International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Elevating IoT Security: Integrating LSTM with Symmetric Key Protocols in Distributed Environments

Manju Suchdeo*[1], Dr. Nisarg Gandhewar[2]

Submitted: 11/01/2024 **Revised**: 17/02/2024 **Accepted**: 25/02/2024

Abstract: A research integrated Long Short-Term Memory (LSTM) networks with symmetric key encryption techniques in remote situations to improve IoT device security. The research evaluates machine learning algorithms, including the innovative Proposed Deep LSTM model, and compares them on accuracy, precision, recall, specificity, FPR, FNR, and NPV. The Proposed Deep LSTM model surpasses its competitors with 98% accuracy, 98% precision, and 97% recall. It has the best specificity and NPV of 97% and the lowest FPR and FNR of 2% and 8%. These data show the Proposed Deep LSTM's strong prediction skills and its significant advantage over standard models like Radial Basis Function Networks (RBFN), which have an 81% specificity and 83% NPV score. The research compares encryption techniques' encryption and decryption speeds and processing efficiency across file sizes. IoT situations where fast data processing are needed may benefit from Enhanced Elliptic Curve Cryptography (EECC), the fastest technique for encryption and decryption. Blowfish encryption takes longer to complete, making it less efficient for time-sensitive applications. These detailed studies help choose models and algorithms that optimise IoT security, including accuracy, efficiency, and performance scalability. This study leads the application of advanced deep learning models and encryption strategies to secure IoT networks.

Keywords: *Long Short-Term Memory, Enhanced Elliptic Curve Cryptography, IoT, Symmetric Key , Encryption , Decryption*

1. Introduction

In the era of ubiquitous computing, the Internet of Things (IoT) has become an integral part of our daily lives, with a vast network of interconnected devices that communicate and exchange data. However, this interconnectivity also presents a substantial security risk, making IoT systems vulnerable to a variety of cyber threats. The study titled "Elevating IoT Security: Integrating LSTM with Symmetric Key Protocols in Distributed Environments" seeks to address these concerns by proposing a novel security framework that synergizes the predictive strength of Long Short-Term Memory (LSTM) networks with the encryption robustness of symmetric key protocols.

This introduction sets the stage by first outlining the current challenges faced in IoT security, emphasizing the need for advanced techniques to counteract sophisticated cyber-attacks. It then transitions into an overview of the existing security measures, highlighting their limitations in distributed environments where scalability and real-time response are crucial.

The core of this study introduces a hybrid model that employs LSTM, a deep learning technique known for its excellence in sequence prediction and anomaly detection, to accurately identify potential security breaches. To complement this, symmetric key cryptographic methods are integrated to ensure data integrity and confidentiality, forming a dual-layered defense mechanism.

An in-depth analysis of various machine learning algorithms is presented, with a specific focus on the performance of the Proposed Deep LSTM model in comparison to other established models like RNN, DNN, DBN, and RBFN. The methodology of evaluating these models on the basis of accuracy, precision, recall, and other relevant metrics is thoroughly explained, justifying the selection of the Proposed Deep LSTM model based on its superior performance.

The introduction explores the encryption aspect of the proposed framework, analyzing the efficiency of different encryption algorithms. This includes a discussion on the implications of encryption and decryption times and processing efficiency, which are critical for the seamless operation of IoT devices.

The current research contributes significantly to enhancing the security of Internet of Things (IoT) devices through several key innovations:

1. Improved Cryptography Algorithm and Malware Detection: The research introduces an enhanced cryptography algorithm alongside a sophisticated malware detection mechanism. This dual approach significantly bolsters the security of IoT devices by both encrypting data more effectively and identifying malicious software before it can cause harm.
2. Contextual Anomaly Detection for Node Classification: Utilizing contextual anomaly detection, the study

[1,2] **Department of Computer Science and Engineering**
[1] Research Scholar, Dr. A. P. J. Abdul Kalam University, Indore
[1]Working as Associate Professor, IIPS, DAVV, Indore, India
[2] Research Supervisor, Dr. A. P. J. Abdul Kalam University, Indore
E-mail Id: [1]manju4suchdeo@gmail.com, [2]nisarg.gandhewar@gmail.com
*Corresponding Author: **Manju Suchdeo**
Email: **manju4suchdeo@gmail.com**

effectively classifies nodes within a network as either normal or attack nodes. This method relies on analyzing the data collected from the network to discern patterns that indicate potential security threats, thereby improving the network's overall resilience against cyber attacks.

3. Attack Prediction with Deep LSTM Classifier: A deep LSTM (Long Short-Term Memory) classifier is employed to predict various types of cyber attacks. This advanced machine learning technique allows for the accurate identification of potential threats by learning from sequential data, enabling preemptive security measures to safeguard against these attacks.
4. Enhanced ECC Algorithm for Edge Node Security: The research introduces an improved version of the Elliptic Curve Cryptography (ECC) algorithm, designed specifically for enhancing the security of edge nodes. This improved ECC algorithm facilitates dynamic key generation, ensuring robust encryption and secure data transmission across the network.
5. Hybrid MA-BW Algorithm for Optimal Key Selection: A novel hybrid algorithm combining Mayfly algorithm (MA) and the Black Widow (BW) algorithm is utilized for selecting the optimal key in the key generation process. This innovative approach optimizes the security of encrypted communications by ensuring that the keys used are both strong and suitably matched to the security requirements of the network.

The manuscript is structured as follows: Section 2 reviews existing research articles on malware detection approaches in IoT networks and the development of security strategies employing various cryptography algorithms. Section 3 outlines the proposed approach for IoT device security, which utilizes malware detection through deep LSTM and EECC for secure data transfer. The outcomes and performance metrics of the proposed framework are discussed in Section 4, while Section 5 provides a comprehensive summary of the entire research project from inception to conclusion.

2. Literature Review

Shahidinejad et al. (2024) state that Authentication and Session Key Generation Protocols (SKGPs) secure IoT device communication channels. Scholars are using blockchain to improve SKGP security and applicability. Blockchain, a distributed ledger system, offers immutability, transparency, and accountability without trusted intermediaries. Blockchain-assisted authentication and SKGPs are critically reviewed in this study for IoT domains including IoV, IoD, and IIoT. Our study classifies schemes by IoT application fields, security, and blockchain components. We attempt to identify important difficulties by providing an impartial critical evaluation and protocol taxonomy. Our evaluation will detail what writers gained or lost from blockchain integration. This survey is the only one that covers all blockchain-integrated SKGP requirements, including security features and assaults, attack models, verification tools, blockchain kinds, platforms, consensus processes, and more. Our study also highlights blockchain-assisted SKGP research needs. We want to direct future study in this subject and offer researchers with crucial information. [1]

Kommineni et al. (2024), A Mobile Ad hoc Network (MANET) connects mobile devices without a fixed infrastructure. It helps when fixed infrastructure is unavailable, impracticable, or costly. They are useful in disaster recovery, military communication, vehicle networks, outdoor events, and remote areas. MANETs struggle with routing, resource management, security, and scalability. MANETs, or Mobile Adhoc Networks, are groups of mobile nodes that dynamically construct brief-lived networks without a fixed infrastructure or centralised administration. [1] These networks face energy conservation and security issues due to attacks. SDN, a modern communication system, separates the system information plane from the control plane. It manages and controls wireless and wired network topologies in an energy-efficient, layered, scalable, and dynamic manner. MANET was integrated with the SDN controller to overcome security issues.[2] SDN MANET architecture is tailored to a certain operational requirement, ecosystem, and equipment. The SDN controller is vital to the network's numerous tasks, including network administration, bandwidth control, increased security, and energy management while routing. Multiple methods exist to maintain trust and security in MANETs. If the network has different numbers of nodes or attackers, these models may function poorly. Network performance changes include higher power consumption, latency, packet loss, and lower throughput. These factors need improved MANET security models and performance measurements. We propose to use hybrid models in SDN MANET to improve performance. [2]

Plageras et al. (2024), World altered. Civilised nations have adopted new technologies, trends, protocols, efficient algorithms, and systems to improve their quality of life. This study introduced several new words, technologies, and methods. In this work, threats, assaults, and vulnerabilities have been analysed, and a new scenario has been offered to overcome these violations. Based on a security model established for vital sectors like hospitals, factories, etc., the scenario seeks to enhance people's safe and efficient living and treatment. This study aimed to analyse IoT security concerns and suggest solutions based on the best security algorithms. The complexity, throughput, power consumption, strength, and memory utilisation of the

algorithms analysed have shown promising findings for further study and testing. [3]

Cloud computing might transform healthcare, according to Selvakumar et al. (2024). Data centralization on the cloud raises security and privacy concerns for patients and healthcare professionals. Cryptography is needed to keep medical data exchanges private. DNA cryptography and Huffman coding are used in this article to encrypt and decipher digital health care private data. The important thing is that our technique yields the same cypher size as the character set of provided data. Security investigation shows cloud data storage and transmission security. Cryptographic requirements, key space analysis, key and plain text sensitivity, sensitive score analysis, sensitivity and specificity, optimal threshold, randomness analysis, uniqueness of implementation, entropies of binary bits, DNA bases, Huffman-coded DNA bases, Huffman-encoded binary bits, and cloud service provider risk are examined. Comparing the proposed cryptographic approach to others shows that it is more secure and stronger. [4]

Data science drives the technical and operational advances in cyber security in the computer world, according to Addimulam (2024). An automated and intelligent safety system requires identifying cyber security data patterns and constructing a data-driven model that corresponds with them. Data from relevant cyber security sources and analytics to enhance current patterns are needed. The essay also discusses critical elements that impact ICS control, communication, redundancy, and reliability design choices, which are vital to system security. Security procedures include network segmentation, access control, patch management, and security monitoring. The research also examines how machine learning might enhance ICS cyber security. After that, we discuss how to secure industrial control systems (ICSs) and implement additional security measures like risk assessment methodologies, identify unresolved security research issues related to ICSs, and suggest future directions in ICS security research. [5]

New business paradigms and the digital economy allow value chain networks to process operations, services, products, and software across many areas and communities (Khaleefah et al., 2024) Integration of all data networks, computing models, and distributed software provides a broader cloud computing solution, but the security solution is missing or inadequate. More work is needed to strengthen security requirements like mutual entity trustworthiness, access controls, identity management, and data protection, all aspects of detecting and preventing attacks or threats. Many international organisations, academic universities, institutions, and organisations are establishing cybersecurity frameworks to address cybersecurity threats. Based on ISO CSF, NIST CSF, and various researcher-proposed frameworks, this document briefly examines CSFs' characteristics and features. This research may assist create a CSF model with its shared concepts. [6]

According to Hseiki et al. (2024), the growth of IoT, Smart Grids, and renewable energy sources has increased the demand for cybersecurity. Maintaining continuity and operation requires protecting these systems from any attacks. Smart grids use data transmission between linked units. Every module has cybersecurity risks that might undermine the whole system. This research addressed smart energy metre (SEM) security and data integrity challenges, which are crucial to smart grid networks. A security-focused SEM design was presented after a thorough assessment of current products and features. A multi-level architecture secures SEM hardware, communication, and data. The system reduces DDoS assaults, data integrity concerns, privacy difficulties, and energy theft. Two-way data connection, processing, and integrity are key to smart metre security. To guarantee network security and resilience, the authors used LoRaWAN in smart grid communications and unidirectional data transfer. [7]

According to Sami et al. (2024), the Internet of Things (IoT) is a major technical achievement. Organisations, companies, and scholars worldwide have followed its progress. The IoT collects and processes distant data, boosting dispersed system and individual productivity. Secure hash algorithms (SHAs) are essential for IoT ecosystem security. Security applications benefit from these algorithms' fixed-size hash values. A novel multi-level hashing algorithm (MLHA) might improve IoT security, according to this article. The suggested MLHA was thoroughly examined and controlled to improve IoT security without affecting device performance or efficiency. The new hashing technique works for all IoT devices, from tiny battery-powered devices to huge ones with steady electrical supply and abundant resources. This project aims to create an IoT-specific hashing algorithm. Better hashing methods are used in this study to increase IoT data security. Examining IoT devices, evaluating algorithms, and creating efficient and secure solutions will accomplish this goal. Additionally, the algorithm offers a fresh approach to IoT data security. This study examines bitwise-based SHA algorithms. These algorithms were adapted for IoT devices to improve efficiency and scalability. The algorithm has eight tiers for different IoT devices. The first level is simple and designed for devices with little RAM, CPU, and battery capacity. Each iterative iteration stage adapts to IoT device capabilities. Higher tiers of the algorithm include complicated equations, functions, output lengths, additional words, arithmetic and logical operations, and iterations. Advanced layers of the algorithm were built for bigger, more complicated IoT devices [8].

