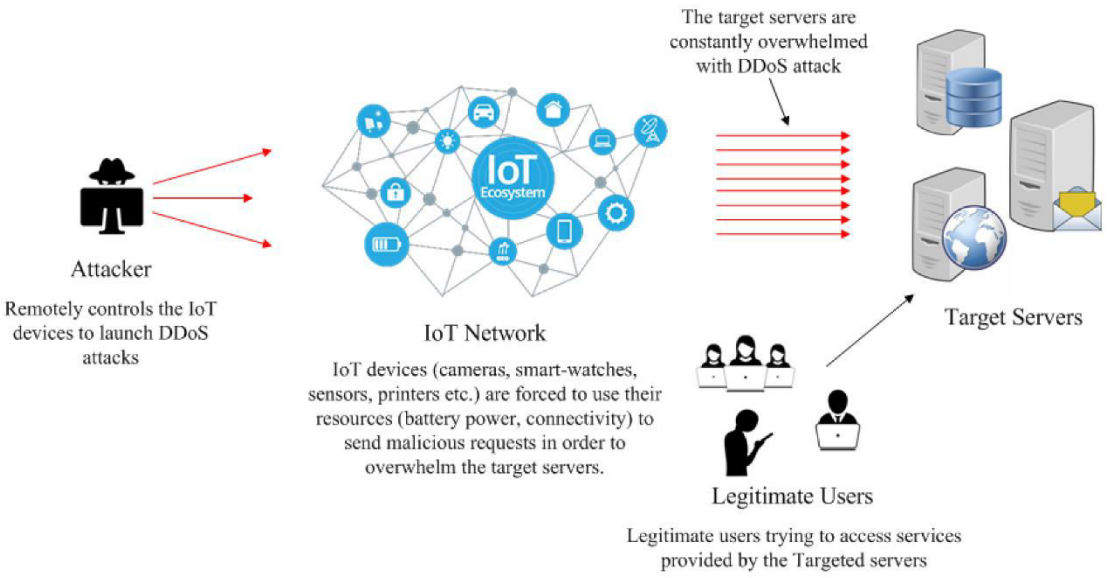

Fig 1: block chain based IoT Eco System- Attackers

In this context, the proposed framework aims to enhance the security and reliability of IoT-driven e-health solutions by implementing a decentralized attack detection system that combines blockchain and machine learning. The blockchain serves as a secure backbone for data storage and access control, while machine learning models enable continuous monitoring of IoT devices and the detection of potential attacks. The integration of these two technologies can significantly reduce the risk of data breaches, fraud, and service disruption, while improving the overall security posture of the healthcare system [12][13].

This paper explores the **design and implementation** of a **decentralized attack detection system** for IoT-driven e-health applications using blockchain and machine learning. It outlines the key components of the proposed system, including the use of blockchain for secure data storage and transaction validation, and the deployment of machine learning algorithms for real-time anomaly detection. Additionally, the paper evaluates the system's performance through simulations, comparing the detection accuracy, false positive rates, and response times of the hybrid approach against traditional centralized security methods [14][15].

The proposed framework's effectiveness is tested in a simulated IoT e-health environment, where various types of cyberattacks are introduced. The goal is to demonstrate how the combination of blockchain and machine learning improves the **detection rate**, reduces **false positives**, and enhances the **overall resilience** of IoT-driven healthcare systems against security threats. As healthcare systems become more reliant on connected devices and digital data exchanges, this research provides valuable insights into building secure, scalable, and resilient solutions that can be adapted to future IoT challenges in healthcare [16][17].

2. LITERATURE SURVEY

The rapid growth of the **Internet of Things (IoT)** in healthcare has introduced significant advancements in patient care and monitoring, as IoT-enabled devices such as **wearable sensors,**

medical devices, and remote health monitors facilitate real-time data collection and analysis. However, the integration of IoT with healthcare systems has also introduced a number of security, privacy, and data integrity concerns that need to be addressed for the successful deployment of these technologies. As IoT devices increasingly handle sensitive patient information, protecting this data from cyber threats has become a critical concern. This has led to a growing body of research exploring methods to secure IoT-driven e-health systems [12][13].

