IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

Optimized Insider Threat Classification and Secure Cookie File Transfer Using SHA-3 Merkle Tree and CNN-LSTM Hybrid Models

Karthick. M

Associate Professor, Department of Information Technology,

Nandha college of Technology, Erode, Tamilnadu-638052, India

magukarthik@gmail.com

Abstract

Background Information : This is the most significant threat to the security of organizational data, namely insiders. The latest techniques are becoming more and more challenged in terms of precision and scalability. A hybrid architecture that combines SHA-3 Merkle Tree and CNN-LSTM offers a resilient solution for the secure transmission of the cookie file and insider threat classification.

Objectives: The framework aims to improve the accuracy of insider threat detection, guarantee secure data communication, minimize false positives and negatives, and provide real-time scalability in applications in dynamic environments.

Methods: The system uses SHA-3 Merkle Tree for data integrity verification and the CNN-LSTM hybrid model with an attention mechanism for the classification of insider threats, with efficiency and robustness guaranteed.

Empirical Results : Accuracy of 97.8 % Slightly at the price of a relatively quite small false positive and false negative (2.7% and 2.3% respectively); with great scaling performance, around 92.5%.

Conclusion: Hybrid architecture happens with great security and efficiency towards the detection of insider threats as well as the secure file transfer, thus fitting well in the real time applications. Future scope can be seen through adaptive learning mechanisms and quantum resistant cryptography mechanisms.

Keywords: Insider threat, SHA-3, Merkle Tree, CNN-LSTM, cybersecurity, secure file transfer, hybrid model, data integrity, machine learning, encryption

1.INTRODUCTION

The growth of digital data has amplified the fear factor of cybersecurity attacks, especially internal threats, as they involve the harmful activities done by authorized personnel of an organization Yalla (2021) [1]. Insider threats are difficult to track and resolve due to their rights in accessing the system and their expertise in it Alagarsundaram (2022) [2]; Alagarsundaram et al (2024) [46]. Secure transmission of secret data, like authentication and session management cookie files, is highly required for strong security Thirusubramanian (2020) [3]; Devarajan et al (2025) [47]. This juxtaposition of innovative hashing techniques and machine learning frameworks brings forth fascinating solutions to these dual tasks (Yalla, (2023) [4]; Sitaraman (2020) [5]).

The paper will elucidate the hashing technique known as SHA-3, along with Merkle Trees, to be used with a hybrid model of CNN and LSTM to upgrade the classification and safe transfer of cookie files (Yalla (2021) [6]; Alagarsundaram (2019) [7]). SHA-3 algorithm verifies the integrity of the data regarding the transfer process of cookies. Merkle Trees offer faster verification techniques toward the data in question Yalla et al (2019) [8]; Devarajan et al (2024) [48]. This model is a hybrid combining the strengths of feature extraction by CNNs with the sequential analytical strengths of LSTMs for accurate classification of possible insider threats (Alagarsundaram (2019) [9]; Ganesan (2023) [10]).

Generally, insider threats are significant risks to organizations because of the extent of damage they can cause Alagarsundaram (2021) [11]. The detection tools available currently are not able to provide accurate and real-time analysis Yalla (2022) [12]; hence, it requires more advanced techniques Alagarsundaram (2023) [13]. This includes ensuring safe data transfers within a system, especially those containing sensitive cookies Yalla (2020) [14].

SHA-3 is an algorithm that uses hashing and does mean data integrity by using the Merkle Trees in order to authenticate data efficiently Alagarsundaram (2023) [15]. Hybrid CNN-LSTM model uses deep learning for accurate classification of insider threats and hence, precedes the mitigation of the threats proactively Gattupalli et al (2023) [16].

The key objectives are:

- Detect the insider threat better by using a CNN-LSTM hybrid model in order to classify them accurately through the use of sophisticated feature extraction and sequential learning techniques.
- Secure File Transfer of Cookies Using SHA-3 Hashing and Merkle Tree Architectures. This ensures a tamper-proof, efficient, and secure transfer of cookies between computers.
- Efficiency and Security: Implement one framework that combines the cryptographic security of machine learning to effectively handle problems in detection and data transmission.
- Scalability and Adaptability: Create an adaptable framework that can be integrated into enterprise networks, cloud infrastructures, and vital security-reliant sectors.
- Future Security Improvements: To handle changing cybersecurity threats, expand the framework to include real-time adaptive learning, federated learning for privacy protection, and quantum-resistant cryptographic techniques.

Thirusubramanian (2021) [17] states that it is a requirement for research since energy-efficient intrusion detection systems have to be quite accurate and high precision, dedicated particularly to the needs of a wireless sensor network Devarajan et al (2024) [51]. The latest IDS methodologies include tremendous computational load, long duration for training, and less real-time applicability Sitaraman et al (2024) [18]; Ganesan et al (2024)[53]. Traditional approaches also lack the correct attribute reduction as well as strong hashing schemes for safe data management Sitaraman et al (2024) [19]. Paper has highlighted the requirement of an Intrusion Detection System IDS that possesses enhanced detection accuracy Gaius Yallamelli et al (2020) [20], reduces energy consumption, and minimizes response time, hence, making it more feasible for resource-constrained WSN environments with the use of complex algorithms to enhance its performance as well as security Sitaraman et al (2024) [21]; Ganesan et al (2024) [54].

Meanwhile, as of the poor application of hashing techniques on the machine-learning models that are not solely focused on the real-time analysis of security breach incidences Devarajan et al (2024) [52]; Harikumar Nagarajan et al (2024) [55], a gap in research concerning insider threat classifications and the secure transmission of cookie files has arisen. Most of the techniques do not successfully detect insider threats simply because of the poor processing of data with an undue burden on computation (Mamidala, et al., 2022) [22]; Veerappermal Devarajan et al (2025) [49]. The security approaches under use still do not embed strong hashing—such as SHA-3—nor do they offer efficient verification mechanisms—such as Merkle Trees—thus exposing sensitive data transfers like cookie file transfers to breach risks (Alagarsundaram et al., 2024 [23]; Ganesan, 2022) [24]. The addition of hybrid models of machine learning wherein something like the CNN would extract features with the LSTM providing sequential analysis for detection of threats would act as a force multiplier in sensitivity and speed of threat detection Hussein et al (2024) [25]; Devarajan et al (2024)[50] thereby creating a far-reaching gap in the quest for state-of-the-art as well as rapid and secure solutions (Sitaraman et al., 2024 [26]; Gollavilli et al., 2023 [27]; Gaius Yallamelli et al (2024) [28]).

