4th Indian International Conference on Industrial Engineering and Operations Management
Hyderabad, Telangana, India, November 07-09, 2024
Publisher: IEOM Society International, USA DOI: 10.46254/IN04.20240101
Published: November 07, 2024

Meta-analysis of Cyber Threat Detection in Blockchain Networks Using Deep Learning

Imreena Ali
Research scholar, Best Innovation University,
Anantapur, Andhra Pradesh–515731, India
imreena.cse@gmail.com
https://orcid.org/0009-0005-9814-0603

Dr Madhu Bhukya
KG Reddy College of Engineering & Technology, Hyderabad, India
madhu0525@gmail.com

Abstract

In the digital era, where cybersecurity threats arise large and blockchain technology promises decentralized security, the intersection of deep learning techniques and blockchain networks emerges as a frontier in safeguarding digital ecosystems. Deep learning, a subset of artificial intelligence, excels at detecting complex patterns and anomalies in vast datasets. We can enhance cyber threat detection capabilities by integrating deep learning with blockchain networks. This meta-analysis systematically reviews existing literature on deep learning in detecting cyber threats within blockchain networks. This study lists the examination of research published in the past 5 years, focusing on Neural network applications and other deep learning architecture and evaluating the performance of these techniques in detecting various types of cyber threats and their impacts. Blockchain is a promising technology that addresses these needs. This study uses a meta-analysis approach to identify key themes, trends, and considerations from the current cyber threat detection approach. The study lists topics of potential future research interest and benefits various stakeholders, including researchers.

Keywords

Blockchain, cyber threat detection, Deep learning, cybersecurity, meta-analysis.

1. Introduction

The importance of cyber threat detection and adaptive defense mechanisms in the modern digital landscape cannot be overstated (Ahmetoglu et al. 2022). With the rapid expansion of digital infrastructure and the increasing interconnectivity of technologies, the risk of cyber-attacks has soared. These attacks can initially disrupt operations, compromise sensitive data, and inflict significant financial and reputational harm on organizations (Aljihani et al. 2021). Effective cyber threat detection requires constant monitoring and analysis of network traffic, system logs, and user behavior to identify and neutralize potential threats in real-time. This proactive approach allows organizations to respond swiftly to emerging threats, preventing them from escalating into full-blown attacks (Cha et al. 2020). Traditional security approaches, such as signature-based detection and perimeter defenses, rely on predefined patterns or rules to identify known threats. However, they struggle to keep pace with the evolving tactics of cybercriminals who continually adapt their strategies to evade detection (El-Kosairy et al. 2023). Moreover, these methods often lack the agility and scalability required to address the complexity of modern cyber threats. Deep learning techniques offer a paradigm shift in cybersecurity by enabling systems to learn from vast amounts of data and automatically identify complex patterns and anomalies. Unlike traditional methods, deep learning algorithms can detect previously unknown threats and adapt to evolving attack techniques in real-time. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are particularly well-suited for analyzing large datasets and identifying subtle patterns

indicative of cyber threats. Additionally, Generative Adversarial Networks (GANs) can simulate adversarial behavior to enhance the robustness of cyber defense mechanisms (Gadekallu et al. 2021). By leveraging the power of Deep Learning (DL), organizations can enhance their cyber resilience by augmenting traditional security measures with adaptive defense mechanisms (Hajizadeh et al. 2020). These mechanisms continuously learn from new data and adjust their strategies, providing a proactive defense against emerging threats. Ultimately, the objective is to integrate deep learning with blockchain networks, to enhance cyber threat detection and adaptive defense mechanisms. • Evaluate the current DL techniques employed in cyber threat detection within blockchain networks. • Investigate the effectiveness of adaptive defense mechanisms utilizing DL algorithms in mitigating cyber threats specific to blockchain ecosystems. • Provide insights into the challenges and opportunities associated with integrating DL methods for enhancing cybersecurity in decentralized systems like blockchain networks. This theoretical framework sets the stage for exploring current state-of-the-art deep learning techniques for cyber threat detection within blockchain networks, investigating the effectiveness of adaptive defense mechanisms utilizing deep learning algorithms, and providing insights into the associated challenges and opportunities. This meta-analysis review summarized the existing academic research literature for systematically understanding and enhancing cybersecurity strategies, leading to safer digital environments for all stakeholders in blockchain technologies using deep learning (Islam et al. 2021, Javaid et al. 2016, Shafay et al. 2024, Zhang et al. 2020).

