

Cyber Sentinel :AI & NLP-Powered Cybersecurity Against Malicious Links

¹MR.K.Premkumar, Professor

Computer Science and Engineering, St.Joseph College of Engineering, Chennai-602117,TamilNadu.

² Christopher.ST, UG Student

Computer Science and Engineering, St.Joseph College of Engineering, Chennai-602117, TamilNadu.

³Saranraj.M, UG Student

Computer Science and Engineering, St.Joseph College of Engineering, Chennai-602117, TamilNadu.

Abstract – Cyber Sentinel is an advanced AI-driven Chrome extension that leverages Gemini AI and NLP techniques to detect and prevent online scams in real time. It scans text from emails, messages, and web pages to identify malicious intent, ensuring proactive protection against cyber threats. The extension classifies visited URLs into categories such as phishing, malware, defacement, or benign, providing instant security alerts to users. With seamless integration, it delivers non-intrusive pop-ups and notifications to warn of potential risks without disrupting browsing. By analyzing linguistic patterns and URL structures, it enhances accuracy in threat detection. Designed for user-friendly interaction, it offers a smooth and efficient security solution. The tool adapts to evolving cyber threats, ensuring up-to-date defense mechanisms. Ultimately, Cyber Sentinel empowers users with real-time scam detection, significantly improving online safety.

Keywords:

Cybersecurity, AI-Powered Detection, NLP, Phishing Protection, Malware Prevention, Real-Time Alerts, Chrome Extension, Scam Detection

INTRODUCTION

In today's digital age, cyber threats such as phishing, malware, and scam links are becoming increasingly sophisticated, posing significant risks to individuals and organizations. Attackers exploit deceptive emails, fraudulent messages, and malicious websites to steal sensitive data, distribute malware, and compromise user security. Traditional security measures often fail to keep up with these evolving threats, leaving users vulnerable to cyberattacks. To address this critical challenge, we introduce Cyber Sentinel, an advanced AI and NLP-powered Chrome extension designed to provide real-time scam detection and URL threat classification.

Cyber Sentinel leverages Google's Gemini AI and Natural Language Processing (NLP) to analyze text from emails, chat messages, and web pages, detecting suspicious patterns indicative of scams. Unlike conventional security tools that rely solely on blacklisted URLs, our solution employs machine learning-based threat assessment, scanning links in real time and classifying them into categories such as benign, phishing, malware, or defacement. Users receive instant security alerts through non-intrusive pop-ups and notifications, enabling them to make informed decisions before interacting with potentially harmful content.

The extension offers a seamless and user-friendly experience, operating in the background without disrupting browsing activities. By combining AI-driven text analysis with real-time URL scanning,

Cyber Sentinel provides a proactive defense mechanism against cyber threats. Whether it's a phishing email, a fraudulent social media link, or a malware-infected website, our tool ensures that users are immediately warned, reducing the risk of falling victim to cybercrime.

With the rise of AI-generated scams and socially engineered attacks, the need for intelligent, adaptive cybersecurity solutions has never been greater. Cyber Sentinel bridges this gap by integrating cutting-edge AI, NLP, and real-time threat intelligence, making it an essential tool for individuals, businesses, and cybersecurity professionals. By deploying this extension, users can browse the internet with confidence, knowing that an AI-powered guardian is continuously working to detect, analyze, and block malicious links before they cause harm.

This project represents a significant step forward in AI-enhanced cybersecurity, offering a scalable, efficient, and user-centric approach to combating online fraud. Future developments may include multi-platform support, enhanced threat intelligence sharing, and deeper AI model fine-tuning to stay ahead of cybercriminals. Cyber Sentinel is not just a protective tool—it's a smart, evolving shield against the ever-growing landscape of digital threats.

BACKGROUND AND MOTIVATION

A. Overview

Cyber Sentinel represents a groundbreaking advancement in browser-based cybersecurity, leveraging cutting-edge artificial intelligence and natural language processing to combat the ever-evolving landscape of online threats. This innovative Chrome extension is specifically designed to address the critical security gap between traditional protection mechanisms and sophisticated modern cyber attacks.

