ISSN 2347 - 3983
Volume 12. No.1, January 2024
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter011212024.pdf
https://doi.org/10.30534/ijeter/2024/011212024

Securing the Dynamic Realm: A Comprehensive Review of ML Algorithms in IoT-Based Home Automation Systems and Beyond

Salmanul Fharis P A[1], Sahana G S[2], Sakshi T U[3], Rasi K S[4]
[1]Alva's institute of engineering and technology, India, 4al20cs123@gmail.com
[2] Alva's institute of engineering and technology, India, 4al20cs121@gmail.com
[3] Alva's institute of engineering and technology, India, 4al20cs122@gmail.com
[4] Alva's institute of engineering and technology, India, 4al20cs114@gmail.com

Received Date: November 22, 2023 Accepted Date: December 16, 2023 Published Date : January 07, 2024

ABSTRACT

This paper comprehensively reviews the imperative for secure IoT systems, emphasizing the challenges posed by their dynamic nature. Exploring various ML algorithms for IoT security, it highlights their advantages while addressing common limitations, including computational overhead and privacy risks. The focus narrows to federated learning (FL) and deep learning (DL) algorithms, showcasing their potential to overcome conventional ML drawbacks by preserving data privacy. The study provides an in-depth analysis of FL and DL-based techniques, emphasizing their efficiency in enhancing security in IoT-based home automation systems. The paper further examines ML's pivotal role in smart homes, presenting a case study that utilizes the support vector machine algorithm to distinguish between regular occupants and intruders. Extending the discussion to face recognition for home automation, the review underscores the utilization of IoT and smart techniques. Beyond home automation, the paper delves into the broader landscape of ML applications in the Fourth Industrial Revolution, offering insights into cybersecurity, smart cities, healthcare, and more. The review briefly introduces the utilization of Convolutional Neural Networks (CNNs) within the broader context of deep learning algorithms. While the main emphasis remains on FL and DL, the paper acknowledges CNNs as a powerful tool for image-based tasks, especially relevant in the context of visual data analysis for security in IoT-based home automation systems. In summary, this concise review encapsulates the transformative impact of ML on IoT-based home automation security, providing valuable perspectives on current trends, challenges, and future research directions. The inclusion of CNNs within the abstract recognizes their relevance, especially in image-based security applications.

Key words: IoT Security, Machine Learning (ML) Algorithms, Home Automation Systems, Federated Learning (FL), Deep Learning (DL), Privacy Preservation, Support Vector Machine, Convolutional Neural Networks (CNNs).

1. INTRODUCTION

In an era characterized by the rapid expansion of the Internet of Things (IoT), the prospect of a connected world is becoming increasingly tangible. Gartner's projections indicate a substantial surge in connected devices, estimating a count of 20.4 billion by 2022 [1]. This surge extends to various global regions, emphasizing the transformative potential of IoT, particularly in Western Europe, North America, and China [1]. Notably, this surge encompasses a spectrum of applications, from smart cities to grids, retail, and farming, marking IoT as a pivotal contributor to the burgeoning digital economy [1].

Within this context, the smart home paradigm emerges as a focal point, where IoT applications intersect with daily living. The imperative for secure and reliable home automation systems is underscored by the increasing prevalence of threats, emphasizing the need for intelligent solutions [18]. As the number of IoT applications is poised to reach 20.4 billion by 2022 [6], the integration of machine learning (ML) algorithms becomes paramount to fortify security and enhance reliability within home automation systems.

Machine learning, with its ability to extract insights and patterns from vast datasets, stands out as a solution to the security challenges posed by the dynamic and heterogeneous nature of IoT devices [6]. As articulated in [4], smart home automation systems play a pivotal role in ensuring safety, security, and convenience. This paper extends this narrative by focusing on the integration of ML algorithms within IoT-based home automation systems, specifically designed to achieve heightened security and reliability.

As virtual assistants become integral to our daily lives, the intersection of machine learning and home automation gains significance [5]. This paper, building on the groundwork laid by [5], delves into the specific application of ML algorithms in detecting human facial expressions. This application holds promise for improving user experience and ensuring the security of smart homes. Through this exploration, the paper seeks to provide a nuanced understanding of how ML

algorithms can be implemented to fortify security and enhance reliability within IoT-based home automation systems.