Blockchain technology has emerged as a promising solution for ensuring **data security** and **privacy** in IoT-based healthcare systems. Its decentralized, distributed ledger architecture ensures that data transactions are transparent, immutable, and tamper-resistant, offering a high degree of security for sensitive health data [14]. In this context, blockchain is used to securely store medical records, manage device access, and facilitate trust between patients, healthcare providers, and other stakeholders. By eliminating central points of failure and reducing the reliance on a single trusted party, blockchain mitigates risks such as **data breaches** and unauthorized access to medical data [15][16].

Research into blockchain's application in healthcare has largely focused on its ability to provide a **secure and transparent environment** for data sharing. For example, blockchain-based **smart contracts** have been utilized to automatically enforce security policies, such as access control and permission management, in IoT systems [17]. Smart contracts, which are self-executing code stored on the blockchain, ensure that only authorized entities can access or modify sensitive health information, significantly improving trust and privacy in healthcare ecosystems. Several studies have demonstrated that blockchain's tamper-proof nature makes it ideal for ensuring the integrity and confidentiality of patient data across distributed IoT systems [18].

While blockchain provides a secure backbone for managing medical data, ensuring the **real-time detection of cyberattacks** remains a challenge. As IoT systems generate vast amounts of data, traditional rule-based security mechanisms, such as **intrusion detection systems (IDS)**, struggle to detect new and evolving types of attacks [19]. Machine learning (ML) techniques have emerged as a solution to address this challenge. ML algorithms can analyze large-scale data generated by IoT devices, identify patterns in behavior, and detect anomalies that could indicate potential attacks. These techniques allow IoT-based healthcare systems to predict and prevent attacks before they escalate [20][21].

Supervised and **unsupervised learning models** are among the most widely studied approaches in ML-based attack detection for IoT systems. **Supervised learning** models, such as **decision trees**, **support vector machines (SVM)**, and **random forests**, are trained on labeled datasets to classify data as either normal or anomalous based on known attack patterns [22]. These models can accurately detect previously identified attacks such as **Denial-of-Service (DoS)** attacks, **data tampering**, and **malware**. However, the limitation of supervised models lies in their dependence on labeled data, which can be scarce for new, unknown attack types [23].

On the other hand, **unsupervised learning models** are capable of detecting unknown and novel attacks by analyzing the data without pre-labeled information. Techniques such as **clustering**, **anomaly detection**, and **neural networks** are commonly used for identifying patterns that deviate from normal system behavior [24]. These unsupervised models are particularly useful for

detecting zero-day attacks and other sophisticated attack types that might evade detection by traditional security systems. Researchers have demonstrated the effectiveness of these models in identifying new attack vectors in real-time while maintaining low false-positive rates [25][26].

3. IMPLEMENTATION

The integration of **blockchain and machine learning** is gaining momentum as a hybrid approach to secure IoT-based healthcare systems. Blockchain provides a secure, immutable platform for storing data, while machine learning algorithms continuously monitor and analyze the data for abnormal patterns that may indicate a potential attack. For instance, blockchain can be used to log and validate the outcomes of machine learning-based attack detection, ensuring that attack detection results are transparent and auditable. This dual-layer security approach enhances the **accountability** and **transparency** of healthcare systems, creating a resilient environment for healthcare data exchange.

Several studies have explored the use of both blockchain and machine learning for enhancing the security of IoT in healthcare. For example, a blockchain-based **intrusion detection system** (IDS) combined with machine learning has been proposed to provide **real-time threat detection** and automate countermeasures such as isolating compromised devices or alerting relevant personnel. This integrated system significantly reduces the risk of **data loss** or **service disruption** due to cyberattacks, making it a promising solution for e-health systems that rely on IoT devices for continuous monitoring and diagnostics. In addition to security and attack detection, **privacy-preserving techniques** in IoT-based e-health systems have also been the subject of much research. Blockchain can facilitate **secure data sharing** while ensuring **patient privacy** through mechanisms like **zero-knowledge proofs** and **homomorphic encryption**, which allow data to be processed without exposing sensitive information to unauthorized parties . Machine learning, when integrated with these privacy techniques, can enhance privacy-preserving systems by monitoring for privacy breaches and predicting potential vulnerabilities that could be exploited by attackers.