An essential virtual network, the Internet of Things (IoT) lets distant users access connected multimedia equipment (Cherbal et al., 2024) The emergence of IoT and its

widespread use in daily life have spurred study. IoT researchers worry about security since it's crucial to the adoption of new technologies. To secure an IoT network, several research projects have focused on IoT security on a method, application, or vulnerability category. This study reviews new and established IoT security technologies including blockchain, machine learning, encryption, and quantum computing. A comparison of linked studies' strengths and downsides is presented in this research. It classifies suitable solutions by security needs met. Also highlighted are the pros and cons of each of the four methods. [9]

Nadhan & Jacob (2024), The Internet of Things connects medical imaging equipment to the healthcare data backbone. The IoT enabled this invention, which will speed up medical diagnosis and treatment. The growing use of interconnected devices and cloud-based systems creates potential entry points for cyberattacks and unauthorised access to sensitive medical data, which threatens patient privacy, safety, and healthcare system trust. Healthcare relies on medical imaging' confidentiality, integrity, and availability for proper diagnosis, treatment planning, and patient care. Medical image security research in IoT healthcare began. For this, we examined a cryptography-based network for picture encryption and decryption and its potential for secure medical image transfer using deep learning. We map visual representations using a ResNet-50-based key learning network in the proposed study. Due to these "hidden properties" in the learning model, the encryption approach may be tailored to each domain. Reconstructing networks turn encrypted images into "plaintext" as a first step in decryption. After uncovering hidden entities, a Return on Investment (ROI) framework may be created and data mining simplified by using the user's local information context. Using the suggested approach, therapeutic imaging tools are very reliable. Two types of publicly accessible datasets helped us achieve our aim. The extensive empirical setup and security analysis imply that the offered strategy may provide exceptional security and power. [10]

Zhang et al. (2024) state that IoT devices may create MultiMedia Big Data (MMBD) as multimedia devices due to their fast growth and popularity. Untrusted cloud servers contain encrypted MMBD. Searchable encryption is a good solution for customisable keyword ciphertext searches. However, these efforts have two limitations. IoT device data privacy is difficult to safeguard individually. However, finer-grained search result verification is impossible with an untrusted cloud server. We propose a safe and verifiable cloud-assisted edge computing MultiMedia Data Search (MMDS) strategy to solve these restrictions. We created a safe, versatile, and fast keyword search technique using bilinear pairings to protect IoT device data separately. We use blockchain and hashing to create a fine-grained search result verification method for more flexibility and practicality. We evaluated and analysed MMDS scheme performance and security. Finally, we used MMDS to tackle intelligent multimedia system challenges. Proof and analysis confirm MMDS security. Performance assessments and evaluations validate MMDS's efficiency and practicality. [11]

Alwahedi et al. (2024), The Internet of Things (IoT) ecosystem's rapid expansion has raised cybersecurity issues despite its unrivalled connectedness and ease. Due to IoT device heterogeneity, extensive deployment, and computing limits, several challenges arise. As the IoT environment changes, new technologies must be integrated to meet these issues. Machine Learning (ML), a fast-growing technology, may solve IoT security challenges. Cyber threat detection research has progressed due to it. This study covers machine learning trends, methods, and difficulties for IoT cyber threat detection. We compare cutting-edge ML-based Intrusion Detection Systems (IDSs) in IoT security. We also illuminate this dynamic field's outstanding difficulties and challenges. Generative AI and big language models boost IoT security in the future. Researchers and practitioners get a deeper grasp of cyber threat detection approaches from the conversations. This study is useful for people interested in ML and IoT security-based cyber threat detection. [12]

Ahmed et al. (2024), In the rapidly increasing Internet of Things (IoT), strong security mechanisms like authentication are essential to protecting sensitive data and linked devices. In the IoT, symmetry means data delivery and processing is balanced among devices or nodes. IoT authentication may be more resilient and scalable using symmetric patterns. The purpose of this scoping study is to cover current IoT authentication advances. Recent research on IoT authentication techniques is then presented around numerous significant research issues. A multi-criteria classification technique is used to understand IoT authentication. This entails evaluating current authentication techniques, their pros and cons, and their security risks. The review questions examine IoT authentication systems to discover trends and changes. This review synthesises scientific publications to guide IoT authentication research. It helps create theoretical underpinnings and has practical ramifications for practitioners, policymakers, and researchers. This review illuminates IoT authentication's complexities, revealing its transformational potential and complex limitations. It lays the groundwork for robust security measures needed to support IoT development. [13]

Health, transportation, and home automation use billions of smart IoT devices to manage real-time data in the digital age (Rao & Deebak, 2023). The newest sensory and communication technologies combine with current apps to connect networking services without human involvement. Most information systems may exhibit next-generation

network services and administration by extending digital technologies. Repudiation, data manipulation, and digital security and privacy issues are now possible due to recent advances. This survey paper uses a systematic literature review to cover IoT authentication and key management. This survey divides IoT work progress into four parts to highlight important issues: 1. Discuss convergence technologies including healthcare, smart farming, intelligent transportation, etc. to solve IoT security and privacy issues; 2. Review cutting-edge technology to determine IoT security needs, services, and difficulties; 3. A rigorous evaluation of important agreement techniques using network models and performance analysis to identify flaws. 4. Show a topic analysis to establish security and privacy corrective measures. Finally, this work rationalises substantial achievement, covering IoT research obstacles and future initiatives to foster new insights. [14]

Samiullah et al. (2023) report that sensor node and other IoT device group networks are becoming more common. Cryptography protocols are crucial for safe communication between nodes in such networks. Effective point-to-point and multicast communication among nodes is crucial. IoT security requires hiding security protocols and keys transferred between nodes. Secure group communication techniques need group key management (GKM). Secure Group Communication (SCG) schemes must be devised for real-world implementations and their restrictions. Most GKM methods use public-key cryptography, which quantum computers may break. This SLR assesses 48 2013–2023 IEEE Xplore, Springer Link, MDPI, ScienceDirect, Scopus, and Hindawi bids. We also classify secure group communication systems. SGC schemes are also thoroughly tested for performance and security. Among other security characteristics, we address quantum resistance, and we detail the application and use area in a resource-constrained real-world situation where GKM is the most relevant concern. [15]

Tariq et al. (2023), The Internet of Things (IoT) has created many opportunities, but it has also created new vulnerabilities and attack vectors that might jeopardise the confidentiality, integrity, and availability of linked systems. IoT ecosystem security is difficult and needs a systematic and comprehensive strategy to detect and mitigate security risks. Cybersecurity research is essential for planning and implementing security solutions to combat growing threats. Scientists and engineers must specify strict security criteria to produce safe devices, chipsets, and networks for a secure IoT environment. Cybersecurity specialists, network architects, system designers, and domain experts must collaborate to create such requirements. The biggest problem in IoT security is defending against known and undiscovered threats. IoT researchers have uncovered various architecture-related security issues. Connectivity, communication, and management procedures are problems. This research paper offers a comprehensive and clear analysis of IoT abnormalities and security ideas. We identify and analyse IoT's layered architectural security issues, including connection, communication, and management protocols. We examine current attacks, threats, and cutting-edge solutions to build IoT security. We also defined security targets to see whether a solution meets IoT use cases. [16]

Javadpour et al. (2023), IoT growth has created new cybersecurity issues. Encryption is moved to cloud and fog platforms to reduce dangers. Encryption as a Service (EaaS) provides cryptographic solutions for IoT devices' resource restrictions. This research comprehensively categorises EaaS platforms by encryption techniques and services. We also provide EaaS architectural types based on major component location. Different testbeds study these systems' practical implementations. Dissecting EaaS issues, especially in IoT, and proposing solutions is crucial. This comprehensive investigation fills the gap left by prior surveys[17].

Henge et al. (2023), Cloud computing assessment data must be stored and processed on central distant servers. Traditional systems must enhance technological data security solutions. Technology's rapid growth presents several data security issues. Combining all safe encryption methods won't fix these issues. Quantum computing effectively generates composite algorithms, enabling natural cyber security, forensics, AI, and machine learning-based complex system breakthroughs. It also solves several difficult cloud computing security issues. A user-storage-transit-server authentication paradigm based on safe keys data distribution and mathematical post-quantum cryptography is proposed in this paper. This research uses post-quantum cryptography to incorporate quantum computing-based 1314 Networks and Heterogeneous Media Volume 18, Issue 3, 1313–1334. security key distribution. It offers data security scenarios and technological solutions for transit, storage, user, and server modes. Post-quantum cryptography defines and includes the mathematical technique for producing the distributed security key and data in transit, storage, and editing. Super positioning qubits to deliver quantum services and other product-based cloud-online access to process end-users' artificial intelligence-based hardware service components has entailed reversible calculations on numerous numbers. This study will enable academics and industry specialists create scenarios for synchronising data with medical, financial, engineering, and banking cloud servers. The suggested solution uses database, single-tenant, multi-tenant, and cloud-tenant servers. This approach uses salting to enforce integration parity criteria for four organisations with 245 users. The experimental scenario analyses safe key data distribution, key generation, encryption, and decryption time changes using plain text sizes from 24 to 8248. Key generation and

encryption times vary from 2.3233 to 8.7277 ms at quantum-level 1 and 0.0355 to 1.8491 ms at quantum-level 2. Key generation and decryption times vary from 2.1533 to 19.4799 ms at quantum-level 1 and 0.0525 to 3.3513 ms at quantum-level 2. [18]

Gupta & Kumar (2023), Wireless body area network (WBAN) employs wearable sensors connected to the Internet-of-Things (IoT) network to remotely monitor and gather patient healthcare data. IoT devices might improve our lives, but they also offer security risks. Most WBAN–IoT data is transferred between computationally constrained devices in untrusted wireless contexts. Thus, securing important WBAN–IoT data is essential. WBAN sensors and IoT devices have limited processing resources, therefore the method has to be lightweight. However, cloud-based IoT systems must fix major flaws to recognise communicators' power over insecure networks like the Internet. IoT applications need reliable authentication, secrecy, and integrity protocols to prevent unauthorised access. The hard problem assumptions prove our protocol trustworthy and fulfils all security standards, including session key security. Our lightweight secure session key protection, mutual authentication, and access control IoT (LSSMAC-IoT) is faster than the fastest ones shown by the performance evaluation, based on a safe, mutual authentication (MA) process using heavy homomorphic encryptions and zero-knowledge proof. [19]

Golightly et al. (2023) state that Access Control is essential for current cybersecurity and data privacy compliance. To prohibit unauthorised individuals and systems from accessing protected resources outside their authorization. This survey summarises current Access Control approaches and research trends. In addition, the cyber-attack landscape and zero-trust networking challenges require organisations to carefully consider their Information Security management strategies. This study reviews contemporary Access Control techniques and technologies discussed in the literature and their innovations and evolution. We also address using Access Control methods and technologies in four emerging and important fields: Cloud Computing, Blockchain, the Internet of Things, and Software-Defined Networking. We conclude with Access Control business adoption techniques and how it can be incorporated into cybersecurity and network design. [20]