1.1 Background and Rationale

The rationale for taking up this study revolves around three key reasons:
1. Traditional cybersecurity defenses are struggling with the variety of security and adaptive nature of modern cyber threats.
2. Understanding how to integrate and leverage these technologies in cybersecurity is critical for developing next-generation security infrastructure.
3. the growing era needs adaptive defense mechanisms that can autonomously learn from new data and experiences to predict and prevent future attacks

1.2 Research Questions

The study attempts to address the following research questions:

a) Are there any correlations between cybersecurity and blockchain vulnerabilities? If so, how are both correlated?
b) How do Deep Learning technologies contribute to their effectiveness in detecting and predicting Cyber Threat Detection?
c) What are the major types of cyber-attacks in blockchain networks that are highly prone to?
d) What are the Positive and Negative Impacts of Deep Learning in Blockchain on Cyber Threat Detection?
e) Are there specific characteristics of deep learning that can contribute to developing adaptive cyber defense mechanisms in blockchain?
f) In what ways do blockchain-enhanced cyber threat detection in Traditional cybersecurity methods, and what are the implications for future defense strategies?

1.3 Inclusion/Exclusion Criteria

1.1.1. Inclusion

a) Studies Explicitly Examining the Application of Deep Learning Techniques for Cyber Threat Detection in Blockchain Networks.
b) Studies focus on assessing the performance of specific deep learning models.
c) Studies published in peer-reviewed academic journals or conference proceedings.
d) Studies published within a defined timeframe (e.g., past 5 years)

1.1.2. Exclusion

a) Exclude studies that do not focus on detecting cyber threats in blockchain use of deep learning techniques.
b) Exclude studies not published in peer-reviewed academic sources.
c) Opinion pieces, editorials, or book chapters.

2. Methods

A well-structured literature search strategy is adopted to conduct a comprehensive meta-analysis of cyber threat

detection in blockchain networks using deep learning algorithms.

3. Literature Search Strategy

Considering the research objective, the literature search strategy included the following:

1. **Academic Databases**: Scopus, Web of Science, IEEE Xplore, ACM Digital Library, Google Scholar, PubMed, cybersecurity, and AI conference journals.

2. **Search Terms**: "Cyber Threat Detection in Blockchain Networks using deep learning" is used. The rationale behind the search term is that it combines terms related to "blockchain" (e.g., blockchain", "blockchain security", "blockchain networks") with terms associated with " cyber threat detection" (e.g. "cyber threat detection", “security threats”, "cybersecurity," "threat intelligence", “distributed ledger technology”) and with "deep learning" (e.g. deep learning”, "machine learning," "neural networks," "CNN" (Convolutional Neural Networks), "RNN" (Recurrent Neural Networks)). Synonyms and alternative phrases are also used to ensure broader coverage.

3. **Boolean Operators**: Boolean operators like "AND" and "OR" are used to refine search results within the context of “deep learning AND blockchain AND cyber threat detection” and “Neural networks OR machine learning AND blockchain

4. **Date Range**: Our search focused on studies published within the past five years, from 2020 to 2024, ensuring that recent advancements and developments are captured..

5. **Grey Literature:** Additionally, conference proceedings, pre-print repositories, and relevant websites of government agencies and research institutions are considered to identify potentially relevant grey literature not indexed in academic databases. This became necessary because the topic is still evolving study Selection Process

A two-stage screening process is undertaken as follows:

1. **Stage 1 (Title and Abstract Screening)**: Two independent reviewers screened titles and abstracts based on pre-defined inclusion criteria. The studies had to (i) investigate Core topics of deep learning and cyber threat detection within blockchain networks., (ii) address at least one of the following key concerns ("deep learning", "cybersecurity", "threat detection", "blockchain", "neural networks"), and (iii) be published in peer-reviewed journals, conference proceedings, or reputable report.

2. **Stage 2 (Full-Text Screening)**: Compile a list of studies that have passed this initial screening phase. Both reviewers underwent a full-text review of the remaining studies to confirm they fully met the inclusion criteria and provided relevant data for analysis..

4. Data Extraction and Coding

Each included study extracted relevant data using a pre-defined data extraction form. This form captured information on the following parameters. The form data is exported to a spreadsheet for further analysis.