At its core, Cyber Sentinel operates through a sophisticated multi-layered defense system that combines:

1. **Real-Time Content Analysis:** The extension continuously monitors and analyzes text content across emails, messaging platforms, and web pages using advanced NLP algorithms powered by Gemini AI. This enables detection of subtle social engineering tactics and scam patterns that conventional security tools often miss.
2. **Dynamic URL Threat Assessment:** Unlike static blacklist-based systems, Cyber Sentinel employs machine learning models to evaluate website URLs in real-time, classifying them into distinct threat categories (phishing, malware, defacement) with high accuracy, even for newly created malicious sites.
3. **Intelligent Alert System:** The solution features a context-aware notification framework that delivers timely, non-disruptive warnings with clear risk explanations, significantly improving user response rates compared to traditional security alerts.

The system architecture integrates seamlessly with the Chrome browser ecosystem, operating with minimal performance impact while providing maximum protection coverage. Key technical components include:

- A lightweight frontend interface for user interaction
- A powerful backend analysis engine utilizing transformer-based models
- Continuous learning mechanisms that adapt to emerging threat patterns
- Privacy-preserving data processing that maintains user confidentiality

What sets Cyber Sentinel apart is its unique combination of linguistic analysis and technical threat detection. While conventional tools focus solely on technical indicators, our solution understands the human element of cyber attacks - the psychological manipulation techniques employed in modern scams. This dual approach enables detection of sophisticated threats that bypass traditional security measures.

The extension is designed for universal accessibility, requiring no technical expertise from end users while offering enterprise-grade protection. Its adaptive AI models ensure ongoing effectiveness against evolving attack methodologies, making it a future-proof solution in the rapidly changing cybersecurity landscape.

By integrating advanced AI capabilities directly into the browsing experience, Cyber Sentinel establishes a new paradigm in proactive cyber defense - one that protects users before they interact with threats rather than responding after damage occurs. This shift from reactive to preventive security represents a significant leap forward in personal and organizational cyber protection.

B. Rising Cyber Threats in the Digital Age

The rapid growth of internet usage has led to an alarming increase in cyber threats, including phishing attacks, malware distribution, and social engineering scams. Cybercriminals constantly refine their tactics, using AI-generated deceptive emails, fraudulent messages, and malicious links to exploit unsuspecting users. According to recent reports, phishing attacks alone account for over 36% of data breaches, costing businesses billions annually. Traditional security solutions, such as blacklist-based URL filters and signature-dependent antivirus software, struggle to keep up with these evolving threats. Many users unknowingly interact with harmful content due to a lack of real-time, intelligent detection systems, highlighting the urgent need for AI-driven cybersecurity solutions.

C. Limitations of Existing Security Measures

Current cybersecurity tools face several challenges:

- **Reactive Rather Than Proactive:** Most solutions detect threats only after they are reported, leaving users vulnerable to zero-day attacks.

- **Over-Reliance on Static Blacklists:** Many systems depend on outdated URL databases, failing to recognize newly created malicious links.
- **Limited Contextual Understanding:** Traditional filters cannot analyze the linguistic patterns in emails or messages, making them ineffective against sophisticated social engineering scams.
- **User Awareness Gaps:** Even with warnings, many individuals ignore security alerts due to poorly designed or intrusive notifications.

These limitations underscore the necessity for an adaptive, AI-powered system that can analyze text, assess URLs in real time, and provide instant, user-friendly warnings—capabilities that Cyber Sentinel is designed to deliver.

D. The Need for AI-Powered Proactive Defense

To combat modern cyber threats effectively, a smarter, more dynamic approach is required. Artificial Intelligence (AI) and Natural Language Processing (NLP) offer unprecedented advantages:

- **Real-Time Threat Detection:** AI models can instantly analyze text and URLs, identifying scams before users interact with them.
- **Behavioral and Linguistic Analysis:** NLP helps detect manipulative language, urgency tactics, and fake sender identities commonly used in phishing.
- **Adaptive Learning:** Machine learning enables continuous improvement, allowing the system to recognize new attack patterns without manual updates.
- **Seamless User Experience:** AI-driven alerts can be context-aware and non-disruptive, ensuring security without hindering productivity.

Cyber Sentinel addresses these needs by integrating Gemini AI for scam detection, real-time URL classification, and intelligent alert systems. By bridging the gap between advanced cybersecurity and everyday usability, this project aims to reduce successful cyberattacks, enhance user awareness, and set a new standard for browser-based protection. The ultimate goal is to create a safer digital environment where users can browse, communicate, and transact without fear of falling victim to malicious schemes.

Motivation for This Research

Given the growing burden of heart diseases and the limitations of traditional diagnostic methods, there is an urgent need for an intelligent, automated, and real-time heart disease detection system. This research aims to:

- E. Develop a robust sensor-based monitoring system capable of collecting real-time cardiac data with minimal patient intervention.