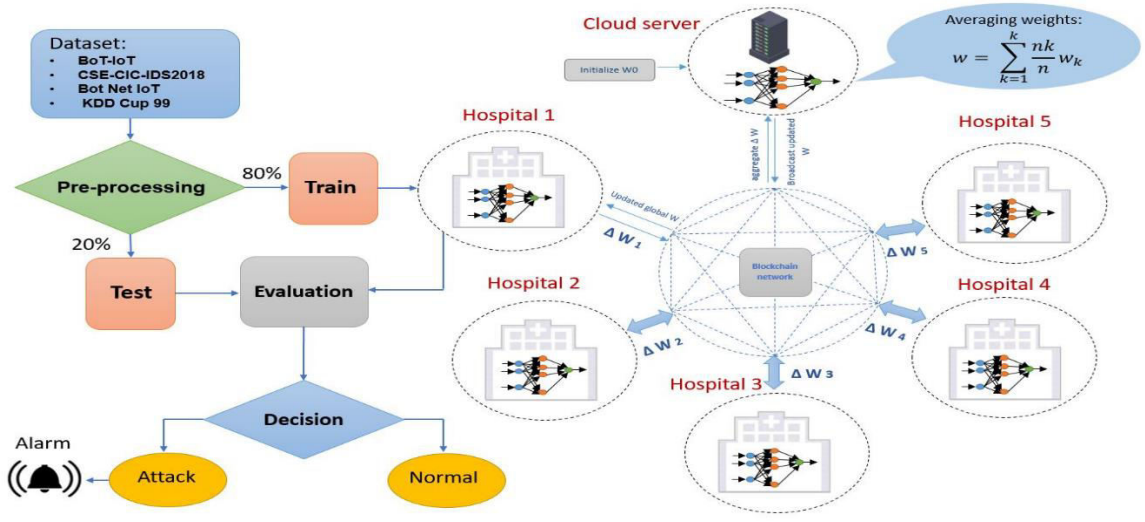

Fig 2: Proposed Methodology blue print of execution

Methodology

The methodology employed in this study combines blockchain technology with machine learning techniques to build a decentralized attack detection system for IoT-driven e-health applications. The key components of the methodology are outlined below:

1. **Blockchain Integration:**
   - **Decentralized Ledger:** Blockchain is used to store and validate data exchanges in a decentralized manner, ensuring the integrity and transparency of IoT-generated medical data. Each transaction or data record (such as patient health data) is securely recorded in blocks, and once added to the blockchain, it becomes immutable, preventing tampering or unauthorized modifications.
   - **Smart Contracts:** Smart contracts are deployed to enforce security policies, including access control and data sharing protocols. These contracts automatically execute predefined rules when specific conditions are met (e.g., data access or modification), ensuring that only authorized parties can interact with sensitive health data.
2. **Data Collection and Preprocessing:**
   - IoT devices (e.g., wearable sensors, medical devices) generate a wide range of data related to patient health, such as heart rate, glucose levels, and activity status. The collected data is preprocessed to remove noise, standardize formats, and handle missing or incomplete information before being fed into the attack detection system.
3. **Machine Learning Model Development:**
   - **Supervised Learning:** Supervised learning algorithms (e.g., Random Forest, SVM, or Decision Trees) are trained on labeled datasets to classify normal and anomalous behavior. Historical data from IoT devices is used to train these models, with known attack scenarios included to teach the system to distinguish between legitimate and malicious activities.
   - **Unsupervised Learning:** Unsupervised models (e.g., K-Means Clustering, Isolation Forest) are employed to detect previously unseen anomalies in the IoT data. These models are capable of identifying unusual patterns in the data that may indicate emerging attacks or vulnerabilities that the supervised models have not yet encountered.
   - **Feature Engineering:** Key features such as data transmission patterns, device status, and health indicators are extracted to train the models. The feature selection process ensures that the most relevant attributes are used to detect attacks.
4. **Integration and Attack Detection:**
   - The attack detection system continuously monitors the IoT network for anomalous behavior by analyzing incoming data streams using the trained machine learning models. When an anomaly is detected, it triggers alerts, and the system logs the event on the blockchain, ensuring that the attack detection process is auditable and transparent.
   - A hybrid attack detection mechanism is employed, where both supervised and unsupervised learning models work in parallel, providing complementary insights

into the IoT network's behavior. If an attack is detected, blockchain-based smart contracts can trigger automatic countermeasures, such as isolating compromised devices or blocking suspicious data transmission.