1. Study details of Author information (year, publication venue)
2. Deep Learning Types of models used (e.g., CNN, RNN, LSTM), configuration details, and modifications specific to the blockchain.
3. Dataset Characteristics: Dataset size, nature (synthetic, real-world), data sources, preprocessing steps, and data augmentation techniques.
4. Outcome measures related to Performance Metrics (e.g. Accuracy, precision, recall, F1 score, detection speed, false positive rates, computational requirements)
5. Any limitations or biases identified by the study authors

The extracted data is then coded using Zotero and MAXQDA qualitative coding software, categorizing information based on pre-defined themes and frameworks relevant to our research question and key concerns.. Figure 1 Show workflow of the proposed approach for the text literature analysis

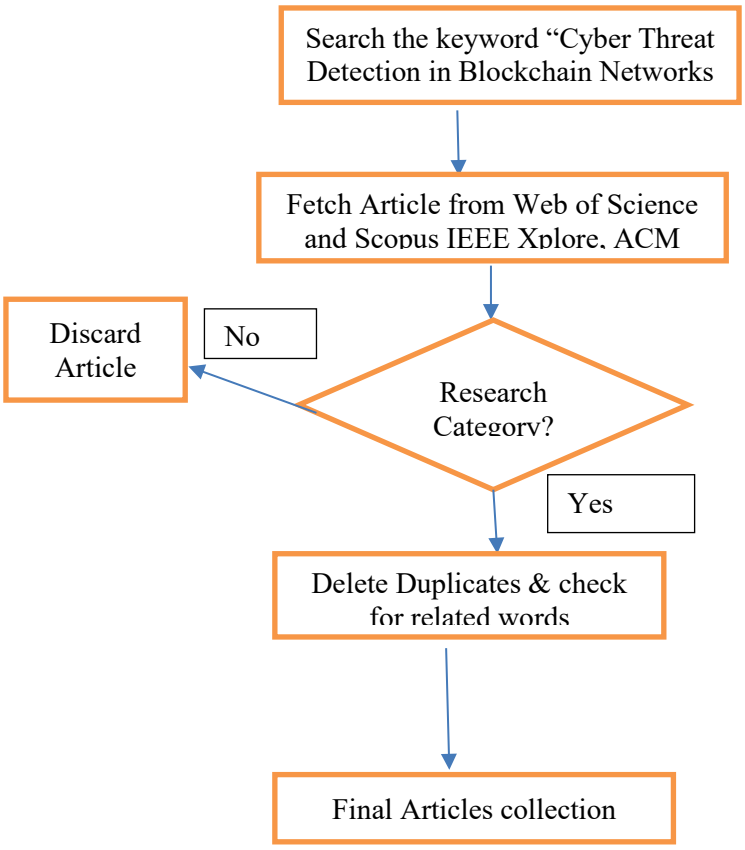

Figure 1. Workflow of the proposed approach for the text literature analysis

Quality Assessment of Studies
Studies selected for review were systematically assessed for risk bias about study design, data collection, analysis, and reporting before considering the major review of included studies.

Meta-analysis Methods
While the research question mainly calls for a qualitative synthesis of current research, a dimension of meta-analysis techniques is applicable for studies that present comparable quantitative data on specific outcomes related to security, transparency, and privacy (e.g., the proportion of successful attacks on the blockchain).

5. Results

Characteristics of Included Studies
Studies included: Table 1 shows the quantum of research studies that have been done on the topic over the years. Both Table 1 and Figure 2 show that the topic is increasinglybecoming an area of research interest. Considering the availability of full papers and several other inclusion and exclusion criteria, 70 papers were selected and used in the study. Figure 2 displays connected papers generated using Lit maps and Figure 3 Connected papers generated using Litmaps.

Table 1. Search trends for the keyword "Cyber Threat Detection in Blockchain Networks."