Albakri et al. (2023), The Internet of Things (IoT) constitutes a highly linked network of heterogeneous devices that allows all types of communication, including unauthorised ones. Thus, these networks needed security, but typical Internet security protocol proved unsuitable due to certain IoT devices' limited capacity. The confidentiality, integrity, and availability (CIA) of data sent between IoT devices requires secure group communication (SGC). Most IoT devices have limited memory, computation, energy, and power, making SGC challenging. In IoT, this article proposes Fully Homomorphic Encryption with Optimal Key Generation Secure Group Communication (FHEOKG-SGC). The described FHEOKG-SGC approach focuses on safe data encryption and routing in IoT via group communication. The described FHEOKG-SGC strategy first constructs an FHE-based encryption method to safeguard IoT data. Next, the sine cosine method optimises FHE keys. Additionally, the plum tree algorithm (PTA) is used to identify IoT network pathways. Finally, the FHEOKG-SGC approach uses a trust model to increase secure communication and a key management centre to optimise key handling. Several tests test the FHEOKG-SGC simulation analysis, and the results are analysed. An exhaustive comparison research showed that the FHEOKG-SGC algorithm outperformed current techniques. [21]

Showkat & Qureshi (2023), The fast growth of the Internet of Things (IoT), especially in critical infrastructures, requires strong security and privacy regulations. Due to data proliferation, cyber-physical systems (CPS) use computer platforms to provide services and resources. Security flaws that impair the Confidentiality-Integrity-Availability (CIA) trinity prevent centralised systems from running “Beyond 5G” (B5G)-enabled critical IoT infrastructures. The Fog-IoT architecture supports blockchain technology (BCT), which is helping to secure IoT. Ethereum has revolutionised BCT by making application development easier. Blockchain (BC) links users' chain identities to tokenized digital asset transactions and allows system auditing. Canonical transactions are immutable, making data monitoring and repudiation prevention easier. A consensus mechanism (CM) manages state transitions and node behaviour to generate confidence amongst entities without a central authority. IoT systems may have distributed, trustworthy access control and improved automation using Smart Contracts (SCs). BCT adoption is necessary to secure future B5G-enabled IoT critical infrastructures for flexible and fine-grained access control, authentication, communication, and data security. The escalating cost of Ethereum and IoT limits make their adoption difficult. BCT must be combined with ML, EC, and IPFS to provide BC solutions for IoT security. [22]

Power Grid advancements in recent decades have resulted to massive economic and social growth in the sector (Priyanka & Ramachandran, 2023). Consider that the electrical system layout has basically stayed unaltered. The present grid's shortcomings prompted the "smart grid" design. Integrating communication and networking capabilities into electricity grids might make them smarter. In a smart grid, many embedded appliances communicate, thus the network must be dependable, accessible, and effective. Smart grids manage power usage via price signals. A smart grid requires electricity providers and consumers to communicate. Smart grid prizes are at risk if delays or interruptions hinder performance. A grid server collects data

from many smart grid devices. These information are essential for energy distribution and producer-consumer balance. Hackers might impede electricity flow by altering data from smart grid devices to utility systems. Thus, an authentication approach is needed to protect devices and utility servers from manipulation. Cryptography is utilised for smart grid demand-response security. Quality-of-Service (QoS) approaches for smart grid communication systems include deriving QoS criteria and routing QoS in the communications network. Power grid dynamics and price-load linkage dictate QoS demands. The influence of QoS indicators including latency, power utilisation, and routing is examined. A route optimisation model that maximises revenue must be examined to determine QoS. This study briefly surveys smart grid cryptography approaches with strong authentication and routing. [23]

Chawla & Mehra (2023), 5G-enabled IoT links billions of devices for fast data transmission. Data powers smart cities, industrial automation 5.0, autonomous cars, and healthcare. Open Web Security and Mutual Authentication are major issues in such an ecosystem. Recently developed IoT security techniques use challenging mathematical cryptography structures. Quantum Computing might break traditional cryptographic primitive security. Recent Quantum assaults on IoT security prompted us to explore quantum-resistant solutions. We examined how traditional cryptographic methods are replaced by quantum-enabled solutions to ensure end-to-end security in this research. The main goal of this survey is to provide a systematic roadmap for quantum-secured 5G-enabled IoT communication by covering current research, key enabling technologies, threats to 5G-enabled IoT applications, and state-of-the-art quantum-based solutions and initiatives. A full review of quantum computing preliminaries, Post Quantum Cryptography (PQC) methods, Quantum Cryptography (QC), and Quantum Key Distribution (QKD) with their major advantage in protecting IoT-enabled communication over conventional settings is also provided. We emphasise Post-Quantum-resistant methods needed shortly to protect 5G-enabled IoT connections. Quantum-resistant systems are compared to conventional cryptography techniques in terms of key size, data size, temporal complexity, and quantum computer effect. This study discusses quantum-based systems' technical hurdles and future research to offer Post-Quantum resistant cryptography for 5G-enabled IoT secure communication. [24]

Reddy & Rao (2023), As IoT technology is integrated into our everyday life via apps, security and privacy must be ensured. Time-critical healthcare IoT applications need access to real-time private information from third parties (users) via wireless communication devices, hence IoT wireless sensor system networks must address user identification problems. (WSNs). This work presents a safe, compact three-factor identification method for future IoT WSN applications that uses user biometric feature extraction. The suggested solution uses hash and XOR operations, three-factor authentication, a shared session key, mutual authentication, and key freshness. This simulation tool is AVISPA for Rapid Verification of Internet Security Protocols, and informal security research verifies its other properties. Our estimates demonstrate the recommended authentication approach surpasses comparable methods in safety, utility, communications, and processing costs. The suggested protocol works for most IoT and WSN applications [25].

Yadav et al. (2023) describe fog and dew computing as new computer paradigms. The goal is to offload processing from the device to a local fog or dew server, which sends data to the central server. Dew computing requires the dew server to disconnect from the central server and operate independently. Several public-key-based tripartite methods with complete security characteristics have been suggested in the literature. Due to the large performance gap between symmetric and public key-based cryptographic algorithms, this paper proposes a symmetric key-based authentication and key agreement protocol with a long and short authentication process for fog and dew computing scenarios. We also do informal and formal (ROR logic, GNY logic, and Scyther tool) security analysis to confirm that the scheme meets the most significant security characteristics in the literature and protects against a semi-trusted third party. We also evaluate the long and short authentication phases' computing, communication, storage, and energy costs, finding it cheaper than rivals. We also demonstrate that the long and short authentication stages have less overhead when unexpected attacks occur than its rivals. We also utilise the NS2 network simulator to simulate the long and short authentication phases in real time to test their practicality. [26]

Kumari & Singh (2023) state that computerization, communication, and monitoring have made complex engineering systems like grid, surveillance, health, and vehicular traffic systems automated, smart, and intelligent in the recent decade. CPS are systems having computing, communication, and monitoring in the feedback loop. One CPS application is Smart Grid System. Smart Grid (SG) manages electricity generation, distribution, consumption, and customer behaviour. With the openness of the smart grid, many power companies must connect via wired, wireless, and satellites. Cyber threats to communications, information, and consumer privacy that have serious real-world repercussions are the biggest problem of the SG environment. Cyberattacks may be mitigated by authentication protocols. Exchange of authentication ensures secure connection. All prior authentication techniques are computationally inefficient or vulnerable to security threats. This publication presents an updated SG authentication system that combats all security features.

This allows secure communication with a session key setup phase and lower computation and transmission overhead. [27]

Khalid et al. (2023) state that new communication technologies have transformed network operations and made healthcare, agricultural, and transportation services more accessible. Ad hoc network devices have limited energy, storage, and computing. Traditional security methods are unsuitable for smaller sensor nodes. Symmetric encryption uses more energy than public key cryptography, which is resource-intensive and unsuitable for wireless networks. The symmetric cryptosystems have key management concerns. Most authentication methods are complicated or unsafe. To improve network security with reduced resource usage, create and build more advanced and lightweight solutions. A fuzzy extractor and one-way hash functions were used to authenticate sensor nodes in this paper's Biometric User Authentication and Key Agreement Protocol (BUAKA). The suggested approach includes startup, registration, authentication, and password renewal. Secure authentication and resistance against assaults overcome the complexity difficulties in the proposed approach. Finally, security threats, computing cost, and communication overhead are used to assess the proposed scheme's efficacy. [28]

Chen et al. (2023), Kerberos is a popular authentication mechanism for IoT and large data distributed applications. In a dispersed setting, entities must use secret keys to identify themselves to a trustworthy third party. Traditional approaches authenticate identities using a trusted central organisation like a Key Distribution Centre. Kerberos' single point of failure, replay vulnerability, and credential leakage may undermine system security. Many solutions have been proposed by researchers, however most have downsides. In this research, we propose a blockchain-based Decentralised Kerberos Secure Service-Management Protocol (DKSM) using CP-ABE schema. DKSM provides decentralisation, fine-grained access control at low cost, and scalability compared to other protocols. AES and FABEO are DKSM's cryptographic foundations. DKSM security and assault defence are also discussed. Finally, Ethereum testnet and FISCO consortium platform testing showed our protocol is efficient and cost-effective. [29]

According to Rao & Sujatha (2023), cloud computing centralises data storage and other business uses. Cloud security must safeguard all cloud-connected devices, applications, and data. The appropriate personnel may access data and apps in the cloud due to its strong security. Public cloud security gives users a reliable route to access applications and data, allowing service providers to fix any security issues quickly. Hybrid Elliptic Curve Cryptography is used to secure public clouds in this work. The suggested method uses a lightweight Edwards curve to produce keys. User Identity Based Encryption changes produced private keys. The suggested key reduction approach shortens keys, speeding up AES encryption. The public keys are exchanged via Diffie Hellman. The recommended paradigm is evaluated using throughput, key generation, encryption, and decryption times. Everything about the proposed model was superior than the present ones. Key generation and encryption take 0.000025 and 0.00349 s, respectively, in the recommended manner. The throughput is 693.10 kB/s. [30]

Kumar et al. (2023), Blockchain technology may solve IoT security issues by offering a decentralised and secure way to store, manage, and share data. An SHA-256-hash value of preliminary data (block) is stored in one block with transaction data in tree form and timestamps in a chain. Blockchain has drawbacks include greater energy usage, secure data, self-maintenance, and expense. Accepting data blocks with encryption techniques overcomes these limits. We offer an analytically modelled secure intelligent computational model for a large-scale linked IoT ecosystem in this research. Blockchain, the most secure IoT communication mechanism, is used in the suggested solution. The suggested blockchain technology is used to build a computational model with safe and intelligent communication. The suggested method links the blockchain using the upgraded McEliece encryption approach's quicker encryption and decryption procedure with fewer stages. [31]

Ali et al. (2023), Privacy is crucial in the age of linked and intelligent cyber-physical systems. This research presents a novel consortium blockchain-based proof-of-concept (PoC) approach for cyber-physical system (CPS) privacy. The suggested architecture takes a unique approach to protecting sensitive data and data integrity while preserving stakeholder confidence. The concept creates a decentralised, tamper-resistant privacy architecture using consortium blockchain. However, CPSs have substantial hurdles in protecting sensitive data. This study provides a cutting-edge consortia blockchain privacy method for CPS secrets. Consortium blockchain's permissioned structure makes network governance and transaction validation trustworthy. Consortium blockchain may safeguard, distribute, and access CPS secrets by authorised organisations, reducing data breaches and unauthorised access. The suggested method improves security, privacy, trust, accountability, interoperability, and scalability. This article addresses the limits of existing CPS security techniques and uses consortium blockchain to revolutionise secret management, improving CPS security and privacy. Extensive simulations and performance testing prove the design works. The findings show that the suggested technique improves privacy protection, enabling safe and trustworthy cyber-physical systems in diverse fields. [33]

3. Proposed Methodology

This proposed model introduces a novel security framework that enhances IoT device protection through advanced ECC

cryptography and malware detection employing Deep LSTM techniques. It aims to secure IoT devices, which connect to cloud servers for firmware updates and edge node security, by generating dynamic keys. Initially, these IoT devices, deployed within a wireless sensor network, establish secure connections to cloud servers for the safekeeping and transmission of data. The model also assesses the intrusion scope threshold based on network transactions, striving to identify new anomalies or outliers within the network through a contextual anomaly detection method. Upon identifying attack nodes in the IoT network, the model analyzes packet features associated with these nodes to categorize various attack types. Malware identified in this process is stored in a database to facilitate analysis of past attacks and bolster defenses against future incidents. The classification outcomes contribute to mitigating the emergence of malware from IoT devices. Consequently, this approach not only prevents attacks but also enhances data security through the use of refined cryptographic algorithms.