In addressing the security concerns associated with IoT, particularly in home automation, the paper draws inspiration from the transformative potential of AI-based techniques [6]. As the number of IoT applications continues to grow, reaching approximately 20.4 billion by 2022 [6], the need for robust security models becomes imperative. This paper positions machine learning, and by extension, deep learning, as a solution to the identified challenges, aiming to implement intelligent algorithms that can discern and predict a range of cyber threats at an early stage [6].

In summary, this paper stands at the intersection of the burgeoning IoT landscape and the transformative capabilities of machine learning algorithms. By focusing on the specific context of home automation, the aim is to implement ML algorithms that not only fortify security but also enhance the reliability of IoT-based home automation systems [19]. Through careful consideration of the cited works, this paper seeks to contribute to the discourse on the integration of machine learning for achieving heightened security and reliability in the context of smart homes and IoT applications.

2. FOUNDATIONS OF MACHINE LEARNING IN IOT SECURITY

2.1 Introduction to Machine Learning in Security

Machine Learning (ML) revolutionizes security by empowering systems to learn from data and autonomously identify patterns. In the realm of IoT-based home automation, ML offers a dynamic approach to counter evolving threats. Federated Learning (FL) [7] ensures privacy in decentralized systems, enabling collaborative learning without compromising sensitive data. Deep Learning (DL) [6] utilizes neural networks to discern complex patterns, making it instrumental in image recognition for bolstering smart home security. This section lays the foundation for exploring how ML, FL, and DL collectively contribute to enhancing security and reliability in IoT-based home automation within the subsequent discussion.

2.2 Types of Machine Learning Models

Machine learning encompasses diverse models, each tailored for specific tasks within IoT-based home automation security.

1.Supervised Learning:

In supervised learning, models are trained on labelled datasets, learning to map input data to corresponding output labels. This approach is instrumental for tasks like intrusion detection, where the system learns from historical data to identify known security threats.

2. Unsupervised Learning:

Unsupervised learning involves training models on unlabeled data, allowing them to identify patterns and structures independently. This type is crucial for anomaly detection in smart homes, where deviations from normal behavior signify potential security risks.

3.Reinforcement Learning:

Reinforcement learning employs a reward-based system, where models learn through interactions with the environment. This is relevant for optimizing security protocols in IoT devices, where systems adapt based on feedback and outcomes.

4. Federated Learning:

Federated learning is well-suited for decentralized IoT systems. It enables collaborative learning across devices without sharing raw data, ensuring privacy. This is vital for smart homes where user data is sensitive, and maintaining privacy is a priority.

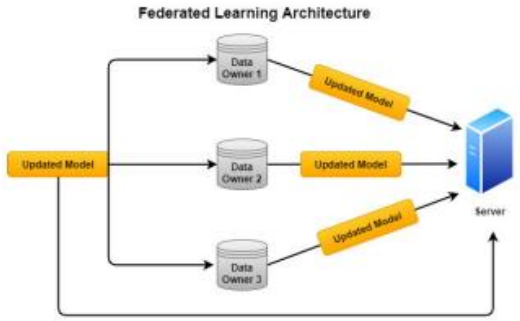

Figure 1: General federated learning architecture

In Figure 1, the federated learning architecture for decentralized IoT systems is depicted. The 'uploaded model' initiates collaborative learning without sharing raw data. Three connections link to 'Data owner 1,' 'Data owner 2,' and 'Data owner 3,' emphasizing decentralized data ownership in smart homes. Converging at the 'server,' the updated models maintain privacy, ensuring secure and user-centric smart home environments.

5. Deep Learning:

Deep learning, a subset of machine learning, involves neural networks with multiple layers which tries to copy human brain function through algorithms [20]. Ideal for tasks requiring complex pattern recognition, such as image and speech processing [11], it holds promise for enhancing security in smart homes through advanced threat detection.