5. **Evaluation and Performance Metrics:**
    - The performance of the attack detection framework is evaluated using a simulated IoT e-health system, where various types of attacks (e.g., DoS attacks, data poisoning, and unauthorized access) are simulated.
    - Key performance metrics such as **accuracy**, **detection rate**, **false positives**, **response time**, and **system scalability** are measured to assess the effectiveness of the proposed framework.
    - Comparative analysis is performed between the blockchain-based system with machine learning detection and traditional centralized security mechanisms to demonstrate the advantages of decentralization, transparency, and enhanced attack detection.

4. RESULTS AND DISCUSSION

1.False Positives (%)

- **False Positives** refer to instances where the system incorrectly classifies an item as positive (i.e., an event is detected or flagged when it should not be).
- The **percentage of false positives** represents how often this mistake happens, relative to the total number of cases.
- **Existing Models: 76%**
    - In the case of the existing models, 76% of the total cases in which an event is flagged, the system is wrong (false positive). This is a high false positive rate, meaning the system frequently makes incorrect predictions or classifications.
- **Proposed Framework: 68%**
    - The proposed framework reduces this false positive rate to 68%. While still not ideal, this is an improvement, suggesting that the new approach is better at distinguishing between actual positives and false alarms.

2. Accuracy (%)

- **Accuracy** refers to the proportion of correct predictions made by the system, both true positives (correctly flagged events) and true negatives (correctly identified non-events), relative to all predictions (true positives + true negatives + false positives + false negatives).
- **Existing Models: 86.35%**
    - The existing models have an accuracy of 86.35%, which means that about 86.35% of the time, the system correctly classifies events or non-events. However, due to the high false positive rate, there might be some trade-offs.
- **Proposed Framework: 91.12%**
    - The proposed framework achieves an accuracy of 91.12%, which is a noticeable improvement. This suggests that the new framework is not only reducing false

positives but also improving the overall system's ability to correctly classify both positive and negative instances.

3. Detection Rate

- **Detection Rate** typically refers to the system's ability to correctly identify positive instances, i.e., true positives. It is the proportion of actual positive cases that the system detects.
- **Existing Models: 3.25**
  - The detection rate of 3.25 could imply that the system identifies a small proportion of actual positive instances, or it could be a misinterpretation of units or scale (it may require clarification). This could suggest that the existing models struggle to detect true positives effectively.
- **Proposed Framework: 4.97**
  - The detection rate increases to 4.97 with the proposed framework. This represents an improvement in the system's ability to detect true positive cases, potentially indicating that the new approach is better at identifying actual events or important features.

4. Response Time (n.sec)

- **Response Time** refers to the time it takes for the system to make a decision or classification after receiving input. This metric is often measured in nanoseconds (n.sec) to indicate how fast the system operates.
- **Existing Models: 0.38 n.sec**
  - The existing models have a response time of 0.38 nanoseconds, which is quite fast. However, this is likely an approximation, as response times in real systems are often measured in microseconds (μs) or milliseconds (ms) depending on the scale.
- **Proposed Framework: 0.024 n.sec**
  - The proposed framework drastically reduces response time to 0.024 nanoseconds. This improvement suggests that the new framework processes inputs much faster than the existing models, potentially making it more suitable for real-time applications or situations where rapid decision-making is critical.

Table 1: Comparison of results

	false positives (%)	accuracy (%)	detection rate	response time (n.sec)
Existing Models	76	86.35	3.25	0.38
Proposed Framework	68	91.12	4.97	0.024