- F. Enhance signal quality through feature extraction techniques that improve classification accuracy.
- G. Leverage Artificial Neural Networks (ANNs) to process and classify cardiac signals efficiently, reducing false positives and false negatives.
- H. Enable remote and continuous monitoring to support early diagnosis and preventive healthcare solutions.
- I. By integrating sensor technology, AI-driven analytics, and real-time monitoring capabilities, this study seeks to contribute to the advancement of smart healthcare systems, ultimately reducing CVD-related morbidity and mortality rates.

NOVEL APPLICATIONS OF SENSORBASED HEART DISEASE DETECTION

The integration of sensor technology with Artificial Neural Networks (ANNs) introduces a novel approach to real-time heart disease detection. Traditional diagnostic methods rely on periodic clinical assessments, which may delay the identification of early cardiac abnormalities. In contrast, this research leverages continuous physiological data collection through biosensors, including electrocardiography (ECG), photoplethysmography (PPG), heart rate variability (HRV), and blood pressure monitoring. The combination of these signals enhances diagnostic precision by overcoming the limitations of single-sensor analysis and providing a more comprehensive evaluation of cardiovascular health.

Feature extraction plays a critical role in transforming raw sensor data into diagnostically relevant parameters. The proposed system utilizes advanced time-domain, frequency-domain, and statistical feature extraction techniques to identify key cardiac markers. Unlike conventional methods that rely on fixed thresholds, the ANN model dynamically learns patient-specific variations in heart rate, ECG morphology, and RR interval fluctuations. This personalized approach improves classification accuracy by reducing false positives and false negatives, ensuring reliable detection of subtle cardiac abnormalities.

The use of ANNs further enhances the system's ability to recognize complex, nonlinear patterns within physiological signals. Unlike traditional classifiers such as Support Vector Machines (SVMs) or Decision Trees, deep learning-based ANN models adaptively refine their decision-making process through continuous learning. By training on large datasets, the model identifies subtle variations indicative of early-stage cardiovascular diseases, leading to higher sensitivity and specificity in classification. The incorporation of edge computing further enables real-time processing, ensuring rapid diagnosis and immediate alerts for patients and healthcare providers.

ROLE AND POTENTIAL OF SENSOR BASED HEART DISEASE DETECTION

I. Role of Sensors in Heart Disease Detection

Sensor-based heart disease detection relies on various physiological parameters to identify abnormalities and potential risks.

A. Continuous Monitoring

Wearable and implantable sensors facilitate 24/7 tracking of heart activity, enabling early diagnosis of arrhythmia, hypertension, and myocardial infarction.

B. Remote Health Monitoring

With IoT integration, sensor-based devices transmit patient data to health care providers, minimizing the need for hospital visits and enabling timely medical interventions [2].

C. Multi-Parameter Analysis

Modern sensors measure multiple physiological parameters, including:

Electrocardiogram (ECG): Monitors heart rhythm and electrical activity.

Photoplethysmography (PPG): Detects blood flow variations.

Blood Pressure Sensors: Measure arterial pressure

fluctuations. Oxygen Saturation (SpO₂): Monitor oxygen levels in the bloodstream.

Temperature Sensors: Identify fever and inflammation-related cardiac issues.

D. AI and Machine Learning Integration

Machine learning algorithms process sensor data to detect abnormal patterns and predict cardiovascular risks [3]. AI-driven diagnostic systems enhance accuracy, reducing false positives and improving detection efficiency.

II. Potential and Future Directions

A. Wearable and Implantable Technology

The miniaturization of sensors allows their integration into smartwatches, fitness bands, and implantable devices for non-invasive, continuous monitoring [4].

B. AI-Enhanced Early Prediction

Deep learning models improve predictive capabilities, facilitating early-stage disease detection and personalized healthcare strategies.

C. Smart Healthcare Ecosystem

Integration with cloud computing and electronic health records (EHRs) streamlines remote diagnostics and treatment planning [5].

D. Cost-Effective and Scalable Solutions

Sensor technology reduces healthcare costs by minimizing hospital admissions, promoting home-based monitoring, and enabling large-scale screening programs

CONCLUSION

Cyber Sentinel revolutionizes cybersecurity with AI-powered real-time protection against evolving online threats. This innovative Chrome extension combines NLP and machine learning to detect phishing, malware, and scams in emails, messages, and URLs. Unlike traditional tools, it

proactively analyzes content and links using advanced algorithms, providing accurate threat classification. The solution features intelligent, non-intrusive alerts that enhance user awareness without disrupting browsing. Its adaptive learning system continuously improves detection capabilities against new attack patterns. Designed for seamless integration, it offers enterprise-grade security with minimal performance impact. Cyber Sentinel bridges the gap between sophisticated protection and user-friendly experience, making advanced security accessible to all. This represents a significant advancement in preventive cybersecurity for safer digital navigation.