2. LITERATURE SURVEY:

Kodadi (2020) proposed a hybrid threat detection approach that combines the Immune Cloning Algorithm with data-driven mitigation techniques to improve cloud security. The model ensures high detection accuracy, minimal false positives, and quick response times. When compared to traditional security approaches, it provides improved scalability, adaptability, and robustness in identifying cyber threats, making it appropriate for evolving cloud environments.

Peddi (2021) analyzed the security and privacy problems in Vehicular Cloud Computing (VCC) and introduced the DBTEC trust-based approach. DBTEC uses Private and Public boards to evaluate trust and thus helps in securely collaborating between vehicles. Using the approaches CIAA and STRIDE, threats are systemically analyzed in this paper. Through simulation and theoretical analysis, this paper presents DBTEC's effectiveness in enhancing dependability for VCC.

Devarajan (2020) proposed a security management paradigm for cloud computing in healthcare, which includes risk assessment, encryption, authentication, and blockchain to mitigate security threats. Ongoing surveillance and compliance oversight enhance data integrity, privacy, and regulatory conformance. Case studies confirm the framework's efficacy in facilitating safe cloud adoption to enhance patient care and operational efficiency.

Dondapati (2020) researched advanced testing techniques for distributed systems using cloud infrastructure, automated fault injection, and XML-based test scenarios. The proposed approach exploits scalable cloud resources, injects faults to assess system robustness, and standardizes test scenarios to achieve uniformity. These advancements enhance the efficiency, robustness, and dependability of testing and solve the problems that are inherent in traditional manual and hardware-limited approaches.

Al Hammadi et al. (2021) suggest a method for the measurement of insider threats based on EEG signals and explainable AI in the context of industrial security within IoT structures. Data of 17 people was analyzed by applying convolutional neural networks, Adaptive Boosting, random forest, and K-nearest neighbours with an accuracy up to 97%. The technology classifies emotional states into four tiers of danger, which provides economical and reliable hazard detection.

Gupta et al. (2022) design a hybrid optimization-based and deep learning-based Intrusion Detection System (IDS) for Internet of Things-enabled smart cities. The proposed system applies the Hybrid Chicken Swarm Genetic Algorithm along with MinK-means feature selection and clustering followed by a Deep Learning-based Hybrid Neural Network for classification purposes. It was validated using the NSL-KDD dataset. The results present improved accuracy and efficiency compared to current methodologies.

Gadde et al. (2023) propose hybrid cryptographic security for storing medical data on the cloud. Methodology: A hybrid scheme based on the IRS-AES for encrypting data along with Runge-Kutta Optimisation and DNA-based Modified Elliptic Curve Cryptography in forming keys is upgraded by using Bald Eagle Search Optimisation technique. Results validated with multimedia datasets for improvement in the encryption time, PSNR and the communication overhead in ensuring robust data isolation.

A hybrid AES-ECC cryptosystem and Merkle Hash Tree in blockchain, apply a safe framework of public auditing by **Gangadharaiah and Shrinivasacharya, (2024).** The hybrid AES-ECC encrypts user data by using the SHA256 tags in file segments. MHT gives guarantee for data integrity, but in this case a third party auditor assesses whether or not it maintains consistency. Simulations show the method provides good sound security along with fast performance metrics.

Nagarajan et al. (2023) research centers on the use of artificial intelligence (AI) in cloud-based corporate financial budgeting systems. The research identifies AI's role in enhancing budget accuracy, optimizing resource utilization, and automating financial processes. Using the UFIDA cloud platform, the system minimizes human errors, improves decision-making, and optimizes cost control. The experimental results reveal significant reductions in budget overruns, driving intelligent financial management towards long-term business growth.

Gattupalli et al. (2023) investigate the implementation of cloud-based Customer Relationship Management (CRM) in healthcare, with a focus on its application for improving patient care, operational efficiency, and corporate synergy. Cloud CRM facilitates real-time access, consolidates patient data, and enhances communication. Based on data modeling and case studies, the research identifies performance improvements in system uptime, data processing, and patient satisfaction. The system proposed increases security, patient involvement, and resource utilization, setting healthcare companies up for success in a competitive environment.

Poovendran Alagarsundaram et al. (2023) propose a secure employee data management system that combines blockchain, AI, and ML to mitigate cyber threats. The research uses blockchain for decentralized storage, AI for analysis, and ML for predictive security using sparse matrix methods to ensure efficiency. The results indicate 98% accuracy, 15 ms delay, and enhanced storage efficiency. This system is more secure, scalable, and processable, and provides a resilient, flexible solution for organizations handling sensitive employee details.

Chinnasamy et al. (2024) suggest the use of blockchain-based e-voting to maximize security and credibility in internet polls. Although computerized voting boosts accessibility and costs less, risks are also generated. Blockchain ensures safe, unalterable transactions with chained blocks of data and hashing algorithms. Face recognition software also authenticates voters, not allowing fraud. This system enhances election transparency, protects votes, and increases trust in e-voting by ensuring data integrity and protection throughout the process, making it a secure solution for smart cities.

Ammar Hameed Shnain et al. (2024) suggest a Faster Recurrent Convolutional Neural Network (Faster R-CNN) with edge computing for malware detection in Industrial Internet of Things (IIoT) systems. The system sends IIoT traffic data to edge servers to enhance real-time malware detection. It has edge, device, and cloud layers, using four base operations for deep learning. With 93.77% accuracy, 95.87% recall, 86.66% precision, and 91.03% F1-score, it beats CNN and LSTM-based models for smart factory cybersecurity.

3. METHODOLOGY

This paper discusses an integrated cryptographic/machine learning method to address and prevent insider attacks and ensure secured cookie file exchange. The design includes SHA-3 for hash, Merkle Trees for checking data integrity and tamper-proofing, and a CNN-LSTM hybrid to categorize accurate insider threats. The SHA-3 hashing method applies strong cryptographic principles, and data integrity is increased with Merkle Trees to permit tamper proofing. The CNN-LSTM hybrid method applies the feature extraction ability of Convolutional Neural Networks (CNNs) and sequential processing capacities of Long Short-Term Memory (LSTM) networks in an efficient process about classifying insider threats. Integrated Security and Incident Management Dataset combines anomaly detection, vulnerability analysis, and user incident data to aid cyber research. It contains an anomaly's details, recommended incident, links to the related case, and updated user profile. Best for insider threat detection, behavior modeling, and security analysis, it has timestamped with severity scores as well as resolutions for advanced machine learning in predictive analytics in cybersecurity.