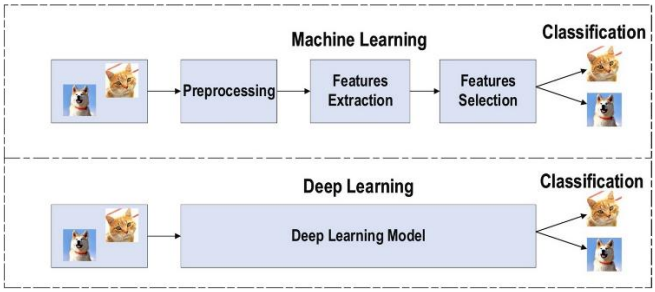

Figure 2: Deep Learning and traditional Machine learning

In the Machine Learning section (Figure 3), a visual representation (cat and dog) undergoes 'processing,' 'feature extraction,' and 'feature selection' stages, culminating in the classification of two images differently. In the Deep Learning section, represented in Figure 3 as well, the process involves a 'Deep Learning model' directly leading to the classification of two images differently. This visual framework emphasizes the intricate layers and capabilities of deep learning, showcasing its potential for advanced threat detection in smart homes. Understanding these machine learning models serves as a crucial foundation for tailoring security solutions to address the specific challenges inherent in IoT-based home automation systems [11].

Understanding the nuances of these machine learning models provides a foundation for tailoring security solutions to the specific challenges presented by IoT-based home automation systems.

3. FOUNDATIONS OF MACHINE LEARNING IN IOT SECURITY

The provided text discusses various applications of Federated Learning (FL) and Deep Learning (DL)[2] in different domains. Here is a summarized version:

1. Financial, Sales, and Industry Applications:

- FL is promising in industries where data cannot be aggregated due to factors like data security, privacy protection, and intellectual property rights [9].
- Customized services, such as product recommendations and sales assistance, benefit from FL methods in scenarios where user data is distributed among different entities [9].

2. Healthcare Applications:

- FL addresses challenges in smart healthcare by enabling collaboration and sharing of medical datasets among different institutions, thereby enhancing the performance of machine learning models [9].
- Federated Transfer Learning, combined with FL, helps fill gaps in medical data and improves the efficiency of machine learning algorithms [9].

3. Wireless Communication:

- FL demonstrates its reliability and security in wireless communication, offering advantages in edge computing and 5G networks [8].
- Light wave power-based FL models and hierarchical FL systems contribute to optimizing transmission efficiency in wireless networks [8].

4. Service Recommendation:

- FL is applied to service recommendation, as seen in the Google keyboard project [9].
- Intelligent medical diagnosis systems benefit from FL, especially in collecting and analyzing health data while maintaining patient confidentiality [9].

5. Healthcare Applications:

- FL in healthcare involves classification tasks for various medical conditions, including COVID-19 detection, cancer diagnoses, and autism spectrum disorder [9].
- Predictive modelling, phenotyping, and patient representation learning are explored in the context of FL in healthcare [8].

7. Self-Driving Cars:

- Deep Learning plays a crucial role in bringing autonomous driving to life by handling unprecedented scenarios and enabling safe navigation through traffic [10].
- Data from cameras, sensors, and geo-mapping contribute to creating sophisticated models for self-driving cars [10].

10. Fraud Detection in Banking:

- Deep Learning aids in fraud detection in the banking sector by identifying patterns in customer transactions and credit scores [10].

11. Personalization:

- E-commerce giants use Deep Learning to provide personalized experiences through product recommendations, personalized packages, and targeted discounts [10].
- Chatbots powered by Deep Learning contribute to personalized experiences on various platforms [10].

This summary provides an overview of the diverse applications of FL and DL across different sectors, showcasing their significance in addressing challenges and optimizing various processes.

4. FOUNDATIONS OF MACHINE LEARNING IN IOT SECURITY

4.1 IoT Security Threats and Challenges [12]

1. Identification of Threats:
   - Cloning, substitution, and firmware attacks pose threats to IoT devices [2].
   - Privacy issues, denial-of-service, and eavesdropping vulnerabilities exist.
2. Key Challenges:
   - Device identity concerns, firmware updating challenges, and authentication issues.
   - Management complexities, implementation of security algorithms, and communication security challenges.

4.2 Detailed Threats and Security Measures [13]

1. IoT Authentication and Access Control:
   - Spoofing and intrusion threats addressed through authentication and access control.
   - DoS attacks and malware risks mitigated for secure IoT operations[3].
2. Secure IoT Offloading:
   - Measures against DoS, jamming, and man-in-the-middle attacks during IoT offloading.
3. IoT Malware Detection:
   - Protection against malware for preventing privacy leakage and network performance issues [2].