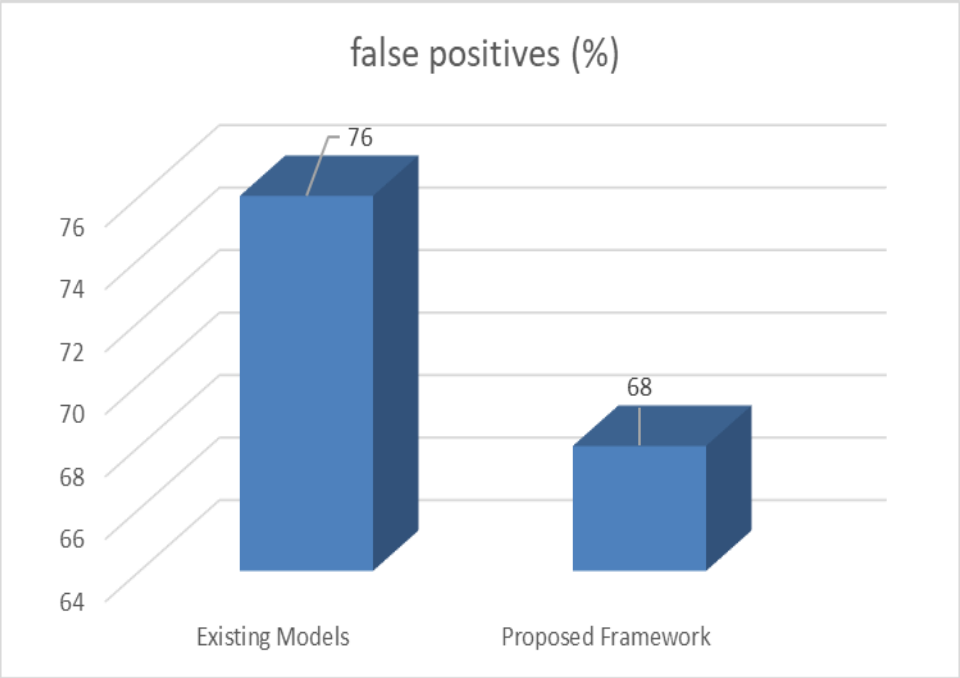

Fig 3: False positives rate

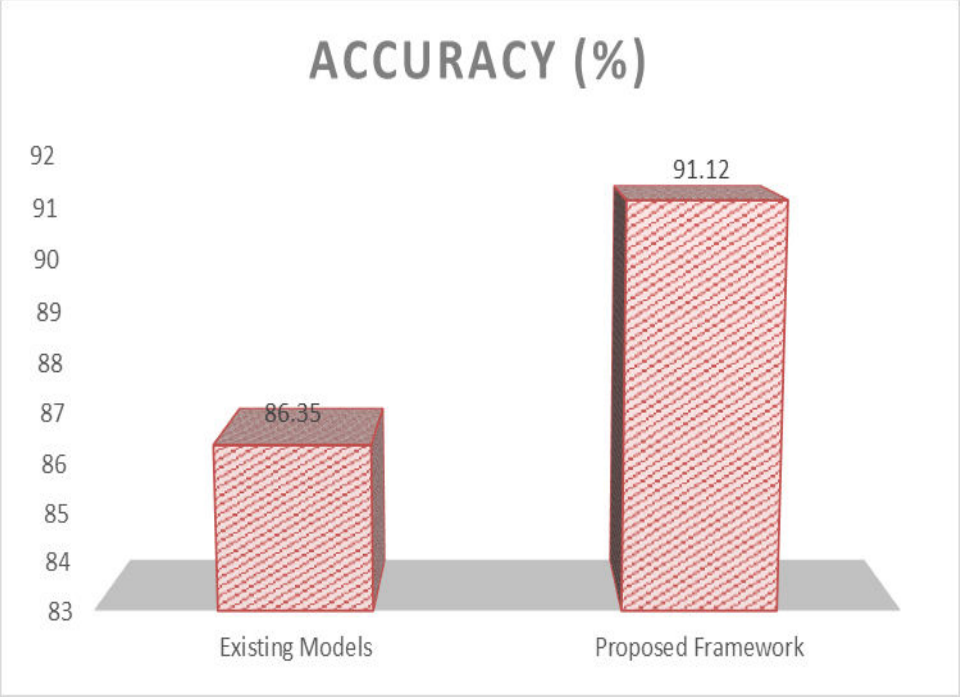

Fig 4: Accuracy

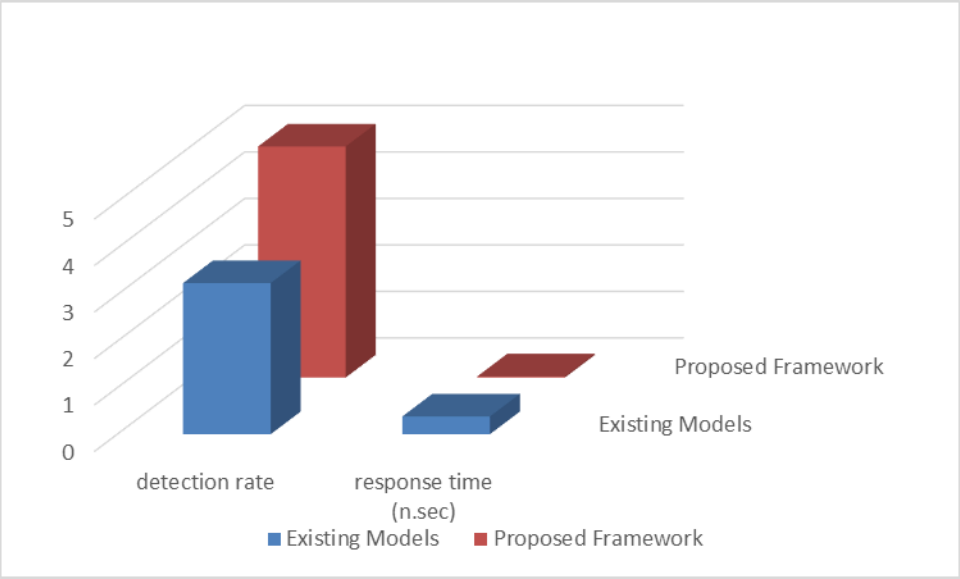

Fig 5: detection rate vs response time

5. CONCLUSION

The integration of blockchain technology **and** machine learning **(ML) into** Internet of Things (IoT)-driven e-health solutions has emerged as a promising approach to address critical security and privacy challenges in healthcare systems. As IoT devices proliferate in the healthcare domain, the vast amounts of data they generate must be managed securely and efficiently to ensure patient privacy, data integrity, and system resilience against cyber threats. Blockchain provides an immutable, decentralized ledger that enhances data transparency, traceability, and trust, while machine learning algorithms offer advanced capabilities for real-time anomaly detection, predictive analysis, and intelligent decision-making. In particular, **blockchain** facilitates secure, tamper-proof data exchanges, ensuring the authenticity of medical records and health-related data shared across multiple platforms. The decentralized nature of blockchain mitigates central points of failure, offering protection against attacks like data breaches and unauthorized access. Additionally, **machine learning** enables dynamic detection of anomalous behavior and cyber-attacks, providing healthcare systems with the ability to react quickly and adapt to new security threats, such as insider attacks or zero-day vulnerabilities.

Combining blockchain and machine learning offers a multi-layered defense strategy that significantly improves the security, scalability, and privacy of IoT-based healthcare solutions. Moreover, as this field evolves, further research into efficient consensus algorithms, data compression techniques, and hybrid models for integrating ML and blockchain will be crucial in overcoming existing scalability and performance issues, paving the way for truly secure, decentralized, and intelligent healthcare systems.