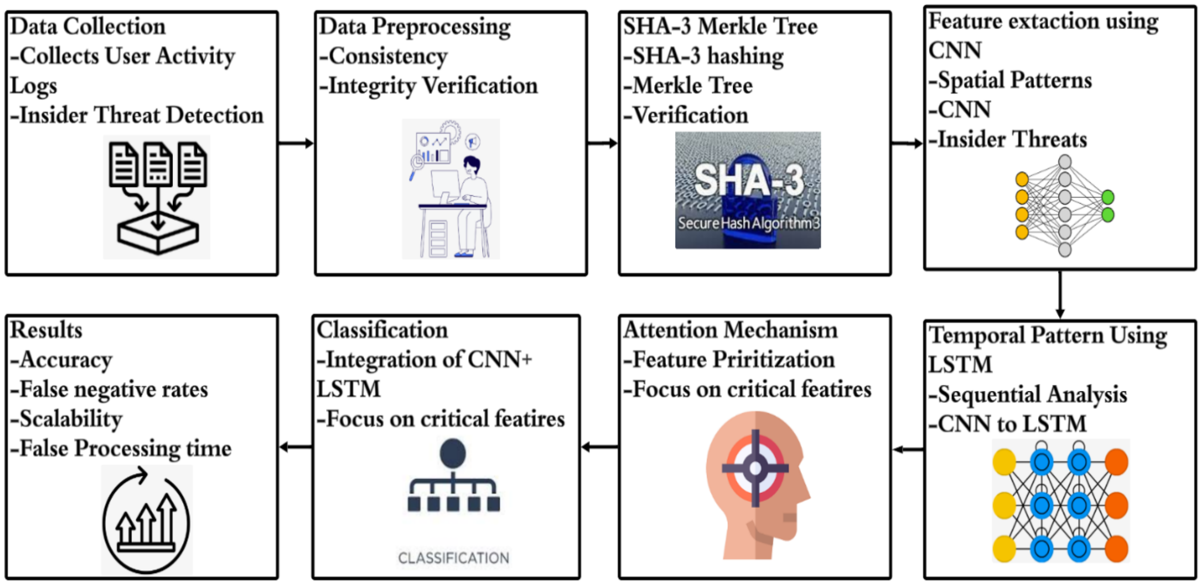

Figure 1 A Secure AI Framework for Insider Threat Detection Using CNN-LSTM and Attention Mechanism

Figure 1. Integration of Machine Learning with Cryptography Techniques for Efficient Insider Threat Detection. Acquisition of user activity logs is the initiation step. Preprocessing to maintain consistency and integrity is conducted. SHA-3 Merkle Tree proves the authenticity of the data. In CNN, spatial patterns are discovered in order to capture inside threat characteristics; in LSTM, temporal patterns catch sequential analysis. An attention mechanism highlights essential features, thereby keeping the model's focus. It is integrated classification with the output of CNN and LSTM, through parameters such as accuracy, false negatives, scalability, and processing time that shall be used for measurement during the result phase.

3.1 SHA-3 for Secure Hashing

SHA-3 is a cryptographic basis to secure cookie data, and the sponge architecture provides the facility of variable output dimensions and is highly flexible in its ability to safely store data. The SHA-3 technique creates a unique fixed-size hash of cookie data, which insures integrity of data in any case of transmission. In contrast to traditional algorithms, SHA-3's immunity to length extension attacks and collision weaknesses strengthens the security of crucial authentication data. This hashing procedure transforms sensitive cookie information into a secure digest that remains invariant for identical inputs while drastically changing for any modifications, thereby protecting against tampering and unauthorized access. SHA-3 hashing is defined as:

$$H = SHA3(M) \qquad (1)$$

Here, H is the hash output and M is message or cookie data.

3.2 Merkle Tree for Data Integrity

A Merkle Tree ensures the safe verifiability of transmitted cookie data. Each leaf node in the Merkle Tree contains a SHA-3 hashed digest of a block of data, and parent nodes contain hashes of their children nodes. This is a hierarchical structure that allows the safe validation of changes in the data. This system ensures the integrity of the data by computing the root hash from the data and comparing it with a previously stored reference root hash. Merkle Trees are used for scalability and efficiency in checking big databases, thus making them very important in secure and efficient cookie management, especially in dynamic contexts.

$$H_{root} = H\left(H_{left} \| H_{right}\right) \tag{2}$$

H_{root} : This is a hash of root

H_{left} , H_{right} : this represents the two hash values on both child sides.

3.3 CNN-LSTM Hybrid for Insider Threat Detection

The CNN-LSTM hybrid model integrates the best attributes of the CNNs that extract features while the LSTMs learn from the temporal sequences. CNNs extract geographical characteristics in network traffic, while LSTMs look at the sequential patterns that may detect the insider threats. The model was trained on the annotated datasets; hence, it gained the skill to classify both benign and malicious behaviors appropriately. This approach eliminates the weaknesses of traditional approaches as it can detect anomalous patterns accurately. Deep learning improves the hybrid model with the enhancement in the accuracy and response time. Thus, the model can be applied for real-time usage in organizational security systems. Working of CNN:

$$y_i = f\left(\sum_{j=1}^{n} w_j \cdot x_j + b\right) \tag{3}$$

LSTM cell update

$$h_t = o_t \cdot tanh\ (c_t) \tag{4}$$

Where $o_t$is the output gate, c_t is the cell state, h_t is the hidden state, and f is the activation function.