4.3 Connectivity Problems in IoT Systems [6]

Solutions proposed for IoT connectivity issues:

1. Unique IPs using IPv6.
2. Development of low-power communication for efficient information transmission.

4.4 Security Challenges in IoT Devices [6]

- Analysis of security challenges in IoT devices in both cyber and physical environments.
- Categorization of threats into active (e.g., Sybil attacks)[3] and passive (e.g., eavesdropping) threats.

Some of the prominent Security Properties are Confidentiality, integrity, authentication, authorization, availability, and non-repudiation.

4.5 Security Critical IoT Applications [1]

1. Smart Cities:
   - Use of computation and communication for smart living.
   - Privacy concerns in smart card services and mobility applications.
2. Smart Environment:
   - Monitoring environmental factors with risks of false negatives and positives[3].
3. Smart Metering and Smart Grids:
   - Vulnerabilities in smart metering systems, susceptible to physical and cyber-attacks.
4. Security and Emergencies:
   - Deployment of IoT for security with consequences for false alarms and breaches.
5. Smart Retail:
   - Extensive IoT use in retail with risks of compromise, data theft, and financial losses.
6. Smart Agriculture and Animal Farming:
   - Monitoring soil, climate, and livestock with risks associated with compromised applications.

This concise summary provides an overview of the identified threats, challenges, and security measures in the IoT landscape, with appropriate citations.

5. FOUNDATIONS OF MACHINE LEARNING IN IOT SECURITY

5.1 Unveiling Convolutional Neural Networks

Convolutional Neural Networks (CNNs), recognized for their prowess in image analysis, emerge as a crucial component in the endeavor to secure IoT-based home automation systems [14]. In the dynamic realm of IoT, where security concerns are paramount, the specialized architecture of CNNs aligns seamlessly with the unique data types associated with home automation, particularly visual data.

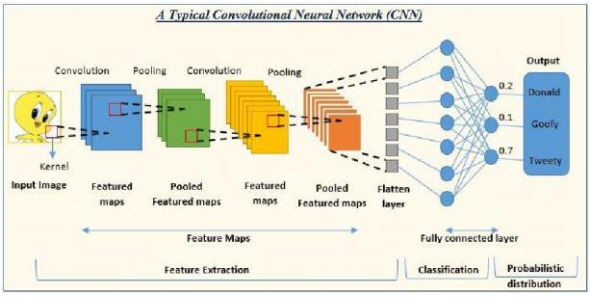

Figure 3: A Typical CNN

The figure 3 as elucidated, a typical Convolutional Neural Network (CNN) comprises essential layers—convolutional,

pooling, and fully connected layers—each playing a distinct role in the extraction, abstraction, and classification of features from images. In the context of home automation security, this structured approach proves invaluable. Moreover, the effectiveness of machine learning (ML) algorithms is intricately tied to the integrity of the input-data representation [16]. Extensive research has demonstrated that a well-crafted data representation significantly enhances performance compared to a suboptimal one. Feature engineering, a cornerstone in ML research for many years, involves constructing features from raw data. This process is inherently field-specific and often demands substantial human effort. Notably, in the realm of computer vision, various types of features, such as histogram of oriented gradients (HOG) [15], scale-invariant feature transform (SIFT) [16], and bag of words (BoW) [17], have been introduced and compared. The introduction of a novel feature that proves effective typically marks the inception of a new research direction pursued over multiple decades.

Furthermore, unlike traditional ML approaches, Deep Learning (DL)-based AI methods automatically extract features, eliminating the need for manual feature extraction [17]. DL algorithms, particularly Convolutional Neural Networks (CNNs), excel in automatically extracting features due to their deep architecture. This has proven particularly effective in applications such as structural health monitoring (SHM), where DL techniques enable the extraction of pertinent data from noisy measurement databases with damage signatures, without requiring predefined classifiers [17]. The extensive use of CNNs in infrastructure monitoring literature reflects their effectiveness in structural condition assessment.

1. Convolutional Layer for Feature Extraction:

In the context of securing home automation systems, the convolutional layer stands as the vanguard, extracting meaningful features from visual data captured by surveillance cameras or other imaging devices. By performing convolutions with specialized filters, CNNs discern intricate patterns crucial for security protocols.