FUTURE RESEARCH DIRECTIONS FOR ENHANCED EDUCATION

J. Future Research Directions

- Energy-Efficient and Self-Powered Sensors
 1. Continuous monitoring requires high energy consumption, necessitating frequent battery replacements.
 2. Future research should focus on energy-harvesting technologies, such as piezoelectric or bioenergy-based sensors, to develop self-powered wearable devices [7].
- Advanced AI and Predictive Analytics
 1. Current AI models can detect heart abnormalities, but future research should emphasize predictive models capable of forecasting potential heart diseases before symptoms appear.
 2. The integration of deep learning and federated learning can improve diagnostic accuracy and enhance personalized healthcare [8]
- Secure and Privacy-Preserving Data Transmission
 1. With the increasing use of cloud-based cardiac monitoring, security risks such as cyberattacks and data breaches must be addressed.
 2. Research should explore blockchain-based security frameworks and homomorphic encryption for secure data storage and sharing [9].
- Integration with Smart Cities and IoT Healthcare Ecosystems
 1. Future research should explore large-scale deployment of sensor-based heart monitoring within smart city infrastructure to improve emergency response and public health surveillance.

K. Enhanced Education and Training

To fully utilize sensor-based heart disease detection technologies, the education and training of healthcare professionals, engineers, and researchers must be improved.

- Interdisciplinary Medical-Engineering Education
 1. Universities should introduce interdisciplinary courses combining biomedical engineering, AI, and cardiology to prepare professionals for the future of digital healthcare [10].
 2. Hands-on training programs for medical practitioners in wearable sensor technology should be developed.
- AI and Big Data Training for Clinicians
 1. Medical professionals must be trained to interpret AI-generated diagnostics and leverage big data for informed decision-making.

2. Institutions should integrate AI and machine learning courses into medical curricula to bridge the gap between technology and healthcare.
- Public Awareness and Patient Education
 1. Patients need education on using wearable devices effectively and interpreting basic health insights from sensor data.
 2. Public health campaigns should promote awareness about early detection of heart disease using wearable technology.
 - Standardization and Certification Programs
 1. Establishing standardized protocols and certification programs for sensor-based cardiac monitoring will ensure reliability and regulatory compliance.
 2. Collaboration between medical boards, IEEE, and healthcare institutions can facilitate universal standards for sensor-based diagnostics.

REFERENCES:

- [1] M.M. R. Khan Mamun and T. Elfouly, "Detection of cardiovascular disease from clinical parameters using a one-dimensional convolutional neural network," *Bioengineering*, vol. 10, no. 7, p. 796, Jul. 2023, doi: 10.3390/bioengineering10070796.
- [2] M. M. Ahsan and Z. Siddique, "Machine learning-based heart disease diagnosis: A systematic literature review," *Artif. Intell. Med.*, vol. 128, Jun. 2022, Art. no. 102289, doi: 10.1016/j.artmed.2022.102289.
- [3] A. B. Naeem, B. Senapati, A. S. Chauhan, S. Kumar, J. C. O. Gavilan, and W. M. F. Abdel-Rehim, "Deep learning models for cotton leaf disease detection with VGG-16," *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 2, pp. 550–556, 2023. [Online]. Available: <https://www.ijisae.org/index.php/IJISAE/article/view/2710>
- [4] A. Albahr, M. Albahr, M. Thanoon, and M. Binsawad, "Computational learning model for prediction of heart disease using machine learning based on a new regularizer," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–10, Nov. 2021, doi: 10.1155/2021/8628335.
- [5] A.B.Naeem,B.Senapati,A.S.Chauhan,M.Makhija,A.Singh,M.Gupta,P.K.Tiwari,andW.M.F.Abdel-Rehim,"Hypothyroidismdiseasediagnosisbyusingmachinelearningalgorithms,"*Int.J.*