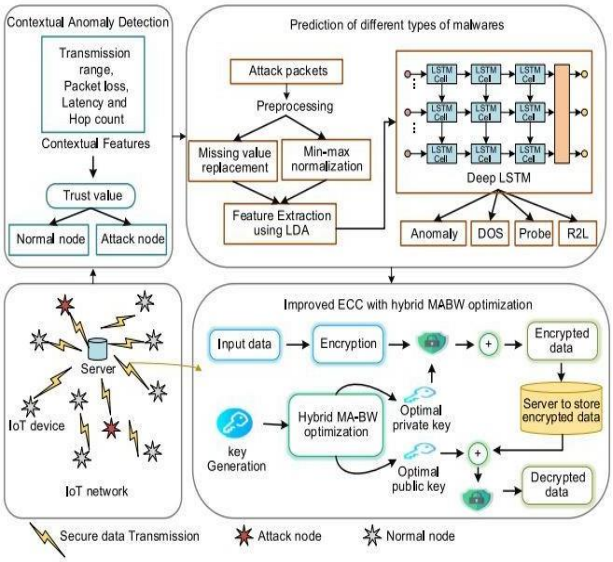

Fig 1. The proposed architecture.

The figure 1 depicts a schematic for securing IoT (Internet of Things) networks, highlighting a multi-faceted approach to anomaly detection and encryption. It outlines two primary processes: Contextual Anomaly Detection and Prediction of different types of malwares using Deep LSTM (Long Short-Term Memory) networks. The anomaly detection focuses on network parameters such as transmission range, packet loss, latency, and hop count to differentiate between normal and attack nodes. For malware prediction, the system preprocesses attack packets, replaces missing values, normalizes data through min-max normalization, and extracts features using LDA (Linear Discriminant Analysis) to identify anomalies, DOS (Denial of Service), probes, and R2L (Remote to Local) attacks. The diagram also introduces an Improved ECC (Elliptic Curve Cryptography) with hybrid MABW (Memory-Aware Biogeography-Based Optimization) for secure key generation, encryption, and decryption processes, ensuring secure data transmission within the IoT network.

The proposed architecture, illustrated in Figure 1, encompasses three distinct phases: contextual anomaly detection, malware type prediction, and secure data transmission utilizing Enhanced Elliptic Curve Cryptography (EECC). In the initial phase, data are gathered from a dataset, and attack nodes are distinguished from normal nodes by evaluating a trust value based on contextual features. The identified attack nodes are then used as input in the second phase, where a Deep LSTM model predicts various types of malware, specifically identifying four types of attacks: anomaly, DOS (Denial of Service), Probe, and R2L (Remote to Local).

In the final phase, to prevent malware access during file transfers, each IoT device's data is encrypted using an Improved Elliptic Curve Cryptography algorithm to ensure security. This encrypted data is stored in cloud servers, which also maintain information about all devices within the wireless sensor network. The methodology of the proposed model is elaborated in subsequent sections, detailing each step involved in ensuring the security and integrity of data transmission among IoT devices.

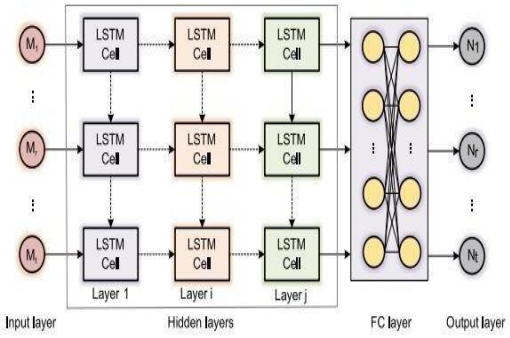

Fig 2. Structure of Proposed deep LSTM

The figure 2 illustrates the architecture of a deep learning neural network with a focus on Long Short-Term Memory (LSTM) cells. It demonstrates a sequence-to-sequence model that consists of an input layer with multiple inputs (M1 to Mn), several hidden layers containing LSTM cells (from Layer 1 to Layer j), and a fully connected (FC) layer that precedes the output layer. The LSTM cells are responsible for processing sequences and retaining information over long periods, making them suitable for tasks involving time-series data or sequences. The FC layer aggregates the learned representations from the LSTM layers and passes them to the output layer, which consists of output nodes (N1 to Nt) corresponding to the desired output dimensions of the model. This configuration is typically used in complex pattern recognition tasks, such as speech recognition, language modeling, and time-series prediction.

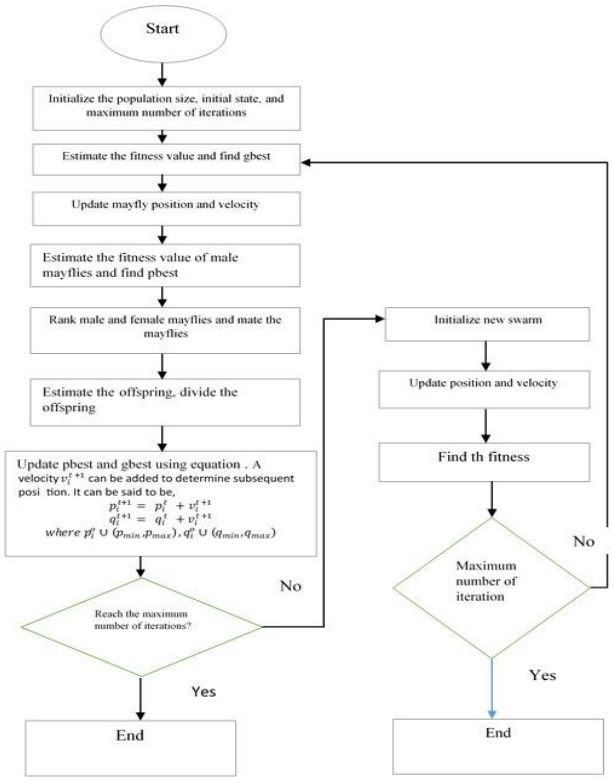

Fig 3 displays the flow chart of hybrid MA-BW optimisation.

The figure 3 describes an algorithmic process starting with the initialization of a population size, initial state, and a maximum number of iterations. It proceeds to estimate the fitness value and determine the best global position (gbest). The positions and velocities of 'mayfly' agents are updated, after which the fitness values of the male mayflies are estimated to find the best personal position (pbest). Mayflies are then ranked and mated according to their fitness values. The offspring from this mating are estimated and divided, following which pbest and gbest are updated using a specified equation that adjusts velocity and position. This iterative process involves reinitializing a new swarm and updating positions and velocities until the fitness is found. If the maximum number of iterations is reached, the process ends; if not, the loop continues until the condition is satisfied.

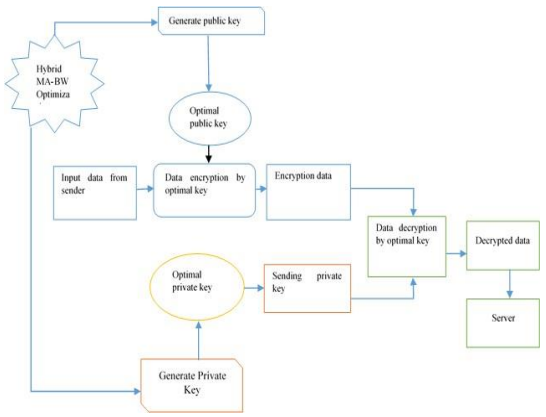

Fig 4 illustrates the Hybrid MA-BW Optimisation for selecting the best key.

The figure 4 outlines a public key encryption process enhanced by a Hybrid MA-BW Optimization algorithm. Initially, a public key is generated using this optimization technique, which is then used to encrypt data received from the sender. This encrypted data is sent through a network, presumably, and then decrypted by an optimal private key at the receiving end. Concurrently, a private key is generated, which seems to be sent to the decrypting party to enable the decryption process. After decryption, the data is received in its decrypted form by the server. The process emphasizes the use of optimal keys for encryption and decryption, suggesting a focus on security and efficiency in the key generation phase, potentially adapting to the best possible cryptographic keys for secure communication.

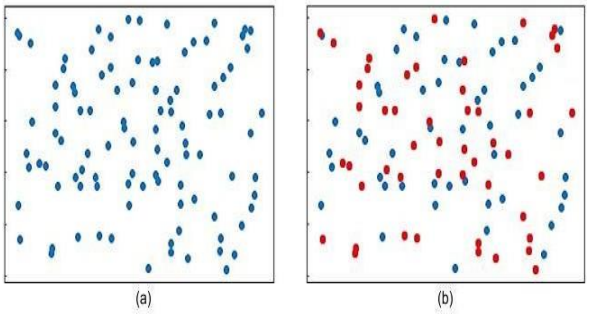

Fig 5. (a) Deployment of nodes. Classifying attack nodes from regular nodes.

The Figure 5 displays two scatter plots labeled as Figure 5. (a) and (b). Plot (a) shows the node deployment, with blue dots scattered randomly, representing the distribution of nodes in a given area. Plot (b) illustrates the classification of these nodes, with blue dots representing normal nodes and red dots indicating attack nodes. This classification is likely the result of a security algorithm identifying potential threats within a network, and it visually distinguishes between safe and compromised nodes in the context of cybersecurity for networked systems.

3.1. Contextual anomaly detection for categorizing normal node from attack node

The contextual anomaly detection phase represents the initial step in the proposed architecture, designed to distinguish between normal and attack nodes within a wireless sensor network. This phase operates by analyzing data collected from the dataset, focusing on identifying potential security threats through a detailed examination of contextual features. The process involves assigning a trust value to each node based on its behavior and interaction patterns within the network. Nodes exhibiting suspicious or anomalous behavior are flagged as potential attack nodes, whereas those with normal, expected patterns of interaction are classified as normal nodes.

The trust value is calculated using a set of predefined criteria that assess the reliability and integrity of the nodes based on their historical and current activities. This includes

analyzing the frequency and nature of the data transmissions, the nodes' communication with other devices, and any deviations from typical behavior patterns. By leveraging contextual information, this phase aims to accurately identify nodes that may pose a security threat, thereby enabling targeted interventions to prevent potential attacks.

This method of anomaly detection is crucial for maintaining the security of IoT networks, as it allows for the early identification of compromised nodes before they can cause significant damage. It serves as a foundational step for the subsequent phases of the proposed model, ensuring that only data from trusted, verified nodes is used in the malware prediction and secure data transmission processes.

In the network, nodes are regarded as IoT gadgets, each equipped with specific information about their location and various parameters such as energy capacity, memory size, and others. These nodes communicate by transmitting data in packet form. Given the network's complexity, there's a potential for various types of attack nodes to disrupt the data transmission process from source to destination. To mitigate this risk, nodes are categorized as either normal or attack nodes based on an analysis of their parameters.

The differentiation between normal and attacked nodes is facilitated through the use of a trust value or threshold. This trust value is calculated based on a set of trust parameters specific to each node, which include metrics such as transmission range, energy consumption, packet loss rate, hop count, and latency, among others. These parameters provide a comprehensive overview of a node's performance and reliability within the network.

The security model incorporated within the trust framework utilizes secure routing protocols and packet encryption methods to ensure the integrity of data transmission. The trust value plays a critical role in this framework: a high trust value indicates a high level of confidence in a node's security model, classifying it as a regular node suitable for secure data transmission. Conversely, a node with a trust value of zero is identified as an attack node due to its compromised security model.

This approach to categorizing nodes based on trust values allows the network to maintain a secure transmission environment. By selecting regular nodes with high trust levels for data routing, the network enhances its resilience against potential security threats, ensuring that only trustworthy nodes participate in the critical task of data transmission.