Academic Database	**2019**	**2020**	**2021**	**2022**	**2023**
Scopus	96	117	132	140	176
Web of Science	44	55	62	55	51
IEEE Xplore	47	51	61	89	108
ACM Digital Library	7017	8051	9302	8455	9517
Dimensions.ai	2787	3605	5006	6337	8022
Google Scholar	7870	9250	11100	13900	10900

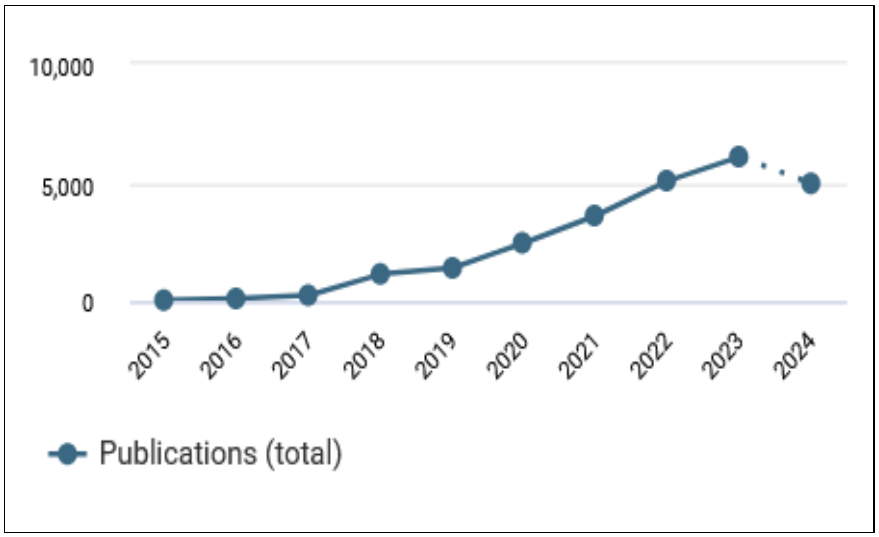

Figure 2. Publication trends for the keyword ""Cyber Threat Detection in Blockchain Network" in dimensions.ai

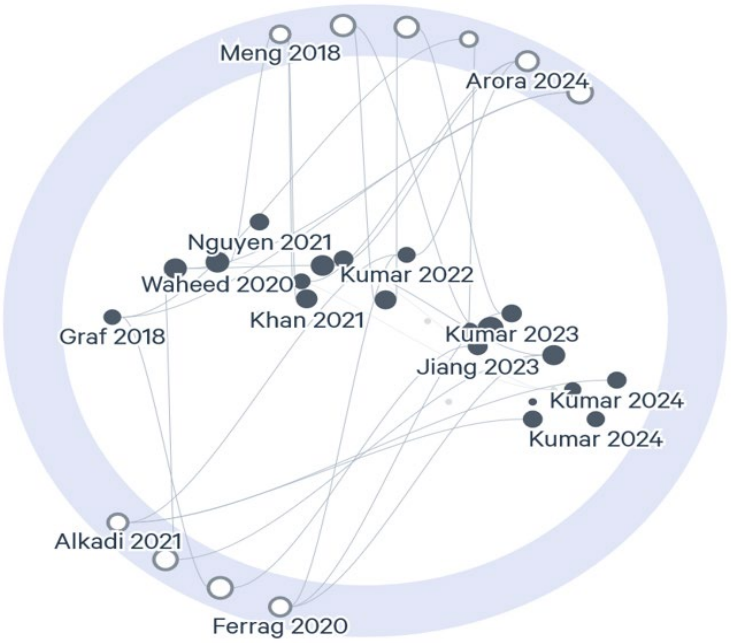

Figure 3. Connected papers generated using Litmaps.

Table 2. Leading Researchers and their affiliation

Name of Researchers	Affiliation
Nikita Borisov	University of Illinois at Urbana-Champaign, USA
Joseph K. Liu	Monash University, Australia
David Chaum	Elixxir, USA
Dimitris Spinellis	iversity of Economics and Business, Greece
Rajesh Kumar	Indian Institute of Technology (IIT),india
Zibin Zheng	University of Sydney, Australia
Zhangjing Shi	Tsinghua University, China
Miklos A. Koren	Budapest University of Technology and Economics, Hungary
Luca P. Carlucci	University of Bologna, Italy

These researchers contribute to various aspects of blockchain, including security protocols, threat detection mechanisms, and decentralized applications. These references provide a foundation for understanding the current Scenario

Table 2 lists leading researchers in the area and their affiliations.

Table 3 shows the type of research publications that happened.

Table 4 shows a list of leading journals that published manuscripts related to the topic.