- Intell. Syst. Appl. Eng., vol. 11, no. 3, pp. 368–373, 2023. [Online]. Available: <https://www.ijisae.org/index.php/IJISAE/article/view/3178>
- [6] I. M. El-Hasnony, O. M. Elzeki, A. Alshehri, and H. Salem, “Multi-label active learning-based machine learning model for heart disease prediction,” *Sensors*, vol. 22, no. 3, p. 1184, Feb. 2022, doi: 10.3390/s22031184.
- [7] G. G. N. Geweid and M. A. Abdallah, “A new automatic identification method of heart failure using improved support vector machine based on duality optimization technique,” *IEEE Access*, vol. 7, pp. 149595–149611, 2019.
- [8] A. Haldorai and A. Ramu, “Security and channel noise management in cognitive radio networks,” *Comput. Electr. Eng.*, vol. 87, Oct. 2020, Art. no. 106784, doi: 10.1016/j.compeleceng.2020.106784.
- [9] M. I. Hossain, M. H. Maruf, M. A. R. Khan, F. S. Prity, S. Fatema, M. S. Ejaz, and M. A. S. Khan, “Heart disease prediction using distinct artificial intelligence techniques: Performance analysis and comparison,” *Iran.J.Comput.Sci.*, vol. 6, pp. 397–417, Jun. 2023, doi: 10.1007/s42044-023-00148-7.
- [10] A. B. Naeem, A. M. Soomro, H. M. Saim, and H. Malik, “Smart road management system for prioritized autonomous vehicles under vehicle-to-everything (V2X) communication,” *Multimedia Tools Appl.*, pp. 1–18, Oct. 2023, doi: 10.1007/s11042-023-16950-1.
- [11] A. Ishaq, S. Sadiq, M. Umer, S. Ullah, S. Mirjalili, V. Rupapara, and M. Nappi, “Improving the prediction of heart failure patients’ survival using SMOTE and effective data mining techniques,” *IEEE Access*, vol. 9, pp. 39707–39716, 2021, doi: 10.1109/ACCESS.2021.3064084.
- [12] N. Karthikeyan, P. Padmanaban, A. Prasanth, and D. Ragnath, “Machine learning based classification models for heart disease prediction,” *J. Phys., Conf.*, vol. 1916, no. 1, May 2021, Art. no. 012092, doi: 10.1088/1742-6596/1916/1/012092.
- [13] M. A. Naser, A. A. Majeed, M. Alsabah, T. R. Al-Shaikhli, and K. M. Kaky, “A review of machine learning’s role in cardiovascular disease prediction: Recent advances and future challenges,” *Algorithms*, vol. 17, no. 2, p. 78, 2024, doi: 10.3390/a17020078.
- [14] A. B. Naeem, F. Khalid, A. M. Soomro, A. D. DelMundo, A. Zaidi, B. Senapati, and O. P. Doshi, “Early gender identification of date palm using machine learning,” *J. Comput. Biomed. Inform.*, vol. 4, no. 2, pp. 128–141, 2023. [Online]. Available: <https://www.jcabi.org/index.php/Main/article/view/147>
- [15] N. Louridi, S. Douzi, and B. ElOuahidi, “Machine learning-based identification of patients with a cardiovascular defect,” *J. BigData*, vol. 8, no. 1, p. 133, Dec. 2021, doi: 10.1186/s40537-021-00524-9.
- [16] S. Abbas, S. Ojo, A. Al Hejaili, G. A. Sampedro, A. Almadhor, M. M. Zaidi, and N. Kryvinska, “Artificial intelligence framework for heart disease classification from audio signals,” *Sci. Rep.*, vol. 14, no. 1, p. 3123, Feb. 2024, doi: 10.1038/s41598-024-53778-7.
- [17] E. Maini, B. Venkateswarlu, B. Maini, and D. Marwaha, “Machine learning-based heart disease prediction system for Indian population: An exploratory study done in South India,” *Med. J. Armed Forces India*, vol. 77, no. 3, pp. 302–311, Jul. 2021, doi: 10.1016/j.mjafi.2020.10.013.
- [18] A. M. Soomro, A. B. Naeem, K. Shahzad, A. M. Madni, A. D. D. Mundo, M. Sajid, and M. A. Baloch, “Forecasting cotton whitefly population using deep learning,” *J. Comput. Biomed. Informat.*, vol. 4, no. 1, pp. 64–76, Dec. 2022, doi: 10.56979/401/2022/67.
- [19] A. B. Naeem, A. M. Soomro, A. Bhuvu, K. Bashir, D. Bhuvu, R. R. Maaliw, and W. M. F. Abdel-Rehim, “Intelligent four-way crossroad safety management for autonomous, non-autonomous and VIP vehicles,” in *Proc. IEEE Int. Conf. Emerg. Trends Eng., Sci. Technol.*, Jan. 2023, pp. 1–6, doi: 10.1109/icest56843.2023.10138829.
- [20] K. M. Mohi Uddin, R. Ripa, N. Yeasmin, N. Biswas, and S. K. Dey, “Machine learning-based approach to the diagnosis of cardiovascular vascular disease using a combined dataset,” *Intell.-Based Med.*, vol. 7, 2023, Art. no. 100100, doi: 10.1016/j.ibmed.2023.100100.
- [21] A. B. Naeem, B. Senapati, M. S. Islam Sudman, K. Bashir, and A. E. M. Ahmed, “Intelligent road management system for autonomous, non-autonomous, and VIP vehicles,” *World Electric Vehicle J.*, vol. 14, no. 9, p. 238, Sep. 2023, doi: 10.3390/wevj14090238.