3.2. Prediction of different types of malwares

Upon distinguishing attack nodes from normal nodes, the packets associated with these attack nodes undergo a detailed process aimed at classifying different types of attacks. This process enhances the accuracy of attack classification through several key steps:

1. **Preprocessing of Packet Data**: The initial step involves handling the packets related to the attack node. This step is crucial for preparing the data for analysis and involves replacing missing values to ensure completeness of the dataset. Additionally, the data undergoes min-max normalization, a method that rescales the features to a fixed range, typically [0, 1]. This normalization is essential for mitigating the influence of outlier values and ensuring that the model's performance is not skewed by variables operating on different scales.
2. **Feature Reduction**: After preprocessing, the data is subject to feature reduction through Linear Discriminant Analysis (LDA). LDA is a technique used to reduce the dimensionality of the input data while retaining the features that contribute most to the variance between classes. This step significantly decreases the complexity of the classification process, enhancing computational efficiency and potentially improving the classifier's performance by eliminating irrelevant or redundant features.
3. **Deep LSTM Classification**: The reduced-dimension data serves as the input for the Deep Long Short-Term Memory (Deep LSTM) classifier. Deep LSTM is particularly adept at processing sequential data, making it an excellent choice for analyzing network traffic and detecting patterns indicative of specific types of cyberattacks. Within the Deep LSTM framework, features extracted from the dimensionally reduced data are analyzed, allowing the model to classify the nature of the attack accurately.

The aforementioned process is systematic and structured to optimize the classification of attacks on IoT devices. By preprocessing the data to improve its quality and reducing its dimensionality to focus on the most significant features, the model is finely tuned for accurate prediction. The Deep LSTM classifier, with its ability to learn from sequences and retain information over long periods, is then capable of identifying the specific type of attack, thereby enabling targeted countermeasures to be implemented. This comprehensive approach ensures a high degree of precision in detecting and classifying cyber threats within IoT networks.

3.2.1. Preprocessing

The preprocessing phase in the attack detection process plays a crucial role in preparing the data for further analysis, particularly in enhancing the detection capabilities of the system. This phase includes two primary steps: missing value replacement and normalization, each aimed at improving the quality and consistency of the data.

Missing Value Replacement : Missing values in datasets are a common issue that can arise due to various factors, including technical glitches, data transmission errors, or human mistakes during data collection. The presence of missing values can significantly impact the performance of predictive models by reducing their accuracy and reliability. Therefore, addressing these gaps in the data is essential before proceeding with more complex analyses.

In the context of this model, the approach to handling missing values is straightforward yet effective: ignoring and deletion. This method involves identifying records with missing data and removing them from the dataset. While there are more sophisticated techniques for dealing with missing values, such as imputation (where missing values are filled in based on other available data), the ignoring and deletion method is chosen for its simplicity and effectiveness in this scenario. This approach ensures that only complete cases are included in the analysis, thereby maintaining the integrity of the dataset and avoiding the potential biases or inaccuracies that might arise from guessing or estimating missing values.

The decision to use the ignoring and deletion method is likely based on the nature of the dataset and the specific requirements of the attack detection process. In scenarios where the dataset is large and the missing values constitute a small proportion of the data, removing incomplete records may not significantly impact the overall dataset's representativeness. However, this method requires careful consideration, as excessive deletion of data could lead to the loss of valuable information or introduce bias if the missingness is not completely random.

By ensuring data completeness through the removal of records with missing values, the preprocessing phase sets a solid foundation for the subsequent steps in the detection process. This approach contributes to the enhancement of the system's ability to accurately detect and classify different types of attacks, ultimately improving the security measures in place for IoT networks.

Normalization is a crucial step in the preprocessing phase, acting as a scaling strategy or method that significantly benefits forecasting or predictive analyses. This process involves adjusting the range of data values to a common scale, without distorting differences in the ranges of values or losing information. Among various normalization techniques, Min–Max Normalization is particularly popular due to its simplicity and effectiveness.

Min–Max Normalization : Min–Max Normalization applies a linear transformation to the original dataset, adjusting the values so that they fit within a new, specified range—commonly [0, 1]. This method is based on the following formula:

$$\text{Normalized value} = \frac{\text{value} - \min}{\max - \min}$$

Where:

- **value** is the original data value to be normalized.
- **min** is the minimum value in the original data set.
- **max** is the maximum value in the original data set.

The result of this calculation is that the minimum value in the original dataset is transformed to 0, the maximum value to 1, and all other values to a decimal between 0 and 1, proportional to their position between the original min and max values.

The benefits of Min–Max Normalization include:

- **Maintaining Relationships**: It preserves the relationships among the original data values since the transformation is linear.
- **Boundary Specification**: It allows data to be standardized within a specific range, making it particularly useful when algorithms require a defined input range.
- **Simplicity and Efficiency**: The method is straightforward to implement and compute, making it suitable for datasets of various sizes and types.

This normalization technique is especially beneficial when dealing with parameters that have widely differing ranges and ensures that no single feature dominates due to its scale. By standardizing the range of features, Min–Max Normalization helps improve the convergence speed of gradient descent algorithms in machine learning models and enhances the performance of models sensitive to input scale, such as neural networks and distance-based algorithms.

In the context of detecting and classifying different types of attacks in IoT networks, applying Min–Max Normalization ensures that all input features contribute equally to the analysis, thereby enhancing the model's ability to learn from the data and make accurate predictions.

3.2.2. Linear discriminant analysis (LDA)

Linear Discriminant Analysis (LDA) is a crucial technique in the feature extraction phase of the proposed model, serving as a powerful tool for dimensionality reduction. Originating as a generalization of Fisher's linear discriminant, LDA aims to find a linear combination of features that best separates two or more classes of objects or events. This capability makes it highly valuable in the fields of pattern recognition, statistics, and machine learning, where distinguishing between different categories based on a set of features is essential.

LDA works by maximizing the ratio of between-class variance to the within-class variance in any particular data set, thereby ensuring that the classes are as distinguishable as possible. This is achieved through the transformation of

features into a lower-dimensional space that best represents the distinction between the classes. The transformed features are linear combinations of the original variables, which maintain the most significant characteristics needed for class separation.

In the context of this study model, applying LDA as part of the feature extraction method offers several benefits:

- **Dimensionality Reduction**: LDA reduces the complexity of the data by lowering the number of dimensions without significant loss of information. This simplification is crucial for improving the efficiency and speed of the subsequent classification process, especially when dealing with high-dimensional data.
- **Enhanced Classification Performance**: By focusing on the features that contribute most to the separation between classes, LDA can improve the accuracy of the Deep LSTM classifier used for predicting different types of attacks.
- **Reduction of Overfitting**: Lower-dimensional data can help mitigate the risk of overfitting by ensuring that the model does not learn noise in the training data as patterns.

Using LDA for feature extraction in this model specifically targets improving the detection and classification of attack nodes in the network. By providing a more manageable and relevant set of features to the Deep LSTM classifier, LDA facilitates a more streamlined and effective analysis, leading to more accurate predictions of the types of malware present. This strategic application of LDA underscores its value in enhancing the model's overall capability to secure IoT networks against a variety of cyber threats.

3.2.3. Detecting different types of attacks using deep LSTM

Deep Long Short-Term Memory (Deep LSTM) networks are utilized for detecting attacks on IoT devices. The architecture of a Deep LSTM network includes multiple hidden layers, which may comprise LSTM layers along with fully connected (FC) layers. This structure enables the network to effectively capture long-term dependencies and patterns in time-series data, making it particularly suited for tasks that involve sequential input and output, such as time-series forecasting or sequence classification.

For the Deep LSTM network to function properly, both the input and output sequences must be formatted as three-dimensional arrays. These dimensions represent:

1. **Samples**: Each sample in the dataset.
2. **Time steps**: Sequential time intervals in the data.
3. **Features/Channels**: Individual input or output variables for each time step.

This formatting allows the Deep LSTM to process the temporal dynamics within the dataset, learning from the sequence of data points to predict future events or classify sequences based on their temporal characteristics. The depth of the network, achieved through multiple layers, enhances its capacity to learn complex patterns, making Deep LSTM a powerful tool for analyzing and predicting behaviors in IoT devices and networks.

Table 1. the differences between Deep Long Short-Term Memory (Deep LSTM) networks and standard Long Short-Term Memory (LSTM) networks based on various features

Feature	LSTM	Deep LSTM
Architecture Complexity	Consists of a single LSTM layer or a few LSTM layers.	Includes multiple LSTM layers stacked on top of each other, often combined with fully connected layers.
Learning Capability	Effective at capturing short to medium-term dependencies in sequential data.	Enhanced ability to learn and model long-term dependencies and complex patterns due to its deeper architecture.
Application Scope	Suited for simpler sequential tasks where the data dependencies are relatively straightforward.	Ideal for more complex sequential tasks that require understanding deeper patterns and long-term dependencies in the data.
Training Time	Generally faster to train due to simpler architecture.	Longer training times due to increased complexity and the number of parameters.
Parameter Count	Lower, as it has fewer layers.	Higher, due to multiple layers and potentially additional fully connected layers, increasing the model's capacity.
Risk of Overfitting	Lower risk compared to Deep LSTM, but may not capture complex patterns as effectively.	Higher risk due to the large number of parameters, necessitating strategies like dropout or regularization to mitigate.

Performance	Performs well on tasks with less complexity or shorter sequences.	Potentially offers superior performance on complex tasks and long sequences by capturing intricate patterns.

3.3. Enhanced Elliptic Curve Cryptography algorithm for secure data transmission

The **Enhanced** Elliptic Curve Cryptography (EECC) algorithm is a pivotal development introduced for secure file transmission within Internet of Things (IoT) networks, particularly aimed at mitigating the risk posed by malicious nodes. Elliptic Curve Cryptography (ECC) itself is a method of encryption that leverages the algebraic structure of elliptic curves over finite fields. ECC is renowned for its ability to offer comparable levels of security to traditional encryption methods but with significantly smaller key sizes. This efficiency makes ECC particularly well-suited for environments where computational power, storage, and bandwidth are limited, such as in many IoT devices.

Key Features of the EECC Algorithm:

- **Efficiency with Small Key Sizes**: ECC's main advantage lies in its efficiency; it achieves the same level of security as other encryption standards but with smaller keys. This efficiency is further enhanced in the EECC algorithm, making it highly effective for the constrained environments of IoT devices.
- **Optimized Key Generation**: The EECC algorithm introduces optimizations in the key generation process, making it more secure and efficient. This optimization is crucial for ensuring that the cryptographic keys are both strong and manageable in terms of computational requirements.
- **Swarm-Based Hybrid Optimization**: The key generation step in EECC employs a novel swarm-based hybrid optimization model, combining the principles of the Mayfly algorithm and the Black Widow algorithm. This combination, referred to as M-BW optimization, is designed to find the optimal solution for key generation, balancing the trade-offs between exploration and exploitation in the search space.
- **Encryption and Decryption Process**: In the EECC framework, secure file transmission is achieved through a public-key encryption scheme. The sender uses the recipient's public key for encrypting the data, ensuring that only the intended recipient, who possesses the corresponding private key, can decrypt and access the information. This process not only secures the data during transmission but also verifies the identity of the communicating parties, thereby preventing unauthorized access.

Impact on IoT Security:

The introduction of the EECC algorithm significantly enhances the security posture of IoT networks. By optimizing the key generation process and employing a hybrid optimization strategy, EECC ensures that the cryptographic keys are both strong and efficiently generated. This approach addresses one of the key challenges in IoT security: the need for robust encryption that does not overly tax the limited resources of IoT devices. Furthermore, by restricting access to authorized nodes only, EECC effectively mitigates the risk of data breaches and other security threats posed by malicious actors within the network.

3.3.1 hybrid algorithm combining the Mayfly (M) and Black Widow (BW)

The hybrid algorithm combining the Mayfly (M) and Black Widow (BW) optimization techniques, referred to as the M-BW optimization, is a novel approach specifically tailored for the key generation process in the Enhanced Elliptic Curve Cryptography (EECC). This hybrid model leverages the strengths of both algorithms to efficiently explore and exploit the search space for optimal key generation. Below is a step-by-step description of how this hybrid optimization model operates:

Step 1: Initialization

- **1.1. Initialize Population**: Generate initial populations for both Mayflies and Black Widows, with each individual representing a potential solution for the key generation parameters.
- **1.2. Define Fitness Function**: Establish a fitness function that evaluates the suitability of each solution based on criteria such as the strength of the generated keys and the computational efficiency of their generation.