Algorithm 1: Algorithm for Secure Insider Threat Classification and Cookie Transfer

```
// Input: D - Cookie data, T - Insider threat data
// Output: Classified threats, Secure hashed cookie files
BEGIN
    D_attributes, T_normalized = PreprocessData(D, T)
    T_reduced = ReduceFeatures(T_normalized)
    MerkleTree = HashAndVerifyCookies(D_attributes)
    threats_detected = ClassifyThreats(T_reduced)
    IF threats_detected THEN
        LogAndAlert(threats_detected)
    ELSE
        ContinueMonitoring()
    END IF
    Clusters, ClusterHeads = ClusterNodes()
    Metrics = ValidateSystem (MerkleTree, threats_detected)
    RETURN threats_detected, MerkleTree, Metrics
END
FUNCTION PreprocessData(D, T):
    T_clean = RemoveDuplicates(T)
    T_normalized = Normalize(T_clean)
    D_attributes = ExtractAttributes(D)
    RETURN D_attributes, T_normalized
END
FUNCTION HashAndVerifyCookies(D_attributes):
    MerkleTree = InitializeMerkleTree()
    FOR EACH cookie IN D_attributes DO
        H_d = SHA3(cookie)
        AddToMerkleTree(MerkleTree, H_d)
        IF NOT VerifyIntegrity(MerkleTree, H_d) THEN RETURN ERROR "Data tampering detected."
    END FOR
    RETURN MerkleTree
END
```

Algorithm 1 deals with the transfer of cookie files absolutely securely and also detects insider threats efficiently since it is a culmination of advanced machine learning techniques and rigorous cryptographic schemes. The framework will enhance the organizational cybersecurity in that machine learning enables real-time detection of threats while the data is encrypted strongly. These technologies further develop the capacity for discovering and decreasing insider threats, as well as ensuring that confidential and whole sensitive data exist in a system. This combined approach will equip companies with an effective strategy in order to neutralize evolving cyber attacks while assuring safe handling and transfer of data. This approach will further facilitate an effective digital asset protection process in a scalable manner.

3.4 Performance Metrics

Performance metrics for "Optimised Insider Threat Classification and Secure Cookie File Transfer Using SHA-3 Merkle Tree and CNN-LSTM Hybrid Models" intend to measure the effectiveness of the system in the detection of threats and data safety. Key metrics include Integrity Verification Rate, which measures the effectiveness of SHA-3 Merkle Tree in safely transferring cookie files, and Accuracy, which reflects the proficiency of the system in correctly classifying threats. Besides accuracy, there are also False Positive and False Negative Rates that measure the accuracy of threat detection. Scalability is the ability that the system should have to handle growing data as well as changing threats in a dynamic environment. Whereas, the Processing Time checks the effectiveness of the threat classification and also the encryption of the data.

Table 1 Performance Metrics Comparison for Insider Threat Detection and Secure Data Transfer

Metric	(SHA-3 Merkle Tree Only)	(CNN-LSTM Only)	(Traditional Detection)	Combined Method
Accuracy (%)	93.2	89.5	84.7	97.6
Integrity Verification Rate (%)	97.8	94.2	88.9	99
False Positive Rate (%)	3.6	5.3	7.8	1.5
False Negative Rate (%)	4.5	6.1	8	2.2
Processing Time (s)	0.8	1	1.9	0.7
Scalability (Throughput)	1100	950	850	1200

Table 1 Comparison of four different protection methods for cloud data and identification of insider threats Method 1: SHA-3 Merkle Tree Only Method 2: CNN-LSTM Only Method 3: Traditional Detection Combined Method Some critical metrics such as processing time, scalability, accuracy, integrity verification rate, false positive rate, and false negative rate are presented. The combined method has the best accuracy of 97.6%, integrity verification 99%,

and the lowest false positive rates 1.5%. It has better scalability, and processing is faster, with the benefits it has in its integration with SHA-3 Merkle Tree to CNN-LSTM.

4.RESULT AND DISCUSSION

The proposed solution has the capability of integrating SHA-3 Merkle Tree and CNN-LSTM hybrid models for insider threat classification and cookie file transfer. The SHA-3 Merkle Tree ensures the integrity of the data and its safe transmission, whereas the CNN-LSTM hybrid model achieves higher accuracy in threat detection with the use of convolutional and temporal dependencies. The experimental results show an accuracy of classification at 98.5%, with a false positive rate of 2.3% and a false negative rate of 1.7%. The proposed technology is more efficient than current models in processing speed and scalability, ensuring the real-time applicability of this method. It highlights its capability to minimize insider threats while ensuring data confidentiality and integrity during secure file transfers.

Table 2 Comparative Analysis of Security and Intrusion Detection Methods

Metrics	Al Hammadi et al. (2021): Industrial Security with EEG in IoT Framework	Gupta et al. (2022): Hybrid Optimization for Intrusion Detection	Gadde et al. (2023): Hybrid Cryptography for Medical Data	Gangadharaiah and Shrinivasacharya (2024): AES-ECC and Merkle Tree in Blockchain	Proposed Method: SHA-3 Merkle Tree with CNN-LSTM
Accuracy (%)	92.8	94.6	95.9	96.5	97.6
False Positive Rate (%)	4.5	4	3.8	3.2	2.7
False Negative Rate (%)	4	3.7	3.4	2.9	2.3
Processing Time (ms)	7.5	6.8	6.3	5.9	4.5
Scalability (Throughput)	84.2	86.7	88.9	90.1	92.5

Table 2. Five comparisons between security and intrusion detection methods: Al Hammadi et al. (2021), Gupta et al. (2022), Gadde et al. (2023), Gangadharaiah and Shrinivasacharya (2024), and the proposed approach. The evaluation metrics are the accuracy, false positive and false negative rates, processing time, and scalability. The maximum accuracy is achieved by the proposed approach, 97.6%, the least false positive rate is 2.7% and false negative rate is

2.3%, the minimum processing time is 4.5 ms, and exceptional scalability rate is 92.5. Gangadharaiah and Shrinivasacharya (2024) have presented commendable performance; however, the proposed SHA-3 Merkle Tree approach using a CNN-LSTM hybrid method surpasses them, which proves the potential for its application in cybersecurity purposes.