Table 3. Leading Publication Types

Type of Publication
Conference Proceedings
Research Articles
Edited Book

Table 4. Leading/Influential Journals List

Name of Journal
MDPI
Journal of Information Processing Systems
IEEE Explore
International Journal of Scientific & Technology Research
Future Generation Computer Systems
Networking and Collaborative Systems(Springer)
International Journal of Smart Home
ACM International Conference Proceeding Series
Security And Communication Networks
AIP Conference Proceedings

1. **Publication years**: The study finds that many of the research publications on the "cyber threat" topic started in 2015 and have rapidly gained pace since then. While early publicationsfocused on primarily foundational security aspects, decentralized networks' more recent studies have explored a wider range of topics and applications.

2. **Study design**: Most researchers use the predominant study designs,conceptual papers, simulations, and prototypes, followed by experimental designs. Further, these studies focused on addressing the key issues of security in blockchain.

3. **Geographic scope**: No geographical bias or selective coverage is being taken. Table 5 shows the list of leading countries and regions where the research is primarily done.

Table 5. Leading countries of research

List of countries/regions
United States
India
Slovenia
China
United Kingdom
Malaysia
Canada
Bangladesh
Indonesia
South Korea

4. **Blockchain platforms**: The study finds that Ethereum, Hyperledger Fabric leading platforms in blockchain networks due to it robust and smart contract capabilities and ecosystem(Cha et al., 2020).combining data from Ethereum-based applications with insights from proprietary systems can enhance threat analysis(Zhang et al., 2020). While some countries Washington D.C. and Russia, may face challenges in threat detection due to potential lack of transparency and accountability(Islam et al., 2021). blockchain platforms offer cryptographic and immutability techniques, to provide a strong security. deep learning model integration will enhance performance and scalability(Aljihani et al., 2021).real-time threat detection by deploying deep learning models that analyze network traffic in real time, allowing for immediate identification and mitigation of threats(Gadekallu et al., 2021).Countries like Australia and Norway, which use commercial systems, can inform best practices for integrating blockchain with deep learning in threat detection. By analyzing the strengths and weaknesses of these implementations, developers can enhance their approaches to provide overall cybersecurity (El-Kosairy et al., 2023).

5. **Consensus mechanisms**: in digital era blockchains are popular implementations and highlighting their suitability for different types of blockchain-based applications(Hajizadeh et al., 2020). The most common consensus mechanisms followed are such asProof of Work (PoW) has High energy consumption and risk of 51% attacks,its is well known for robust security and decentralization, Proof of Stake (PoS) Reduces energy usage but potential centralization concerns but PoS may be susceptible to new types of attacks(Aljihani et al., 2021).Delegated Proof of Stake (DPoS) improves transaction Efficiency but trade-offs with a decentralization nature. In some works, a hybrid model is used to address the problems of securing (Ahmetoglu & Das, 2022).

6. **Privacy-enhancing techniques (PETs)**: The study finds Secure Multi-Party Computation (MPC), Homomorphic encryption, Zero-knowledge proofs, Ring signatures,Confidential Transactions and Stealth Addresses are thetop PETs being used in enhancing security(Shamsan Saleh, 2024).These privacy-enhancing techniques can help secure user data and transaction details, making blockchain networks more robust and privacy-preserving.

7. **Outcome measures**: Briefly mention the outcome measures used to assess security,transparency, and privacy making blockchain networks more robust and privacy-preserving in the studies.

6.Discussion

Deep learning excel in analyzing large datasets to detect complex pattern behavior for cyber threats security(Javaid et al., 2016).By integrating deep learning with blockchain may affect the overall scalability The potential of deep learning has been witnessed in almost all industrial sectors(Shafay et al., 2023).While the blockchain system handles transparency requirements, a pseudonym mechanism can be used for identity privacy, while homomorphic encryption technology can be used forcyber threats detection. it is difficult to achieve the availability of labeled data in sufficient quantities to train DL models since blockchain data are mostly private and decentralized. We will have to resolve synthetic data and need a federated learning method for sharing data while keeping privacy(Aljihani et al., 2021).

Since cyber threats are not a normal activity, DL models may face a problem in learning from an imbalanced dataset. We can use special techniques to balance the data by using Different deep learning models like CNN,GAN , RNN that work for different needs. CNNs are good for analyzing patterns, RNNs are better for sequences (like transaction history), and GANs can generate data to train models(Javaid et al., 2016). More complex models can be more accurate, but they may require more computing power.Deep learning models have a large number of layers and complex architecture .Model like RNN and GNN can be used for analyzing sequential data and transaction flows ,GNN can be used to model graph like structure of blockchain network.