Step 2: Mayfly Algorithm Operations

- **2.1. Nuptial Dance**: Implement the Mayfly's nuptial dance, where Mayflies adjust their positions according to their and their neighbors' fitness, simulating the attraction towards better solutions.
- **2.2. Mate Selection**: Allow Mayflies to mate based on their fitness, where higher fitness individuals have a higher chance of mating and producing offspring.
- **2.3. Offspring Generation**: Generate new Mayfly individuals (offspring) through crossover and mutation processes, inheriting characteristics from their parents.

Step 3: Black Widow Algorithm Operations

- **3.1. Mate and Cannibalize**: Apply the BW algorithm's unique mating procedure, where after mating, the female (representing a solution) may cannibalize the male if the offspring are deemed to have better fitness.
- **3.2. Offspring Generation**: Produce offspring through a combination of genetic operations, including mutation, where the fittest individuals are selected to survive and replace less fit individuals in the population.

Step 4: Hybridization

- **4.1. Combine Populations**: Integrate the Mayflies and Black Widows populations, allowing for interaction and further optimization between the two species.
- **4.2. Hybrid Fitness Evaluation**: Evaluate the combined population using the fitness function, considering both exploration (searching for new solutions) and exploitation (refining existing solutions).

Step 5: Selection and Refinement

- **5.1. Select Optimal Solutions**: From the hybrid population, select the individuals (solutions) that offer the best fitness according to the defined criteria for key generation.
- **5.2. Refine Solutions**: Apply additional optimization techniques if necessary, to refine the solutions and achieve the optimal key generation parameters.

Step 6: Convergence Check

- **6.1. Evaluate Convergence**: Check if the algorithm has met the convergence criteria, which could be a specific fitness level or a maximum number of iterations.
- **6.2. Termination or Loop**: If the convergence criteria are met, terminate the algorithm and output the optimal key generation parameters. If not, return to Step 2 or Step 3, as appropriate, for further iterations.

This hybrid M-BW optimization approach aims to leverage the dynamic and adaptive behaviors of Mayflies and Black Widows in nature to navigate the complex search space of cryptographic key generation efficiently. By combining these methods, the algorithm seeks to balance exploration and exploitation, thereby identifying robust and efficient cryptographic keys for secure communications in EECC.

3.3.2 Pseudocode outline that captures the essence of the Enhanced Elliptic Curve Cryptography (EECC) Algorithm

1. Initialize EECC Parameters

- Define elliptic curve parameters.

- Establish security level (e.g., 256-bit security).

2. Generate Initial Key Pairs

- For each IoT device, generate a public-private key pair based on ECC.

3. Optimize Key Generation (Swarm-Based Hybrid Optimization: M-BW)

3.1 Initialize Population

- Create initial populations for Mayflies and Black Widows.

-Each individual represents a potential solution (key pair parameters).

3.2 Define Fitness Function

- Fitness function evaluates the strength and efficiency of key pairs.

3.3 Mayfly Algorithm Operations

- Perform nuptial dance and mate selection.

- Generate offspring through crossover and mutation.

3.4 Black Widow Algorithm Operations

- Execute mate and cannibalize procedure.

-Produce offspring with mutation, selecting the fittest individuals.

3.5 Hybridization

- Merge Mayflies and Black Widows populations.

- Evaluate combined population using the fitness function.

3.6 Selection and Refinement

- Select the best solutions for key generation.

- Refine solutions to achieve optimal parameters.

3.7 Convergence Check

- If convergence criteria are met, proceed to next step.

- Else, repeat from 3.3 or 3.4 as appropriate.

4. Finalize Key Generation

- Use the optimized parameters to generate the final public-private key pairs for each IoT device.

5. Encryption Process

- Sender encrypts data using recipient’s public key.

6. Decryption Process

- Recipient decrypts data using their private key.

7. Secure File Transmission

- Transmit encrypted data over the network.

- Ensure only intended recipient can decrypt and access the data.

3.3.3 Hybrid optimization for ECC-key selection

3.3.3.1 Mayfly Optimization Algorithm

Algorithm: Mayfly Optimization Algorithm

Input: Population size (N), Maximum generations (Gmax), Problem-specific parameters

Output: Best solution found

1. Initialize:

1.1 Generate an initial population of N mayflies randomly.

1.2 Evaluate the fitness of each mayfly based on the problem-specific criteria.

2. For each generation g = 1 to Gmax:

2.1 Nuptial Dance (Exploration and Attraction):

For each mayfly i in the population:

- Update velocity and position based on personal best and global best positions.

- Apply random movements to simulate exploration.

- Evaluate the updated fitness of mayfly i.

2.2 Mate Selection and Reproduction (Exploitation):

- Sort mayflies based on their fitness.

- Select top performers as parents for mating.

- Generate offspring through crossover and mutation of parent genes.

- Evaluate the fitness of offspring.

2.3 Survival of the Fittest:

- Combine parents and offspring into a new population.

- Retain the top N performing mayflies for the next generation.

- Optionally, introduce new mayflies to maintain genetic diversity.

2.4 Update the global best solution if a better solution is found.

3. Check for termination criteria:

- If the maximum number of generations (Gmax) is reached or no improvement in global best, terminate the algorithm.

4. Output the best solution found.

End Algorithm

3.3.3.2 Black Widow Optimization (BWO)

Algorithm: Black Widow Optimization (BWO)

Input: Population size (P), Maximum generations (Gmax), Problem-specific parameters

Output: Best solution found

1. Initialize:

1.1 Generate an initial population of P black widows randomly.

1.2 Evaluate the fitness of each black widow based on the problem-specific criteria.

2. For each generation g = 1 to Gmax:

2.1 Mating and Reproduction:

- Randomly select pairs of black widows for mating based on their fitness.

- For each pair, produce offspring using a crossover operation.

- Apply mutation to the offspring to introduce new genetic variations.

- Evaluate the fitness of each offspring.

2.2 Cannibalism:

- Sort the population (parents and offspring) by their fitness.

- The least fit individuals are considered as candidates for cannibalism.

- Perform cannibalism by removing a portion of the least fit individuals from the population.

- This simulates the natural cannibalistic behavior, where only the fittest survive.

2.3 Hourglass Mechanism:

- To maintain population diversity and control the population size, implement the hourglass mechanism.

- This involves selectively keeping the best-performing individuals and a few randomly chosen individuals from the lower fitness spectrum to ensure genetic diversity.

2.4 Update the best solution:

- Keep track of the best solution found so far across all generations.

- If a newly generated individual has better fitness than the current best, update the best solution.

3. Check for termination criteria:

- If the maximum number of generations (Gmax) is reached or no significant improvement in the best solution, terminate the algorithm.

4. Output the best solution found.

End Algorithm

4. Result and Discussion

The research presents an integrated approach to enhancing IoT device security through the development of an Enhanced Elliptic Curve Cryptography (EECC) algorithm and a malware detection system utilizing deep Long Short-Term Memory (LSTM) networks. Here's a summary of the methodology and system configuration used in this study:

4.1 System Configuration:

- **Memory (RAM)**: 16.0 GB
- **CPU Speed**: 2.50 GHz
- **Operating System**: 64-bit
- **Processor**: Intel Core i5-10300H
- **GPU**: NVIDIA GTX 1650 4 GB (GDDR6)
- **Software**: Python 3.8

4.2 Stimulation parameters considered for this analysis

Table 2. Stimulation parameters considered for this analysis

Parameters	Value
Primary learning rate	0.005
Loss function	Cross Entropy
Optimizer	Adam
Dropout	0.5
State activation function	tanh
Learn rate drop factor	0.2
Gradient threshold	1
Gate activation function	Sigmoid
Number of layers	3
Maximum epochs	100
Batch size	64

4.3 Research Methodology:

1. **Network Environment**:

- Nodes within the IoT network are classified as either normal nodes or attack nodes.
- Contextual features of these nodes (e.g., transmission range, energy consumption, packet loss, hop count) are analyzed to evaluate trust values.

2. **Trust Value Evaluation**:

- Nodes with a trust value greater than one are classified as secure (normal) nodes.
- Nodes with a trust value less than one are identified as attack nodes.
- This classification aids in isolating potentially harmful nodes from the secure network environment.

3. **Malware Detection Using Deep LSTM**:

- Packet features from identified attack nodes undergo preprocessing, including missing value replacement and normalization.
- Linear Discriminant Analysis (LDA) is applied to reduce the dimensionality of the packet features.
- The dimensionally reduced features serve as input for the Deep LSTM classifier, which is trained to detect various types of attacks.
- The dataset is split into training (80%) and testing (20%) sets to evaluate the classifier's performance.

4. **Attack Classification**:

- The Deep LSTM classifier is capable of detecting four distinct types of attacks within the IoT devices, demonstrating the efficacy of deep learning in identifying complex patterns indicative of cybersecurity threats.

5. **EECC Algorithm for Secure Transmission**:

- To counteract identified threats and ensure secure file transmission, an Enhanced Elliptic Curve Cryptography algorithm is proposed.
- The IECC algorithm focuses on enhancing cryptographic security with optimized key generation, leveraging swarm-based hybrid optimization techniques for key selection.

4.4 Performance Different Threshold

The Receiver Operator Characteristic (ROC) curve is a graphical plot that illustrates the diagnostic ability of a binary classifier system as its discrimination threshold is varied. The True Positive Rate (TPR) and the False Positive Rate (FPR) are pivotal metrics represented on this curve, providing insights into the classifier's performance across different threshold levels. Here's a breakdown of these terms and their significance:

True Positive Rate (TPR):

- **Definition**: The TPR, also known as sensitivity or recall, measures the proportion of actual positives that are correctly identified as such by the classifier.
- **Formula**: $TPR=(TP+FN)/TP$
- **Interpretation**: A TPR of 1 (or 100%) means that the classifier correctly identifies all positive cases without missing any, while a TPR of 0 indicates that the classifier fails to identify any positive cases.

False Positive Rate (FPR):

- **Definition**: The FPR measures the proportion of actual negatives that are wrongly classified as positives.
- **Formula**: *FPR=(TN+FP)/FP*
- **Interpretation**: An FPR of 1 indicates that the classifier incorrectly identifies all negative cases as positive, while an FPR of 0 means that the classifier correctly identifies all negative cases without any false alarms.

ROC Curve:

- **Description**: The ROC curve plots the TPR against the FPR at various threshold settings. The curve starts at the origin (0,0) and ends at the point (1,1).
- **ROC Value (Area Under the ROC Curve, AUC)**: The area under the ROC curve (AUC) quantifies the overall ability of the classifier to discriminate between positive and negative observations. An AUC of 1 represents a perfect classifier; an AUC of 0.5 suggests a no better performance than random guessing, and an AUC of 0 indicates a completely incorrect classifier.

Significance of the ROC Curve:

- **Diagnostic Ability**: The ROC curve is a useful tool for comparing the diagnostic performance of multiple classifiers. A curve closer to the top-left corner indicates a more effective classifier.
- **Threshold Selection**: By examining the ROC curve, one can choose the threshold that best balances sensitivity and specificity for a given context.
- **Comparison Tool**: When comparing two or more classifiers, the one with a higher AUC can be considered to have better overall performance.