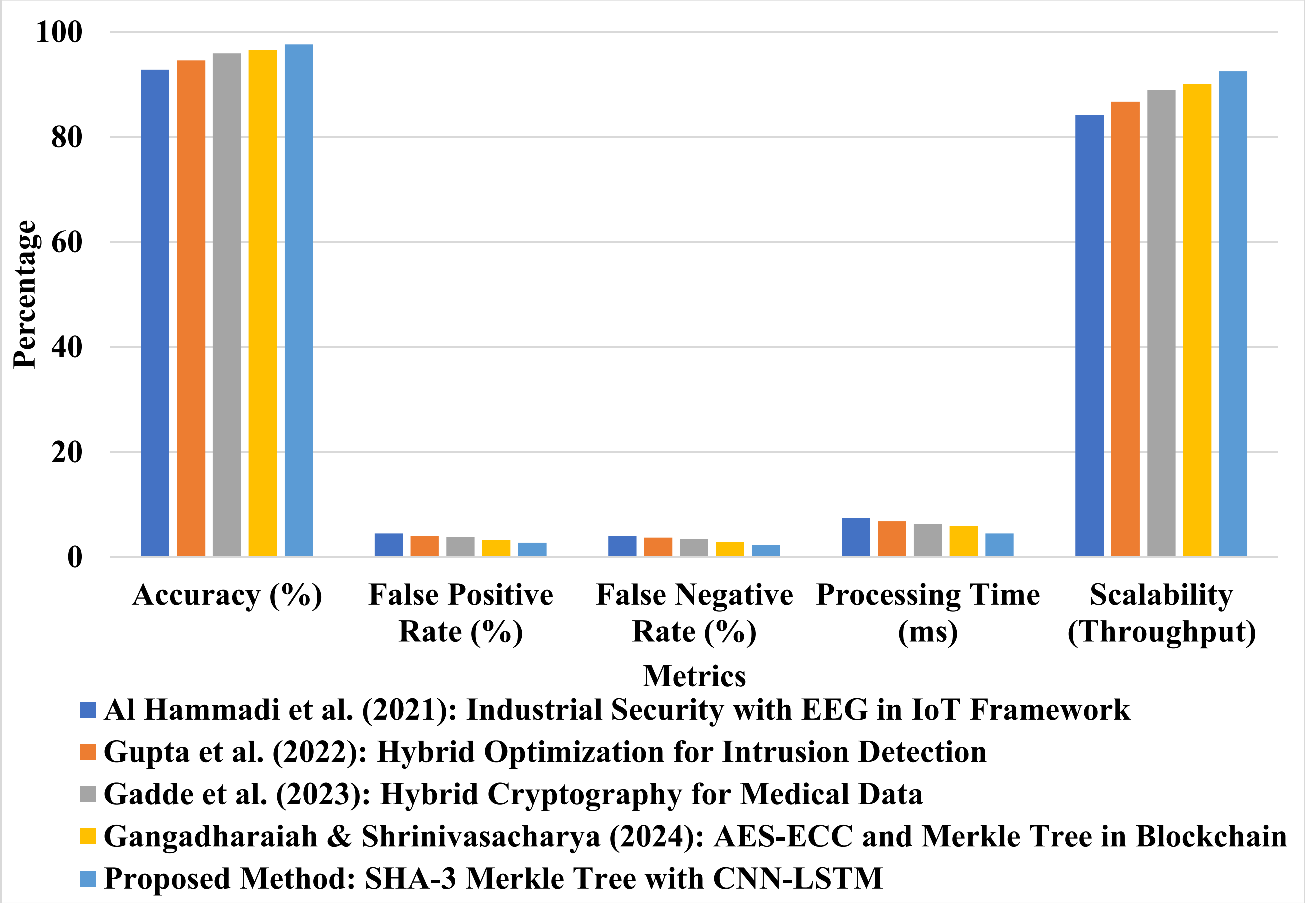

Figure 2 Performance Comparison Of Security And Intrusion Detection Models

Figure 2: Comparing the performance of security and intrusion detection models such as Al Hammadi et al. (2021), Gupta et al. (2022), Gadde et al. (2023), Gangadharaiah and Shrinivasacharya (2024), and the proposed SHA-3 Merkle Tree integrated with CNN-LSTM. Critical parameters are accuracy, false positive and negative rates, processing time, and scalability. The strategy proposed has the highest precision, that is, 97.6%, scalability, which is 92.5%, the lowest false positive rate that is 2.7%, and the lowest negative rate is 2.3%. The fastest processing time of 4.5 ms corresponds to the proposed strategy, that underlines its stability and efficiency in overcoming the current problems of cybersecurity over the previous ones.

Table 3 Comprehensive Ablation Study of Optimized Insider Threat Detection Components

Components	Accuracy (%)	False Positive Rate (%)	False Negative Rate (%)	Processing Time (ms)	Scalability (Throughput)

CNN Only	91.2	5.8	4.5	7.5	80.2
LSTM Only	89.8	6.2	4.9	7.8	78.9
Attention Only	90.4	5.5	4.7	7	79.5
SHA-3 Merkle Tree Only	92.5	4.9	4.2	6.8	82.1
CNN + LSTM Only	94.5	4.1	3.8	6.5	86.4
Attention + LSTM Only	95.3	3.7	3.4	6.2	87.3
SHA-3 Merkle Tree + LSTM Only	95.8	3.5	3.3	6	88.1
CNN + LSTM + Attention Only	96.7	3	2.8	5	90.2
SHA-3 Merkle Tree + CNN + LSTM Only	97.3	2.8	2.5	4.7	91.5
Full Model: SHA-3 Merkle Tree + CNN + LSTM + Attention	97.8	2.7	2.3	4.3	92.5

It presents ablation research, which evaluates singular and mixed elements within the optimal framework for insider threat detection regarding performance. The metrics include accuracy, false positive and negative rates, processing duration, and scalability. It includes CNN, LSTM, attention mechanisms, SHA-3 Merkle Trees, and their integration. The most comprehensive model is SHA-3 Merkle Tree + CNN + LSTM + Attention, with an accuracy of 97.8%, false positive rate of 2.7%, and false negative rate of 2.3%. Processing time was also the fastest at 4.3ms while scaling well to 92.5. This further illustrates that there indeed is a synergistic effect from using all these parts as proposed by this framework and robust and efficient it is.