As blockchain networks generate humongous data, it is very hard to get a good-quality dataset for training the models,the fact encrypted transaction information can restrict the capabilities of trained models in terms of explanation regarding insight into information, so it needs advanced methodologies. federated learning can address problems related to scarcity and issues with privacy.Efficient threat detection requires diverse data sources such as sources such as (transaction pattern and network traffic) preprocessing of large blockchain datasets is require to capture cyber threats(El-Kosairy et al., 2023). Blockchains need to detect cyber threats in real time. The deep learning model needs to be optimized by balancing between complexity and speed of computation. Which can support lightweight models for faster processing.The blockchain system may need to identify threats very quickly therefore deep learning models need to be

fast. A model should handle real-time data by utilizing specialist tools designed for real-time processing.

The Blockchain mechanisms, like PoW, PoS, affect DL models. As PoW is slow but gives adequate time for analysis, and PoS is fast but may limit the time taken for processing. Training DL models use a significant amount of energy. We need to reduce this, perhaps by providing energy-efficient algorithms.

deep learning models can support numerous transactions and interaction processing within their blockchain network's Privacy and Security. Deep learning models depend on transaction data and thus can include sensitive information. A technique is required to improve model updating without violating the privacy of the individuals. Techniques like federated learning and differential privacy can be beneficial for model training while still protecting individual privacy. Techniques in continual learning allow the model to retain prior knowledge and learn new data and identify new threat patterns.

The proposed model needs to be strong enough against adversarial attacks. Techniques such as adversarial training, input preprocessing, using robust architectures might help mitigate such vulnerabilities.

Practical and Policy Implications

Six practical and policy implications arise from the findings of the study:

1. Integrating deep learning with blockchain security will enhance the security for industrial sectors like Healthcare ,finance and supply chain management ,where data security and integrity play crucial roles.
2. Deep learning model are more efficient in identifying threats in real time applications where quick response time is needed.
3. Implementing a Deep Learning-based model will provides security solutions for large network which addresses scalability
4. While deep learning significantly enhances security cost of deploying this model may be more,but cost may be neglected over benefit of improved threat detection techniques.
5. Deeplearning model should work efficiently across different blockchain platforms. This will increase flexibility and reduce the complexity of managing security across network.
6. This integration of Deeplearning and blockchain must policy rule and redulation against data privacy,security and ethical consideration.

7. Regulatory bodies and authorities (such as Governments and organization) could explore implementing blockchain security using deeplearning to address existing security, transparency, and privacy concerns with traditional . There isclear evidence that blockchain's decentralized nature need federate learning model.

8. Technical standards and best practices need to be developed for blockchain network. Areas like cryptography methods, consensus algorithms, and protocols for authentication, privacy, and verifiability require guidance.

9. Legal and regulatory frameworks must be updated and best practices for implementing deep learning in blockchain security, there is need for balance between security and privacy and ethical issues.

10. International cooperation is important as many studies are conducted globally. Standardization efforts and guidelines developed across different administrations can help the proliferation of best practices.

11. Accessibility still needs to be addressed as the digital divide remains.

Comparison of Techniques

Table 6 shows a comparison of deep learning algorithm

Table 6. Comparison of deep learning algorithm

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
CNNs	93.5	91	88.5	89.7
LSTMs	94.1	92.2	90.1	91.1
Autoencoders	89.3	86.7	84.5	85.6
GANs	92.7	91	87.6	8.5
DBNs	88.5	85.5	83	10.2

Key Findings

The CNNs and the LSTMs performed very well in terms of accuracy, precision, and recall. In this light, these were the best deep-learning techniques for cybersecurity threat detection in blockchain. Autoencoders performed outstandingly well in unsupervised learning scenarios but were pretty bad with false negatives relative to their supervised counterparts. GANs seem to promise much for the detection of rare and sophisticated threats since it generates attack scenarios, although training instability is a major challenge. DBNs, though effective, require a significant amount of computational resources and training time, which in turn limits their practical applications in real-time threat detection (Figure 4).