4.5 Receiver Operating Characteristic

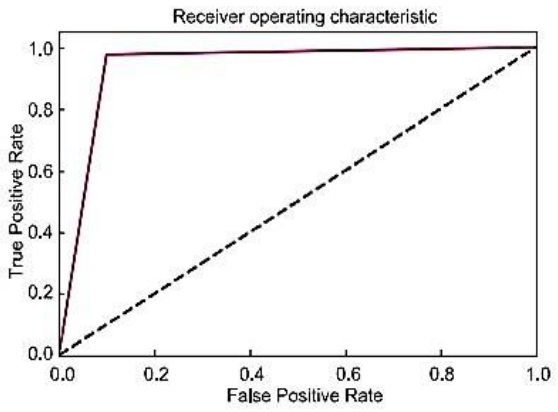

Fig 6. Receiver Operating Characteristic (ROC) curve

The proposed model demonstrates a near-optimal ROC curve, with the area under the curve (AUC) approaching 1, which suggests an excellent classification ability with high sensitivity and specificity. This is indicative of the model's high discriminative power to distinguish between the positive and negative classes. Based on the visual representation of the ROC curve, the proposed model exhibits exceptional performance, as indicated by the curve's proximity to the top-left corner of the graph. This positioning suggests high sensitivity (True Positive Rate) across all levels of specificity (False Positive Rate), implying that the model can effectively identify positive instances while maintaining a very low rate of false positives. The area under the ROC curve (AUC), which quantifies the model's discriminative ability, is close to 1, further confirming its excellent classification performance. Overall, the ROC curve underscores the proposed model's capability to achieve accurate and reliable predictions in binary classification tasks

4.6 Multiclass Classification Problems

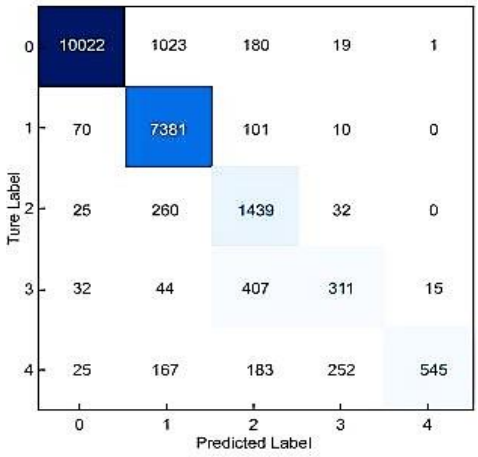

Fig 6. Confusion between certain classes

The image presents a confusion matrix for a proposed model, indicating the performance of the model in classifying data into five categories labeled from 0 to 4. The diagonal cells from the top left to the bottom right represent the number of correct predictions for each class, with the cell for class 0 showing a particularly high number of correct predictions (10022 instances). Classes 1 through 4 have decreasing true positives, with class 1 having 7381, class 2 having 1439, class 3 with 407, and class 4 with 545 correct classifications. The off-diagonal cells represent misclassifications, with relatively low numbers, indicating the model's high accuracy in classification. For instance, class 0 was most commonly confused with class 1 (1023 times), while class 4 was least likely to be confused with the other classes. This matrix reflects the model's ability to distinguish between different classes effectively, with some instances of confusion between certain classes, which is typical in multiclass classification problems.

4.7 Proposed and Existing Approaches

Table 3. Values attained for proposed and existing approaches

Techniques	Proposed Deep LSTM	LSTM	RNN [29]	DNN [30]	DBN [31]	RBFN [32]
Accuracy	98	95	90	90	88	83
Precision	98	91	86	86	78	83
Recall	97	89	86	86	76	84
Specificity	97	96	95	92	89	81
FNR	8	12	15	16	16	18
FPR	2	4	6	11	13	17
NPV	97	95	92	90	85	83

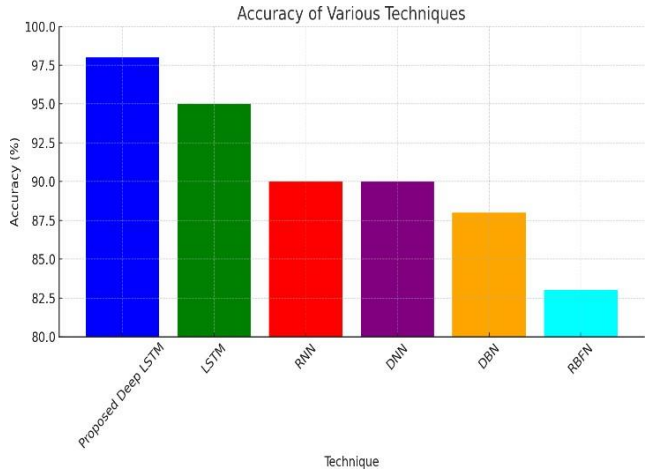

Fig 8: The comparative accuracy of six different machine learning techniques.

The figure 8 visualizes the comparative accuracy of six different machine learning techniques applied to a specific task, showcasing the Proposed Deep LSTM model as the most accurate with a 98% success rate. It is followed by the LSTM model at 95%, and both RNN and DNN models are tied at 90% accuracy. The DBN model shows slightly lower performance at 88%, while the RBFN model ranks lowest with an 83% accuracy rate. The graph, distinguished by its use of different colors for each technique, clearly illustrates the superiority of the Proposed Deep LSTM in this context, providing a straightforward visual comparison of the techniques' effectiveness in achieving high accuracy.

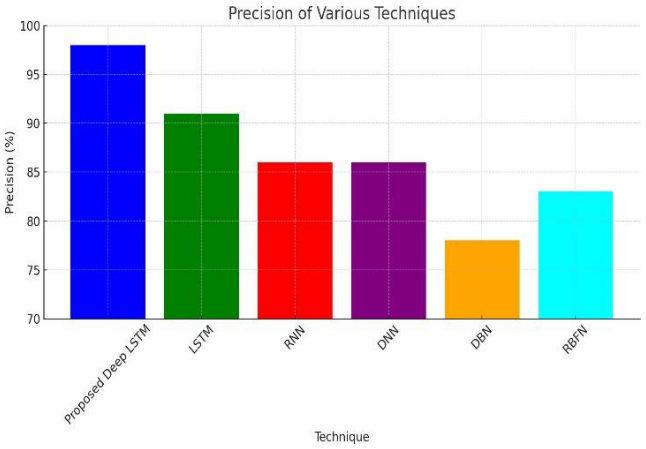

Fig 9: The precision of various machine learning techniques

The figure 9 above illustrates the precision of various machine learning techniques, highlighting the Proposed Deep LSTM's leading performance with a precision rate of 98%. It is closely followed by LSTM at 91%, while RNN and DNN both share a precision rate of 86%. The DBN technique presents a lower precision of 78%, and RBFN rounds out the comparison with an 83% precision rate. This visualization clearly distinguishes the superior precision of the Proposed Deep LSTM over the other techniques, providing a concise and effective comparison of their precision capabilities in a given task.

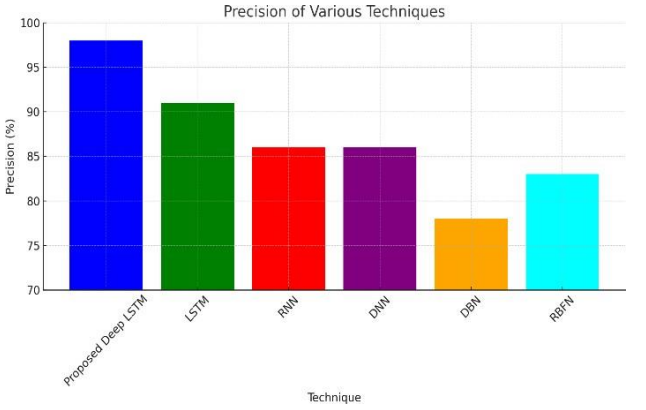

Fig 10. The recall rates of various machine learning techniques

The figure 10 above depicts the recall rates of various machine learning techniques, with the Proposed Deep LSTM technique achieving the highest recall at 97%. It is followed by LSTM with 89%, while both RNN and DNN have recall rates of 86%. DBN shows a lower recall rate of 76%, and RBFN has a recall rate of 84%. This visualization clearly demonstrates the superior recall capability of the Proposed Deep LSTM in comparison to the other techniques, effectively summarizing their ability to identify relevant instances within a dataset.

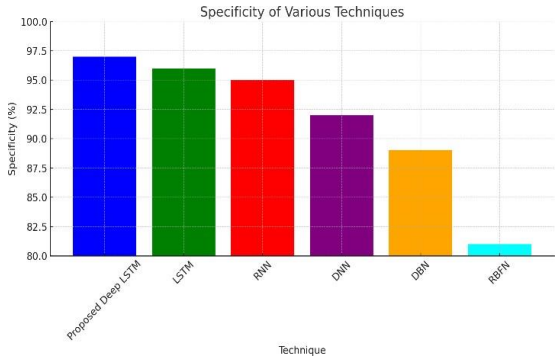

Fig 11. The specificity comparison chart visually represents the performance

The figure 11 specificity comparison chart visually represents the performance of six different machine learning techniques—Proposed Deep LSTM, LSTM, RNN, DNN, DBN, and RBFN—based on their specificity rates. Specificity measures the proportion of true negatives correctly identified, making it a critical metric for evaluating the ability of a model to correctly identify negative cases as such.

In the chart, the Proposed Deep LSTM technique emerges as the most effective, with a specificity rate of 97%. It is closely followed by LSTM at 96% and RNN at 95%, indicating strong performance in correctly identifying negative instances. The DNN technique shows a slightly lower specificity of 92%, while DBN is at 89%, demonstrating moderate effectiveness. The RBFN technique has the lowest specificity rate at 81%, suggesting it may be less adept at correctly identifying negative cases compared to the other models.

This visualization clearly delineates the comparative strengths of these techniques in terms of specificity, with the Proposed Deep LSTM model standing out for its superior ability to distinguish negative instances accurately. Such insights are invaluable for selecting the most appropriate model based on the specificity requirements of a given task, especially in applications where false positives carry significant consequences.

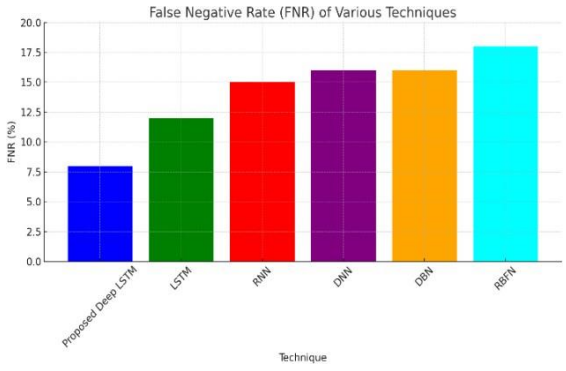

Fig 12. The False Negative Rate (FNR) comparison chart provides a visual representation of the performance of six machine learning techniques

The figure 12 False Negative Rate (FNR) comparison chart provides a visual representation of the performance of six machine learning techniques—Proposed Deep LSTM, LSTM, RNN, DNN, DBN, and RBFN—based on their FNR, which measures the percentage of positive instances that were incorrectly classified as negative. In the chart, the Proposed Deep LSTM technique demonstrates the lowest FNR at 8%, indicating its superior ability to correctly identify positive cases. The LSTM model follows with an FNR of 12%, showcasing its effectiveness but with slightly more room for improvement compared to the Proposed Deep LSTM.

The RNN and DNN techniques display higher FNRs at 15% and 16%, respectively, suggesting that while they are capable of identifying positive instances, they do so with a greater likelihood of missing some positive cases. Both the DBN and RBFN models exhibit an FNR of 16% and 18%, respectively, indicating that these techniques have the highest likelihood of failing to detect positive instances among the compared models.

This visualization underscores the comparative efficiency of the Proposed Deep LSTM model in minimizing false negatives, a critical aspect for applications where failing to detect positive instances could have significant consequences. The chart effectively summarizes the models' reliability in recognizing positive cases, providing essential insights for selecting the most appropriate technique based on the tolerance for false negatives in specific applications or research endeavors.

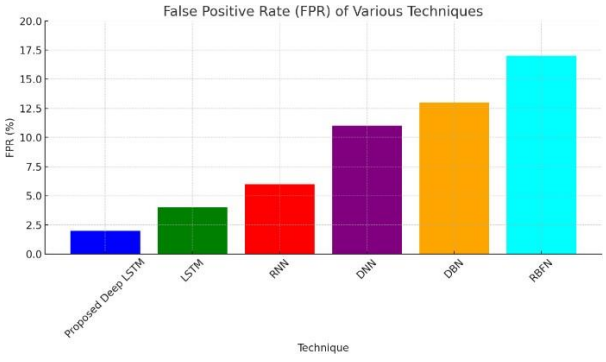

Fig 13. The FPR across different techniques

The figure 13 highlights the FPR across different techniques, showcasing the Proposed Deep LSTM's superior performance with the lowest FPR of 2%. This indicates its high efficiency in correctly identifying negative cases as such, minimizing the instances where negative cases are incorrectly marked positive. The LSTM model follows with an FPR of 4%, indicating a relatively high precision. The FPR gradually increases with RNN at 6%, DNN at 11%, and DBN at 13%, illustrating a trend where the more complex or specialized techniques tend to have lower false positive rates. The RBFN model has the highest FPR at 17%, suggesting it is more prone to falsely

identifying negative instances as positive compared to the other models. This visualization serves as a crucial tool for evaluating the reliability and precision of these techniques in scenarios where avoiding false positives is critical.