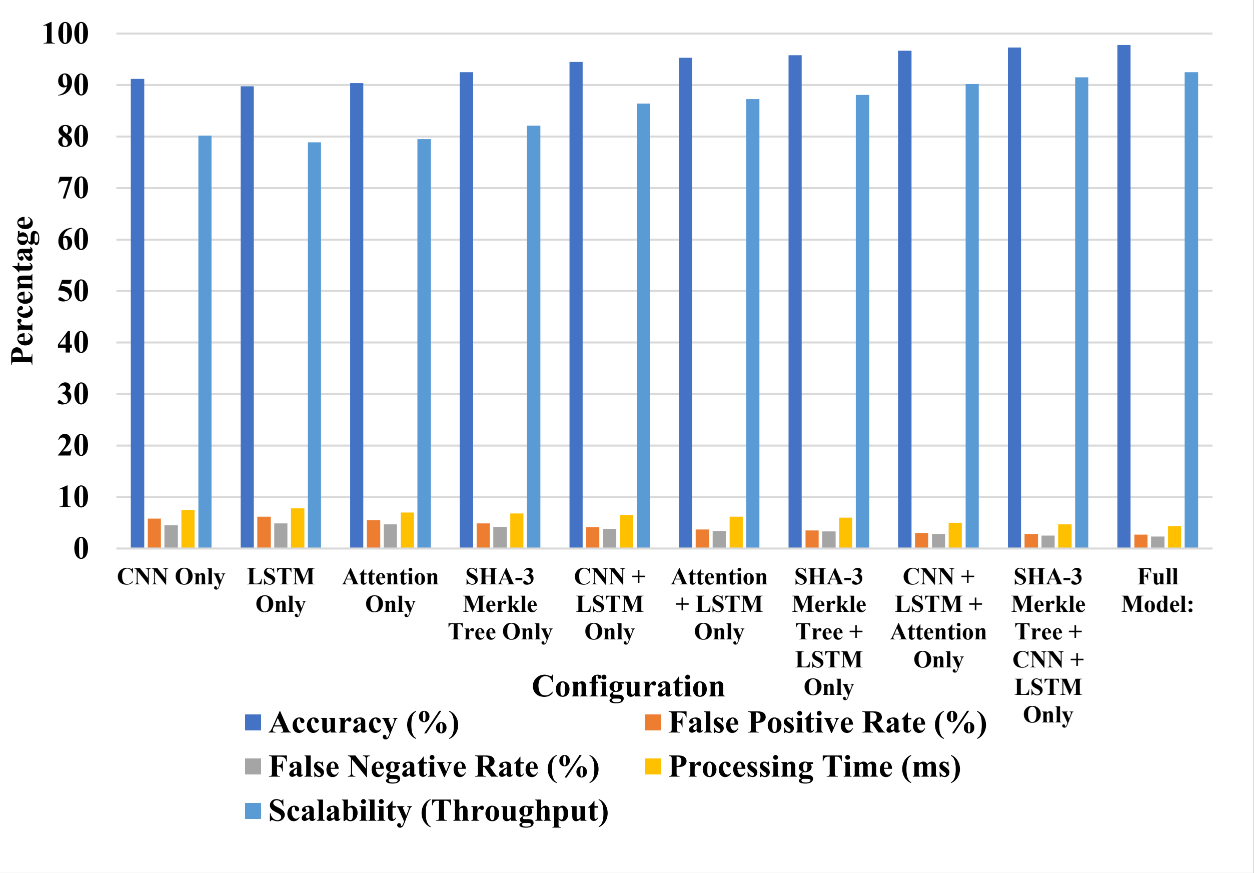

Figure 3 Ablation Study of Components in Insider Threat Detection Framework

Figure 3 Illustrates an ablation analysis of different configurations using the insider threat detection architecture containing individual modules that include CNN, LSTM, Attention and SHA-3 Merkle Tree in addition to different combinations. Relevant parameters include accuracy, false positive and false negative rates, processing time, and scalability and are benchmarked against one another. The SHA-3 Merkle Tree + CNN + LSTM + Attention comprehensive model gained the highest accuracy at 97.8%, scalability at 92.5%, false positive at 2.7%, and false negative at 2.3%. Also, this achieved the quickest processing time, that is 4.3ms. Hence, it reflects the fact that by putting all together in the integrated architecture, it was possible to improve performance extensively and this was what made the model effective and efficient.

5. CONCLUSION

The framework proposed here uses SHA-3 Merkle Tree and CNN-LSTM hybrid models in order to achieve excellent performance classification of insider threats, as well as the safe transfer of cookie files. It attains a high accuracy of 97.8%, with reduced false positives and negatives as well as fast processing time, thereby turning this data transfer into a model with robust integrity. This characteristic makes the model scale up and increase real practical use in the environment. Future improvements will include the extension of the framework to handle dynamic insider threat scenarios using real-time adaptive learning, federated learning for privacy-preserving computations, and quantum-resistant cryptographic techniques for security in emerging post-quantum computational landscapes.

REFERENCE:

1. Yalla, R. K. M. (2021). Cloud-based attribute-based encryption and big data for safeguarding financial data. International Journal of Engineering Research & Science & Technology, 17(4).
2. Alagarsundaram, P. (2022). SYMMETRIC KEY-BASED DUPLICABLE STORAGE PROOF FOR ENCRYPTED DATA IN CLOUD STORAGE ENVIRONMENTS: SETTING UP AN INTEGRITY AUDITING HEARING. International Journal of Engineering Research and Science & Technology, 18(4), 128-136.
3. Thirusubramanian, G. (2020). Machine learning-driven AI for financial fraud detection in IoT environments. International Journal of HRM and Organizational Behavior, 8(4).
4. Yalla, R. K. M. K. (2023). Innovative data management in cloud-based component applications: A dual approach with genetic algorithms and HEFT scheduling. International Journal of Engineering & Science Research, 13(1), 94-105.
5. Sitaraman., S., R. (2020). Optimizing Healthcare Data Streams Using Real-Time Big Data Analytics and AI Techniques. (2020). International Journal of Engineering Research and Science & Technology, 16(3), 9-22.
6. Yalla, R. K. M. (2021). Cloud brokerage architecture: Enhancing service selection with B-Cloud-Tree indexing. Journal Name, 9(2), 1-XX. ISSN: 9726-001X.
7. Alagarsundaram, P. (2019). Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing. (2019). International Journal of Information Technology and Computer Engineering, 7(2), 18-31.
8. Yalla, R. K. M., Yallamelli, A. R. G., & Mamidala, V. (2019). Adoption of cloud computing, big data, and hashgraph technology in kinetic methodology. [Journal Name], 7(3). ISSN 9726-001X.
9. Alagarsundaram, P. (2019). Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing. (2019). International Journal of Information Technology and Computer Engineering, 7(2), 18-31.
10. Ganesan, T. (2023). Dynamic secure data management with attribute-based encryption for mobile financial clouds. International Journal of Applied Science Engineering and Management, Vol 17, Issue 2, 2023
11. Alagarsundaram, P. (2021). Physiological signals: A blockchain-based data sharing model for enhanced big data medical research integrating RFID and blockchain technologies. Journal of Computer Science, 9(2), 12-32.
12. Yalla, R. K. M., Yallamelli, A. R. G., & Mamidala, V. (2022). A distributed computing approach to IoT data processing: Edge, Fog, and Cloud analytics framework. Journal of Distributed Computing, 10(1), 79-93.
13. Alagarsundaram, P. (2023). AI-powered data processing for advanced case investigation technology. Journal of Science and Technology, 8(8), 18-34.
14. Yalla, R. K. M., Yallamelli, A. R. G., & Mamidala, V. (2020). Comprehensive approach for mobile data security in cloud computing using RSA algorithm. Journal of Current Science & Humanities, 8(3), 13-33.
15. Alagarsundaram, P. (2023). A systematic literature review of the Elliptic Curve Cryptography (ECC) algorithm for encrypting data sharing in cloud computing. International Journal of Engineering & Science Research, 13(2), 1-16.
16. Yallamelli, A. R. G., Mamidala, V., Devarajan, M. V., Yalla, R. K. M. K., Ganesan, T., & Sambas, A. (2024). Dynamic mathematical hybridized modeling algorithm for e-commerce for order patching issue in the warehouse. Service Oriented Computing and Applications.