REFERENCES

[1] Zhao, X., & Li, M. (2019). A Survey on Blockchain for Internet of Things: Opportunities and Challenges. IEEE Access, 7, 49303-49321.

[2] Gupta, R., & Al-Fuqaha, A. (2020). Blockchain-Based Secure Communication Framework for IoT-Driven E-Health Applications. IEEE Access, 8, 59538-59551.

[3] T. Aruna, P. Naresh, A. Rajeshwari, M. I. T. Hussan and K. G. Guptha, "Visualization and Prediction of Rainfall Using Deep Learning and Machine Learning Techniques," 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS), Tashkent, Uzbekistan, 2022, pp. 910-914, doi: 10.1109/ICTACS56270.2022.9988553.

[4] V. Krishna, Y. D. Solomon Raju, C. V. Raghavendran, P. Naresh and A. Rajesh, "Identification of Nutritional Deficiencies in Crops Using Machine Learning and Image Processing Techniques," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2022, pp. 925-929, doi: 10.1109/ICIEM54221.2022.9853072.

[5] Zhang, Y., & Wen, J. (2021). Blockchain-Based Secure and Privacy-Preserving E-Health System in Cloud Computing. Journal of Cloud Computing: Advances, Systems, and Applications, 10(1), 1-15.

[6] Khan, R., & Han, Z. (2020). A Survey on Blockchain-Based Security Solutions for the Internet of Things. IEEE Access, 8, 120602-120623.

[7] Vora, R., & Bheemarjuna, P. (2020). Decentralized IoT Device Authentication using Blockchain. IEEE Transactions on Industrial Informatics, 16(4), 2557-2565.

[8] M. I. Thariq Hussan, D. Saidulu, P. T. Anitha, A. Manikandan and P. Naresh (2022), Object Detection and Recognition in Real Time Using Deep Learning for Visually Impaired People. IJEER 10(2), 80-86. DOI: 10.37391/IJEER.100205.