2. Pooling Layer for Dimensionality Reduction:

The subsequent pooling layer optimizes the processing of visual data by down-sampling, reducing computational complexity while retaining salient information. This step aligns with the need for efficient analysis in resource-constrained IoT environments.

3. Fully Connected Layers for Classification:

The fully connected layers, akin to standard artificial neural networks, refine the extracted features and produce class scores relevant to security classifications. In the context of home automation, these classifications could include normal activities, potential intrusions, or other security-relevant events.

Algorithm summarized for reducing the cost function: [14]

Step 1: Give the network an input vector.
Step 2: Convolution with a filter is used to create a feature map.
Step 3: Run ReLU on the resulting feature map to add non-linearity.
Step 4: Utilize the pooling method to add translation invariance to the feature map that has been produced.
Step 5: To repeat the layers, repeat Steps 2 through 4.
Step 6: The fully linked layer receives the acquired feature maps and uses them for categorization.
Step 7: Send the result to a classifier like SoftMax.
Step 8: Compute the gradient with respect to all the learnable parameters and account for computer loss at the last layer.
Step 9: Update the parameters and backpropagate the error component.
Step10: Until the network converges, execute the forward pass and repeat Steps 2 through 9 with the modified settings.

The summarized algorithm for minimizing the cost function outlines a comprehensive process for integrating CNNs into the security framework of IoT-based home automation systems. Starting from input provision to the network, through convolution, non-linearity introduction, pooling, and classification, the algorithm encapsulates the core functionalities.

5.2 Integration with Home Automation Security

In the specific context of home automation security, CNNs can be applied to analyze visual data from surveillance cameras, identify known individuals through facial recognition, and detect anomalies indicative of potential security threats. The step-wise algorithm aligns with the need for real-time, efficient processing in home automation scenarios.

To further fortify security measures, privacy-preserving techniques can be integrated into the CNN architecture. Techniques such as federated learning or edge computing can be explored to address concerns related to the storage and processing of sensitive visual data.

In summary, the application of CNNs in IoT-based home automation systems offers a robust solution to enhance security measures. The structured approach of CNNs, as outlined in the algorithm, provides a systematic and efficient framework for addressing security challenges in the dynamic IoT landscape.

6. CONCLUSION

In summary, this comprehensive review underscores the critical intersection between machine learning (ML) algorithms and Internet of Things (IoT)-based home

automation systems, emphasizing the imperatives of security and reliability in the dynamic IoT landscape. As Gartner projects a surge in connected devices, estimating 20.4 billion by 2022, the transformative potential of IoT becomes evident across various domains, with a specific focus on securing smart homes. Federated Learning (FL) and Deep Learning (DL) algorithms, notably Convolutional Neural Networks (CNNs), stand out as indispensable tools in mitigating challenges posed by the dynamic and heterogeneous nature of IoT devices. FL ensures privacy in decentralized systems, crucial for safeguarding sensitive user data in smart homes, while DL, facilitated by CNNs, proves instrumental in image-based security applications, essential for robust visual data analysis in home automation systems.

Looking ahead, future enhancements in this field could explore the integration of edge computing with ML algorithms to address concerns related to latency and bandwidth in IoT applications. The synergy between edge computing and ML holds promises for localized processing, optimizing response times in real-time applications crucial for home automation security. Additionally, advancements in explainable AI (XAI) could be seamlessly incorporated to enhance the transparency and interpretability of ML models. This becomes particularly crucial in critical applications such as healthcare and finance, where clear understanding and trust in AI-driven decisions are paramount.
Further research avenues could delve into the development of lightweight ML models suitable for resource-constrained IoT devices. Striking a balance between performance and energy efficiency is essential to ensure the seamless integration of ML algorithms into diverse IoT ecosystems. Moreover, the exploration of blockchain technology to enhance the security of FL in decentralized IoT systems presents a compelling avenue for future investigation. By leveraging the inherent security features of blockchain, researchers can contribute to the fortification of FL, ensuring the integrity and privacy of data exchanges in IoT environments.

In conclusion, by addressing these evolving challenges and exploring innovative avenues, researchers can contribute to the continual evolution and improvement of ML-based security solutions for IoT-based home automation systems and beyond. The dynamic nature of IoT demands adaptive and forward-thinking approaches to ensure the continued success and safety of connected ecosystems.