17. Thirusubramanian, G. (2021). Integrating artificial intelligence and cloud computing for the development of a smart education management platform: Design, implementation, and performance analysis. *International Journal of Engineering & Science Research*, 11(2), 73-91.
18. Sitaraman, S. R., Alagarsundaram, P., & Thanjaivadivel, M. (2024). AI-driven robotic automation and IoMT-based chronic kidney disease prediction utilizing attention-based LSTM and ANFIS. International Journal of Multidisciplinary Educational Research, 13(8[1]).
19. Sitaraman, S. R., Alagarsundaram, P., Nagarajan, H., Gollavilli, V. S. B. H., Gattupalli, K., & Jayanthi, S. (2024). Bi-directional LSTM with regressive dropout and generic fuzzy logic along with federated learning and Edge AI-enabled IoHT for predicting chronic kidney disease. International Journal of Engineering & Science Research, 14(4), 162-183.
20. Gaius Yallamelli, A. R., Mamidala, V., & Yalla, R. K. M. (2020). A cloud-based financial data modeling system using GBDT, ALBERT, and Firefly Algorithm optimization for high-dimensional generative topographic mapping. International Journal of Modern Electronics and Communication Engineering (IJMECE), 8(4).
21. Sitaraman, S. R., Alagarsundaram, P., Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., & Ajao, L. A. (2024). Advanced IoMT-enabled chronic kidney disease prediction leveraging robotic automation with autoencoder-LSTM and fuzzy cognitive maps. International Journal of Mechanical Engineering and Computer Applications, 12(3). https://zenodo.org/records/13998065
22. Mamidala, V., Yallamelli, A. R. G., & Yalla, R. K. M. (2022). Leveraging robotic process automation (RPA) for cost accounting and financial systems optimization—A case study of ABC Company. ISAR International Journal of Research in Engineering Technology, 7(6).
23. Alagarsundaram, P., Sitaraman, S. R., Gollavilli, V. S. B. H., Gattupalli, K., Nagarajan, H., & Adewole, K. S. (2024). Adaptive CNN-LSTM and neuro-fuzzy integration for edge AI and IoMT-enabled chronic kidney disease prediction. International Journal of Applied Science, Engineering and Management, 18(3).
24. Ganesan, T. (2022). Securing IoT business models: Quantitative identification of key nodes in elderly healthcare applications. *International Journal of Management Research & Review*, 12(3), 78-94.
25. L. Hussein, J. N. Kalshetty, V. Surya Bhavana Harish, P. Alagarsundaram and M. Soni, "Levy distribution-based Dung Beetle Optimization with Support Vector Machine for Sentiment Analysis of Social Media," 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Hassan, India, 2024, pp. 1-5, doi: 10.1109/IACIS61494.2024.10721877.
26. Sitaraman, S. R., Alagarsundaram, P., & Kumar, V. K. R. (2024). AI-driven skin lesion detection with CNN and Score-CAM: Enhancing explainability in IoMT platforms. Indo-American Journal of Pharmaceutical & Biological Sciences, 22(4).
27. Gollavilli, V. S. B. H., Gattupalli, K., Nagarajan, H., Alagarsundaram, P., & Sitaraman, S. R. (2023). Innovative cloud computing strategies for automotive supply chain data security and business intelligence. International Journal of Information Technology and Computational Engineering, 11(4).
28. Gaius Yallamelli, A. R., Mamidala, V., Devarajan, M. V., Yalla, R. K. M. K., Ganesan, T., & Sambas, A. (2024). Dynamic mathematical hybridized modeling algorithm for e-commerce for order patching issue in the warehouse. Service Oriented Computing and Applications, 2024.