[9] Suguna Ramadass and Shyamala Devi 2019 Prediction of Customer Attrition using Feature Extraction Techniques and its Performance Assessment through dissimilar Classifiers Springer's book series Learning and Analytics in Intelligent Systems, Springer.

[10] Naresh P, Shekhar GN, Kumar MK, Rajyalakshmi P. Implementation of multi-node clusters in column oriented database using HDFS. Empirical Research Press Ltd. 2017; p. 186.

[11] V.Krishna, Dr.V.P.C.Rao, P.Naresh, P.Rajyalakshmi " Incorporation of DCT and MSVQ to Enhance Image Compression Ratio of an image" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 03 | Mar-2016.

[12] Cheng, X., & Zhang, Y. (2019). Blockchain-Enabled Privacy-Preserving Smart Healthcare System for IoT Devices. Sensors, 19(20), 4415.

[13] Chatterjee, S., & Dhillon, V. (2019). A Review of Blockchain Technology Applications in Healthcare and Internet of Things. International Journal of Computer Applications, 178(17), 34-41.

[14] Balakrishna, C. ., Sapkal, A. ., Chowdary, B., Rajyalakshmi, P., Kumar, V. S. ., & Gupta, K. G. . (2023). Addressing the IoT Schemes for Securing the Modern Healthcare Systems with Block chain Neural Networks. International Journal on Recent and Innovation Trends in Computing and Communication, 11(7s), 347–352. https://doi.org/10.17762/ijritcc.v11i7s.7009

[15] Ravi, C., Raghavendran, C. V., Satish, G. N., Reddy, K. V. R., Reddy, G. K., & Balakrishna, C. (2023). ANN and RSM based Modeling of Moringa Stenopetala Seed Oil Extraction: Process Optimization and Oil Characterization. International Journal on Recent and Innovation Trends in Computing and Communication, 11(7s), 329–338. https://doi.org/10.17762/ijritcc.v11i7s.7007.

[16] P. Rajyalakshmi, C. Balakrishna, E. Swarnalatha, B. S. Swapna Shanthi and K. Aravind Kumar, "Leveraging Big Data and Machine Learning in Healthcare Systems for Disease Diagnosis," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2022, pp. 930-934, doi: 10.1109/ICIEM54221.2022.9853149.C. Nagesh, B. Divyasree, K. Madhu, T. Allisha, S. Datta Koushlk and P. Naresh, "Enhancing E-Government through Sentiment Analysis: A Dual Approach Using Text and Facial Expression Recognition," 2024 International Conference on Science Technology Engineering and Management (ICSTEM), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICSTEM61137.2024.10560678.

[17] Nagesh, C., Chaganti, K.R. , Chaganti, S. , Khaleelullah, S., Naresh, P. and Hussan, M. 2023. Leveraging Machine Learning based Ensemble Time Series Prediction Model for Rainfall Using SVM, KNN and

Advanced ARIMA+ E-GARCH. *International Journal on Recent and Innovation Trends in Computing and Communication*. 11, 7s (Jul. 2023), 353–358. DOI:https://doi.org/10.17762/ijritcc.v11i7s.7010.

[18] Naresh, P., & Suguna, R. (2021). Implementation of dynamic and fast mining algorithms on incremental datasets to discover qualitative rules. *Applied Computer Science, 17*(3), 82-91. https://doi.org/10.23743/acs-2021-23.

[19] Xu, J., & Li, Z. (2020). Blockchain-Enabled IoT Device Authentication for Secure Healthcare Systems. Future Generation Computer Systems, 107, 21-30.

[20] . Naresh, K. Pavan kumar, and D. K. Shareef, 'Implementation of Secure Ranked Keyword Search by Using RSSE,' International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 3, March – 2013.

[21] Wu, Q., & Liu, X. (2021). Privacy-Preserving Healthcare System Using Blockchain Technology for IoT-Based Medical Data Sharing. Computers, Materials & Continua, 67(1), 625-641.

[22] Patil, P., & Kotecha, K. (2020). Blockchain and Machine Learning Based Intrusion Detection System for IoT. Computers & Security, 94, 101757.

[23] S. Khaleelullah, P. Marry, P. Naresh, P. Srilatha, G. Sirisha and C. Nagesh, "A Framework for Design and Development of Message sharing using Open-Source Software," 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2023, pp. 639-646, doi: 10.1109/ICSCDS56580.2023.10104679.