ACKNOWLEDGEMENT

We express our sincere gratitude to Dr. G. Srinivasan for his invaluable mentorship, which greatly contributed to the development of this review paper. We also appreciate the authors and researchers whose referenced works have enriched the content, reflecting the collaborative spirit within the academic community.

REFERENCES

1. Vikas Hassija, Vinay Chamola , Vikas Saxena , Divyansh Jain , Pranav Goyal and Biplab Sikdar. **A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures**, IEEE *Access*, March 2019.
2. Fan Liang, William G. Hatcher, Weixian Liao, Weichao Gao and Wei Yu. **Machine Learning for Security and the Internet of Things: the Good, the Bad, and the Ugly**, IEEE *Access*, March 2020.
3. Iqbal H and Sarker. **Machine Learning: Algorithms, Real World Applications and Research Directions**, March 2021.
4. Olutosin Taiwo and Absalom E. Ezugwu. **Internet of Things-Based Intelligent Smart Home Control System**, University of Kwazulu-Natal, South Africa, Sep 2021.
5. Shriram Gaurishankar Ughade, Shubham Maruti Khutwad, Yadnesh Gulabrao Shinde and Shubham Rajendra Bhapkar. **Smart Home Automation System Using Machine Learning**, Pune, Maharashtra, India, May 2023.
6. Vinay Gugueoth, Sunitha Safavat and Sachin Shetty. **Security of Internet of Things (IoT) using federated learning and deep learning — Recent advancements, issues and prospects,** Science direct, March 2023.
7. Mohammed Aledhari, Rehma Razzak, Reza M. Parizi and Fahad Saeed. **Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications**, IEEE Access, August 2020.
8. Valerian Rey, Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán and Gérôme Bovet. **Federated learning for malware detection in IoT devices**, Elsevier, March 2022.
9. Subrato Bharatia, M. Rubaiyat Hossain Mondala, Prajoy Poddera and V.B. Surya Prasath. **Federated learning: Applications, challenges and future directions**, ResearchGate, March 2021.
10. Chitra A. Dhawale, Kritika Dhawale and Rajesh Dubey. **A Review on Deep Learning Applications**, ResearchGate, March 2021.
11. Lujun Zhai1, Yonghui Wang, Suxia Cui, and Yu Zhou. **A Comprehensive Review of Deep Learning-Based Real-World Image Restoration**, IEEE Access, March 2023.
12. Kazi Masum Sadique, Rahim Rahmani and Paul Johannesson. **A Comprehensive Review of Deep Learning-Based Real-World Image Restoration**, Elsevier, March 2018.
13. Sanskriti Jain, Aarushi Dwivedi, Ashish Khanna. **Implementation of Machine Learning and Deep Learning Techniques in IoT Security: A Review**, ICICC, March 2021.
14. Sakshi Indoliaa, Anil Kumar Goswamib, S. P. Mishrab and Pooja Asopaa. **Conceptual Understanding of Convolutional Neural Network- A Deep Learning Approach**, ICCIDS, March 2018.

15. Keiron O'Shea and Ryan Nash. **An Introduction to Convolutional Neural Networks**, ICCIDS, March 2018.
16. Laith Alzubaidi, Jinglan Zhang, Amjad J. Humaidi, Ayad Al-Dujaili, Ye Duan, Omran Al-Shamma, J. Santamaría, Mohammed A. Fadhel, Muthana Al-Amidie and Laith Farhan. **Keiron O'Shea and Ryan Nash "An Introduction to Convolutional Neural Networks**, Springer, March 2021.
17. Sandeep Sony, Kyle Dunphy, Ayan Sadhu and Miriam A M Capretz. **A Systematic Review of Convolutional Neural Network-Based Structural Condition Assessment Techniques**, Western university, July 2021.
18. Arun Cyril Jose1 and Reza Malekian. **Smart Home automation Security: A literature review**, ResearchGate, July 2021.
19. Arindom Chakraborty, Monirul Islam, Fahim Shahriyar, Sharnali Islam, Hasan U. Zaman, and Mehedi Hasan. **Smart Home System: A Comprehensive Review**, Hindawi, Jan 2023.