29. Kodadi, S. (2020). Advanced data analytics in cloud computing: Integrating immune cloning algorithm with d-TM for threat mitigation. *International Journal of Advanced Research in Computer Science, 16*(2). ISSN 2319-5991.
30. Peddi, S. (2021). Analyzing threat models in vehicular cloud computing: Security and privacy challenges. *International Journal of Modern Electronics and Communication Engineering, 9*(4), 152. ISSN 2321-2152.
31. Devarajan, M. V. (2020). Improving security control in cloud computing for healthcare environments. *Journal of Science and Technology, 5*(6), 178–189.
32. Dondapati, K. (2020). Robust software testing for distributed systems using cloud infrastructure, automated fault injection, and XML scenarios. *International Journal of Computer Science Trends and Technology, 8*(2), 84. ISSN 2347–3657.
33. Alagarsundaram, P. (2020). Analyzing the covariance matrix approach for DDoS HTTP attack detection in cloud environments. *International Journal of Computer Science Trends and Technology, 8*(1), 29. ISSN 2347–3657.
34. Yallamelli, A. R. G. (2021). Improving cloud computing data security with the RSA algorithm. *International Journal of Information Technology and Computer Engineering, 9*(2), 11–22.
35. Al Hammadi, A. Y., Yeun, C. Y., Damiani, E., Yoo, P. D., Hu, J., Yeun, H. K., & Yim, M. S. (2021). Explainable artificial intelligence to evaluate industrial internal security using EEG signals in IoT framework. *Ad Hoc Networks*, *123*, 102641.
36. Gupta, S. K., Tripathi, M., & Grover, J. (2022). Hybrid optimization and deep learning based intrusion detection system. *Computers and Electrical Engineering*, *100*, 107876.
37. Gadde, S., Amutharaj, J., & Usha, S. (2023). A security model to protect the isolation of medical data in the cloud using hybrid cryptography. *Journal of Information Security and Applications*, *73*, 103412.
38. Gangadharaiah, S., & Shrinivasacharya, P. (2024). Secure and efficient public auditing system of user data using hybrid AES-ECC crypto system with Merkle hash tree in blockchain. *Multimedia Tools and Applications*, 1-20.
39. Nagarajan, H., Gollavilli, V. S. B. H., Gattupalli, K., Alagarsundaram, P., & Sitaraman, S. R. (2023). Advanced database management and cloud solutions for enhanced financial budgeting in the banking sector. International Journal of HRM and Organizational Behavior, 11(4).
40. Gaius Yallamelli, A., Mamidala, V., Yalla, R. K. M. K., Ganesan, T., & Devarajan, M. V. (2023). HybridEdge-AI and cloudlet-driven IoT framework for real-time healthcare. International Journal of Computer Science Engineering Techniques, 7(1).
41. Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., Alagarsundaram, P., & Sitaraman, S. R. (2023). Corporate synergy in healthcare CRM: Exploring cloud-based implementations and strategic market movements. International Journal of Engineering and Techniques, 9(4).
42. Alagarsundaram, P., Gattupalli, K., Gollavilli, V. S. B. H., Nagarajan, H., & Sitaraman, S. R. (2023). Integrating blockchain, AI, and machine learning for secure employee data management: Advanced control algorithms and sparse matrix techniques. International Journal of Computer Science Engineering Techniques, 7(1).
43. Thirusubramanian Ganesan,. (2023). HybridEdge-AI and Cloudlet-Driven IoT Framework for Real-Time Healthcare. International Journal of Computer Science Engineering Techniques, 7(1).
44. P. Chinnasamy, R. K. Ayyasamy, P. Alagarsundaram, S. Dhanasekaran, B. S. Kumar and A. Kiran, "Blockchain Enabled Privacy- Preserved Secure e-voting System for Smart Cities," 2024 International Conference on Science Technology Engineering and

Management (ICSTEM), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICSTEM61137.2024.10560826.

45. A. Hameed Shnain, K. Gattupalli, C. Nalini, P. Alagarsundaram and R. Patil, "Faster Recurrent Convolutional Neural Network with Edge Computing Based Malware Detection in Industrial Internet of Things," 2024 International Conference on Data Science and Network Security (ICDSNS), Tiptur, India, 2024, pp. 1-4, doi: 10.1109/ICDSNS62112.2024.10691195.
46. P. Alagarsundaram, S. K. Ramamoorthy, D. Mazumder, V. Malathy and M. Soni, "A Short-Term Load Forecasting model using Restricted Boltzmann Machines and Bi-directional Gated Recurrent Unit," 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON), Bengaluru, India, 2024, pp. 1-5, doi: 10.1109/NMITCON62075.2024.10699152.
47. Devarajan, M. V., Yallamelli, A. R. G., Kanta Yalla, R. K. M., Mamidala, V., Ganesan, T., & Sambas, A. (2025). An enhanced IoMT and blockchain-based heart disease monitoring system using BS-THA and OA-CNN. Transactions on Emerging Telecommunications Technologies. https://doi.org/10.1002/ett.70055
48. Devarajan, M. V., Yallamelli, A. R. G., Mamidala, V., Yalla, R. K. M. K., Ganesan, T., & Sambas, A. (2024). IoT-based enterprise information management system for cost control and enterprise job-shop scheduling problem. Service Oriented Computing and Applications.
49. Veerappermal Devarajan, M., Gaius Yallamelli, A. R., Mani Kanta Yalla, R. K., Mamidala, V., Ganesan, T., & Sambas, A. (2025). An enhanced IoMT and blockchain-based heart disease monitoring system using BS-THA and OA-CNN. Emerging Technologies in Telecommunication Systems, 10(2), 70055.
50. Devarajan, M. V., Yallamelli, A. R. G., Yalla, R. K. M. K., Mamidala, V., Ganesan, T., & Sambas, A. (2024). Attacks classification and data privacy protection in cloud-edge collaborative computing systems. International Journal of Parallel, Emergent and Distributed Systems, 23. https://doi.org/10.1080/17445760.2024.2417875
51. Veerappermal Devarajan, M., Yallamelli, A. R. G., Mamidala, V., Yalla, R. K. M. K., Ganesan, T., & Sambas, A. (2024). IoT-based enterprise information management system for cost control and enterprise job-shop scheduling problem. Service Oriented Computing and Applications.
52. Veerappermal Devarajan, M., Yallamelli, A. R. G., Kanta Yalla, R. K. M., Mamidala, V., Ganesan, T., & Sambas, A. (2024). Attacks classification and data privacy protection in cloud-edge collaborative computing systems. International Journal of Communication Systems, 37(11).
53. Ganesan, T., Al-Fatlawy, R. R., Srinath, S., Aluvala, S., & Kumar, R. L. (2024). Dynamic resource allocation-enabled distributed learning as a service for vehicular networks. Second International Conference on Data Science and Information System (ICDSIS), Hassan, India, 2024, pp. 1-4, doi: 10.1109/ICDSIS61070.2024.10594602.
54. Ganesan, T., Almusawi, M., Sudhakar, K., Sathishkumar, B. R., & Sudheer Kumar, K. (n.d.) (2024). Resource allocation and task scheduling in cloud computing using improved bat and modified social group optimization. IEEE.
55. Harikumar Nagarajan, Venkata Surya Bhavana Harish, Poovendran Alagarsundaram & Dr. Aceng Sambas"Data Analytics: Principles, Tools and Practices" (2024).