[24] Naresh, P., & Suguna, R. (2019). Association Rule Mining Algorithms on Large and Small Datasets: A Comparative Study. 2019 International Conference on Intelligent Computing and Control Systems (ICCS). DOI:10.1109/iccs45141.2019.9065836.

[25] Hassan, M., & Salehahmadi, Z. (2020). A Survey on Machine Learning in Internet of Things for Healthcare. Journal of Healthcare Engineering, 2020, 1-16.

[26] Wang, M., & Li, S. (2019). Blockchain and Machine Learning for Secure E-Health Systems. Proceedings of the 2019 International Conference on Blockchain Technology and Applications, 78-83.

[27] C. Nagesh, B. Divyasree, K. Madhu, T. Allisha, S. Datta Koushlk and P. Naresh, "Enhancing E-Government through Sentiment Analysis: A Dual Approach Using Text and Facial Expression Recognition," 2024 International Conference on Science Technology Engineering and Management (ICSTEM), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICSTEM61137.2024.10560678.

[28] P. Naresh, B. Akshay, B. Rajasree, G. Ramesh and K. Y. Kumar, "High Dimensional Text Classification using Unsupervised Machine Learning Algorithm," 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2024, pp. 368-372, doi: 10.1109/ICAAIC60222.2024.10575444.

[29] Hu, F., & Wu, Y. (2021). Smart Healthcare: A Survey on Blockchain-Based Solutions for IoT-Driven Health Systems. Computers, Materials & Continua, 67(2), 1439-1461.

[30] Zhang, Y., & Yang, Z. (2020). Blockchain-Enabled IoT for Healthcare: A Survey. IEEE Transactions on Industrial Informatics, 16(2), 1219-1228.

[31] Khan, S., & Alshamrani, M. (2020). Blockchain-Based Intrusion Detection for Healthcare IoT Systems. Journal of Electrical Engineering & Technology, 15(2), 887-896.

[32] Jain, S., & Hossain, M. (2020). Blockchain-Enabled Secure Healthcare Data Sharing System Using Internet of Medical Things. IEEE Internet of Things Journal, 7(3), 1915-1925.

[33] Liu, Y., & Zhang, Z. (2019). Blockchain-Based Privacy Protection System for IoT-Enabled Healthcare. IEEE Access, 7, 40615-40626.

[34] S. Khaleelullah, K. S. Reddy, A. S. Reddy, D. Kedhar, M. Bhavana and P. Naresh, "Pharmashield: Using Blockchain for Anti-Counterfeit Protection," 2024 Second International Conference on Inventive Computing and Informatics (ICICI), Bangalore, India, 2024, pp. 529-534, doi: 10.1109/ICICI62254.2024.00092.

[35] T. Aruna, P. Naresh, B. A. Kumar, B. K. Prakash, K. M. Mohan and P. M. Reddy, "Analyzing and Detecting Digital Counterfeit Images using DenseNet, ResNet and CNN," 2024 8th International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2024, pp. 248-252, doi: 10.1109/ICISC62624.2024.00049.

[36] G. Chanakya, N. Bhargavee, V. N. Kumar, V. Namitha, P. Naresh and S. Khaleelullah, "Machine Learning for Web Security: Strategies to Detect and Prevent Malicious Activities," 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), Coimbatore, India, 2024, pp. 59-64, doi: 10.1109/ICoICI62503.2024.10696229.

[37] Koushik Reddy Chaganti, Chinnala Balakrishna, P.Naresh, P.Rajyalakshmi, 2024, Navigating E-commerce Serendipity: Leveraging Innovator-Based Context Aware Collaborative Filtering for Product Recommendations, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 13, Issue 05 (May 2024).

[38] Naresh, P., Reddy, A. J., Kumar, S. P., Nikhil, C., & Chandu, T. (2024). Transfer Learning Based Kidney Stone Detection in Patients Using ResNet50 with Medical Images 47. In CRC Press eBooks (pp. 286–291). https://doi.org/10.1201/9781032665535-47.

[39] Liu, X., & Li, X. (2020). A Blockchain and Machine Learning-Based Framework for Secure Healthcare Data Sharing. International Journal of Distributed Sensor Networks, 16(5), 1550147720929513.