- [22] R. G. Nadakinamani, A. Reyana, S. Kautish, A. S. Vibith, Y. Gupta, S. F. Abdelwahab, and A. W. Mohamed, "Clinical data analysis for prediction of cardiovascular disease using machine learning techniques," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–13, Jan. 2022, doi: 10.1155/2022/2973324.
- [23] U. Nagavelli, D. Samanta, and P. Chakraborty, "Machine learning technology-based heart disease detection models," *J. Healthcare Eng.*, vol. 2022, pp. 1–9, Feb. 2022, doi: 10.1155/2022/7351061.
- [24] A. M. Soomro, A. B. Naeem, B. Senapati, K. Bashir, S. Pradhan, R. R. Maaliw, and H. A. Sakr, "Constructor development: Predicting object communication errors," in *Proc. IEEE Int. Conf. Emerg. Trends Eng., Sci. Technol.*, Bahawalpur, Pakistan, Jan. 2023, pp. 1–7.
- [25] A. Rahim, Y. Rasheed, F. Azam, M. W. Anwar, M. A. Rahim, and A. W. Muzaffar, "An integrated machine learning framework for effective prediction of cardiovascular diseases," *IEEE Access*, vol. 9, pp. 106575–106588, 2021, doi: 10.1109/ACCESS.2021.3098688.
- [26] A. B. Naeem, B. Senapati, G. A. L. Mahadin, V. Ghulaxe, F. Almeida, S. I. Sudman, and M. I. Ghafoor, "Determine the prevalence of hepatitis B and C during pregnancy by using machine learning algorithm," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 13, pp. 744–751, 2024. [Online]. Available: <https://www.ijisae.org/index.php/IJISAE/article/view/4704>
- [27] A. Saboor, M. Usman, S. Ali, A. Samad, M. F. Abrar, and N. Ullah, "A method for improving prediction of human heart disease using machine learning algorithms," *Mobile Inf. Syst.*, vol. 2022, pp. 1–9, Mar. 2022, doi: 10.1155/2022/1410169.
- [28] J. Talukdar and T. P. Singh, "Early prediction of cardiovascular disease using artificial neural network," *J. Paladyn Behav. Robot.*, vol. 14, no. 1, Feb. 2023, Art. no. 20220107, doi: 10.1515/pjbr-2022-0107.
- [29] R. Tr, U. K. Lilhore, S. Simaiya, A. Kaur, and M. Hamdi, "Predictive analysis of heart diseases with machine learning approaches," *Malaysian J. Comput. Sci.*, pp. 132–148, Mar. 2022, doi: 10.22452/mjcs.sp2022no1.10
- [30] S. Tuli, N. Basumatary, S. S. Gill, M. Kahani, R. C. Arya, G. S. Wander, and R. Buyya, "HealthFog: An ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments," *Future Gener. Comput. Syst.*, vol. 104, pp. 187–200, Mar. 2020, doi: 10.1016/j.future.2019.10.043.
- [31] L. Zhu, J. Shen, L. Xie, and Z. Cheng, "Unsupervised topic hypergraph hashing for efficient mobile image retrieval," *IEEE Trans. Cybern.*, vol. 47, no. 11, pp. 3941–3954, Nov. 2017.
- [32] A. Sharma and P. K. Mishra, "Performance analysis of machine learning based optimized feature selection approaches for breast cancer diagnosis," *Int. J. Inf. Technol.*, vol. 14, no. 4, pp. 1949–1960, Jun. 2022, doi: 10.1007/s41870-021-00671-5.