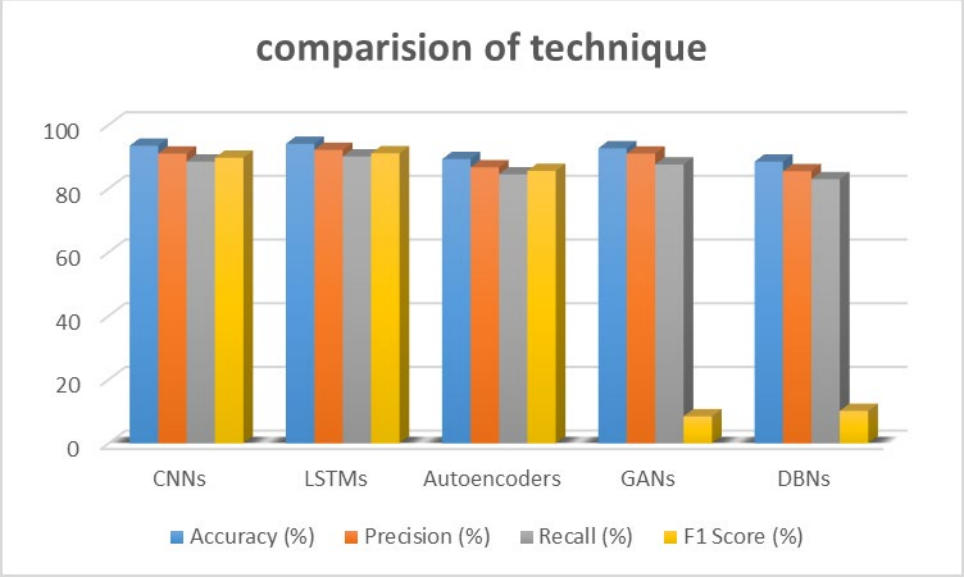

Figure 4. comparison of deep learning algorithm.

Future Research

Researchers highlight four potential areas that have scope for future research. These include:

1. **Scalability and Performance**: The scalability and performance of a blockchain system can be measured in the dimensions of block generation rate, transaction speed, and block size(Shafay et al., 2023). Optimized deep learning model need to be design to work efficiently on blockchain network. Explore distributed learning frameworks to train model to work over blockchain network to improve scalability while maintaining performance. Minimizing delays and improving overall system response over threat detection using load balancing strategies

2. **Privacy-Enhancing Techniques**: While blockchain offers transparency, Explore more on the practical implementation of federated learning in blockchain to enhance privacy techniques,use of homomorphic encryption for threat detection without exposing sensitive information.Future research can explore some advances in cryptographic techniques, such as zero-knowledge proofs, ring signatures, and homomorphic encryption, to strengthen privacy guarantees without compromising verifiability.

3. **Usability and Accessibility**: Integrating deeplearing with blockchain infrastructure and systems and ensuring user-friendliness is important. This is because the application will be used by a diverse population with little or no technical knowledge . educating users on the benefits and functionalities of Deeplearning security tools, enhancing their ability to utilize these systems effectively.The concept ofthe user interface for distributed applications (dApps) is still in its infancy. Research should focus on intuitive interfaces, make threat detection tools user with disabilities, and integration accessible with existing system mechanisms.

4. **Standardization and Regulations**: Clear standards and regulations are needed for secure and consistent implementation across different jurisdictions. Research should explore collaborative efforts to develop interoperable standards, promote consistency and trust, and address data protection concerns.

5. **Long-Term Security and Maintenance**: Blockchain systems require ongoing maintenance and upgrades to address evolving security threats, continuous monitoring, and real-time adjustment. Hence, research should explore sustainable funding models, secure maintenance procedures, and long-term security guarantees in blockchain networks.

7.Conclusion

This literature review analyzed and synthesized prior research that went into developing andapplying the concept of cyber threat detection in a blockchain environment. The study identified various deep learning approaches that enhance cyber threat detection in blockchain. However, as the study finds, additional research is still needed to realize the full potential of the use case/application. Scalability and performance must be improved. More work is also required todevelop advanced privacy-enhancing techniques, intuitive user interfaces, and international standardization efforts. Long-term maintenance and ongoing security also present challengesthat future research could help address. As the technology progresses, blockchain has the potential to improve trust substantially. Further research should focus on a hybrid model for enhancing privacy and shaping the future of security within the blockchain network.

References

Ahmetoglu, H., & Das, R., A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions. *Internet* of *Things*, *20*, 100615, 2022. https://doi.org/10.1016/j.iot.2022.100615

Aljihani, H., Eassa, F., Almarhabi, K., Algarni, A., & Attaallah, A., Standalone Behaviour-Based Attack Detection Techniques for Distributed Software Systems via Blockchain. *Applied Sciences*, *11*(12), 5685, 2021. https://doi.org/10.3390/app11125685

Cha, J., Singh, S. K., Pan, Y., & Park, J. H., Blockchain-Based Cyber Threat Intelligence System Architecture for Sustainable Computing. *Sustainability*, *12*(16), 6401, 2020. https://doi.org/10.3390/su12166401

El-Kosairy, A., Abdelbaki, N., & Aslan, H., A survey on cyber threat intelligence sharing based on Blockchain. *Advances in Computational Intelligence*, *3*(3), 10, 2023. https://doi.org/10.1007/s43674-023-00057-z

Gadekallu, T. R., M K, M., S, S. K., Kumar, N., Hakak, S., & Bhattacharya, S., Blockchain-Based Attack Detection on Machine Learning Algorithms for IoT-Based e-Health Applications. *IEEE Internet of Things Magazine*, *4*(3), 30–33, 2021. https://doi.org/10.1109/IOTM.1021.2000160

Hajizadeh, M., Afraz, N., Ruffini, M., & Bauschert, T., Collaborative Cyber Attack Defense in SDN Networks using Blockchain Technology. *2020 6th IEEE Conference on Network Softwarization (NetSoft)*, 487–492, 2020. https://doi.org/10.1109/NetSoft48620.2020.9165396

Islam, M. R., Rahman, M. M., Mahmud, M., Rahman, M. A., Mohamad, M. H. S., & Embong, A. H., A Review on Blockchain Security Issues and Challenges. *2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC)*, 227–232, 2021. https://doi.org/10.1109/ICSGRC53186.2021.9515276

Javaid, A., Niyaz, Q., Sun, W., & Alam, M., A Deep Learning Approach for Network Intrusion Detection System. Proceedings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies (Formerly BIONETICS). 9th EAI International Conference on Bio-inspired Information and

Communications Technologies (formerly BIONETICS), New York City, United States, 2016. https://doi.org/10.4108/eai.3-12-2015.2262516

Shafay, M., Ahmad, R. W., Salah, K., Yaqoob, I., Jayaraman, R., & Omar, M., Blockchain for deep learning: Review and open challenges. *Cluster Computing*, *26*(1), 197–221, 2023. https://doi.org/10.1007/s10586-022-03582-7

Shamsan Saleh, A. M., Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. *Blockchain: Research and Applications*, *5*(3), 100193, 2024. https://doi.org/10.1016/j.bcra.2024.100193

Zhang, Y., Xiong, F., Xie, Y., Fan, X., & Gu, H., The Impact of Artificial Intelligence and Blockchain on the Accounting Profession. *IEEE Access*, *8*, 110461–110477, 2020. https://doi.org/10.1109/ACCESS.2020.3000505

Biographies

Imreena Ali Research scholar at **BEST Innovation University(BESTIU)** with almost 11 years of teaching experience in Engineering college. Active role in organizing and participating in numerous workshops and FDP.Academic contributions include a wide range of publications in national and international reflecting my expertise and advancing my research Knowledge. Currently, I am researching the Blockchain domain.

Dr. Bhukya Madhu It is a privilege and distinct pleasure to be guided by Dr. B. Madhu, who is known across the world as a distinguished scholar and a specialist in the field of engineering education Presently, he holds a position of a Professor in the Computer Science Department at KG Reddy College of Engineering & Technology where he has been for over eight years. He also holds the coveted NFST National Fellowship and represents the university as a co-supervisor to four Ph.D. scholars at Bharatiya Engineering Science and Technology Innovation University (BESTIU). He also held and attended the organizing committee of many workshops, FDPs and has been published widely in national and international research articles in esteemed international journals, focusing on IoT security, machine learning, and sustainable technologies, books and journals. His conference papers cover innovative areas, such as deep learning for IoT networks, attack severity classification, and blockchain. In his credits publishing the book *Deep Learning Approaches for Intrusion Detection and Attack Severity Classification in IoT Networks* and contributing to *Blockchain for the Traditional Stock Markets*.While conducting my research, I find his expertise and guidance crucial to my work.