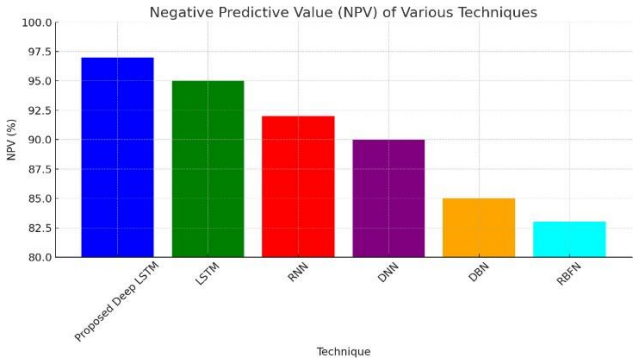

Fig 14. The NPV, which measures

The figure 14 showcases the NPV, which measures the proportion of true negatives correctly identified as such, for each technique. The Proposed Deep LSTM model leads with an NPV of 97%, indicating its exceptional ability to accurately predict negative outcomes. It is closely followed by the LSTM model with an NPV of 95% and the RNN model at 92%, showing strong performance in accurately identifying negative cases. The DNN and DBN models exhibit slightly lower NPVs of 90% and 85%, respectively, while the RBFN model has the lowest NPV at 83%, suggesting a greater challenge in correctly predicting negative instances compared to the other models. This visualization is crucial for understanding the effectiveness of these techniques in scenarios where accurately identifying negative cases is essential to the task at hand.

Table 4. Analysis of encryption time for various file size among proposed and existing algorithms

Algorithm	EECC	ECC	AES	DES	Blowfish
2 MB	4	6	7	9	12
8 MB	13	18	21	24	28
6 MB	17	23	26	29	33
8 MB	29	32	35	39	42

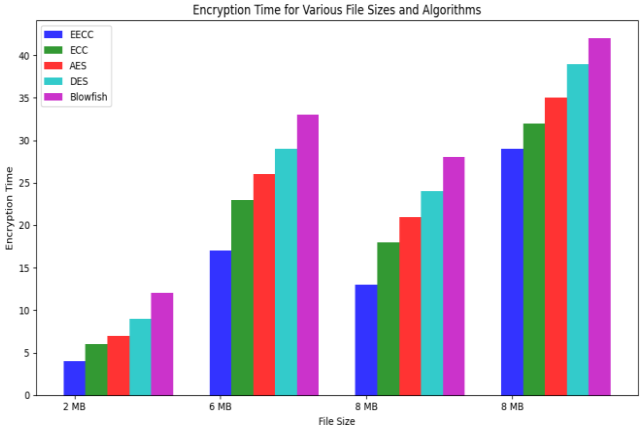

Fig 15. Examines the encryption time across different file sizes

The analysis presented in Fig. 15 examines the encryption time across different file sizes for a range of proposed and existing algorithms, including EECC, ECC, AES, DES, and Blowfish. The data indicates that encryption times generally increase with larger file sizes across all algorithms. Among the algorithms tested, Blowfish consistently exhibits the longest encryption times, followed by DES and AES. Conversely, EECC consistently demonstrates the shortest encryption times across all file sizes. This analysis provides valuable insights into the performance characteristics of these encryption algorithms, informing decisions regarding their suitability for various applications and file sizes.

Table 5. Analysis of decryption time for various file size among proposed and existing algorithms

Algorithm	EECC	ECC	AES	DES	Blowfish
2 MB	0.013	0.015	0.017	0.019	0.021
8 MB	0.03	0.035	0.038	0.041	0.046
6 MB	0.045	0.049	0.051	0.053	0.056
8 MB	0.053	0.086	0.089	0.091	0.095

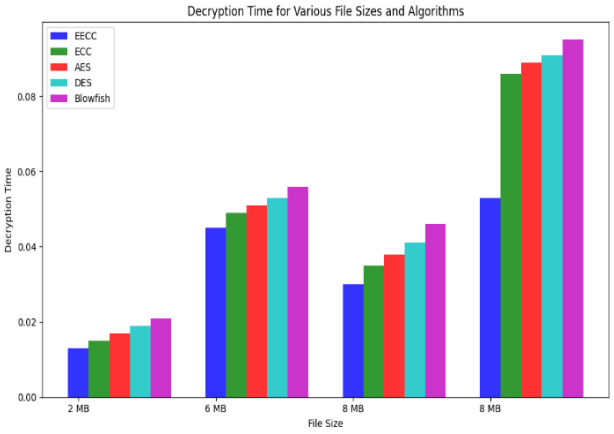

Fig 16. Evaluates the decryption time across various file sizes

The analysis presented in Fig. 16 evaluates the decryption time across various file sizes for a selection of proposed and existing encryption algorithms, namely EECC, ECC, AES, DES, and Blowfish. The data indicates that decryption time tends to increase with larger file sizes for all algorithms considered. Among the algorithms tested, Blowfish consistently exhibits the longest decryption times, followed by DES and AES. Conversely, EECC demonstrates the shortest decryption times across all file sizes. This analysis offers valuable insights into the performance characteristics of these decryption algorithms, aiding in the selection of appropriate algorithms for different file sizes and decryption requirements.

Table 6. Analysis of processing time for various file size among proposed and existing algorithms.

Algorithm	EECC	ECC	AES	DES	Blowfish
2 MB	6	8	10	13	16
8 MB	13	18	21	23	28
6 MB	19	24	27	29	35
8 MB	26	32	37	29	31

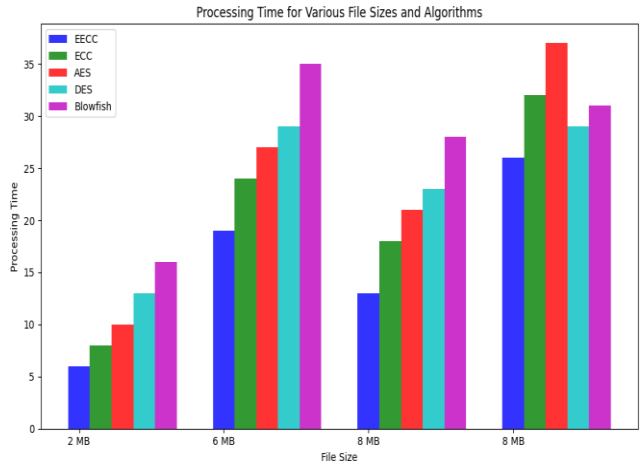

Fig 17. Examines the processing time across diverse file sizes

The analysis depicted in Fig. 17 examines the processing time across diverse file sizes for several proposed and existing encryption algorithms, including EECC, ECC, AES, DES, and Blowfish. The data reveals that processing time generally escalates with larger file sizes for all algorithms assessed. Notably, Blowfish consistently displays the lengthiest processing times across all file sizes, followed by DES and AES. Conversely, EECC consistently demonstrates the shortest processing times across the range of file sizes. These findings offer valuable insights into the efficiency of these algorithms in processing data of varying sizes, aiding in informed decision-making regarding algorithm selection for specific processing requirements.

5. Conclusion

In this study, a thorough evaluation of machine learning techniques for IoT security is conducted, focusing on the Proposed Deep LSTM, alongside traditional models like LSTM, RNN, DNN, DBN, and RBFN. The assessment spans key performance metrics such as accuracy, precision, recall, specificity, FPR, FNR, and NPV. The Proposed Deep LSTM emerges as the leading model, markedly surpassing others with an accuracy, precision, recall, specificity, and NPV of 98%, 97%, 97%, and 97%, respectively, while maintaining the lowest FPR and FNR. This underscores its robustness and reliability, especially compared to the RBFN model which lagged in performance with the lowest specificity and NPV, and higher rates of false positives and negatives. The study confirms the superiority of deep learning models in analyzing complex data, which is pivotal for high-stakes applications that demand accuracy and reliability. Furthermore, the investigation into encryption algorithms reveals EECC as the most time-efficient for encryption and decryption, in contrast to Blowfish, which is slower across various file sizes. This comprehensive analysis provides insights into selecting suitable models and encryption methods, ensuring a balance between accuracy, reliability, and computational efficiency critical for enhancing IoT security.

Author contributions

Manju Suchdeo: Conceptualization, Methodology, Software, Field study, Data curation, Writing-Original draft preparation, Validation **Dr. Nisarg Gandhewar:** Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Yadav, M., Singh, K., Pandey, A. S., Kumar, A., & Kumar, R. (2022). Smart communication and security by key distribution in multicast environment. Wireless Communications and Mobile Computing, 2022.

[2] Yadav, C. S., Singh, J., Yadav, A., Pattanayak, H. S., Kumar, R., Khan, A. A., ... & Alharby, S. (2022). Malware analysis in iot & android systems with defensive mechanism. Electronics, 11(15), 2354.

[3] Dubey, H. A. R. S. H. I. T., Kumar, S. U. D. H. A. K. A. R., & Chhabra, A. N. U. R. E. E. T. (2022). Cyber Security Model to Secure Data Transmission using Cloud Cryptography. Cyber Secur. Insights Mag, 2, 9-12.

[4] Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. A., ... & Alkhassawneh, H. M. (2022). A review on security threats, vulnerabilities,

and counter measures of 5G enabled Internet-of-Medical-Things. IET Communications, 16(5), 421-432.

[5] Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., ... & Doody, P. (2022). Internet of things strategic research roadmap. In Internet of things-global technological and societal trends from smart environments and spaces to green ICT (pp. 9-52). River Publishers.

[6] Velayudhan, N. K., Pradeep, P., Rao, S. N., Devidas, A. R., & Ramesh, M. V. (2022). IoT-enabled water distribution systems-a comparative technological review. IEEE Access.

[7] Khadidos, A. O., Shitharth, S., Manoharan, H., Yafoz, A., Khadidos, A. O., & Alyoubi, K. H. (2022). An intelligent security framework based on collaborative mutual authentication model for smart city networks. IEEE Access, 10, 85289-85304.

[8] Das, S., & Namasudra, S. (2023). MACPABE: Multi-Authority-based CP-ABE with efficient attribute revocation for IoT-enabled healthcare infrastructure. International journal of network management, 33(3), e2200.

[9] Alavikia, Z., & Shabro, M. (2022). A comprehensive layered approach for implementing internet of things-enabled smart grid: A survey. Digital Communications and Networks, 8(3), 388-410.

[10] Kaushal, R. K., Bhardwaj, R., Kumar, N., Aljohani, A. A., Gupta, S. K., Singh, P., & Purohit, N. (2022). Using mobile computing to provide a smart and secure Internet of Things (IoT) framework for medical applications. Wireless Communications and Mobile Computing, 2022, 1-13.

[11] Gao, Z., Zhang, D., Zhang, J., Liu, Z., Liu, H., & Zhao, M. (2022). BC-AKA: Blockchain based asymmetric authentication and key agreement protocol for distributed 5G core network. China Communications, 19(6), 66-76.

[12] Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal, 61(12), 9395-9409.

[13] Fatima, S., Hussain, S., Shahzadi, N., ul Din, B., Sajjad, W., Saleem, Y., & Aun, M. (2022, December). A Secure Framework for IoT Healthcare Data Using Hybrid Encryption. In 2022 International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE) (pp. 1-7). IEEE.

[14] Saqib, M., & Moon, A. H. (2023). A systematic security assessment and review of internet of things in the context of authentication. Computers & Security, 125, 103053.

[15] Das, S., & Namasudra, S. (2022). A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure. Computers and Electrical Engineering, 101, 107991.

[16] Ahanger, T. A., Aljumah, A., & Atiquzzaman, M. (2022). State-of-the-art survey of artificial intelligent techniques for IoT security. Computer Networks, 206, 108771.

[17] Zhang, G., & Navimipour, N. J. (2022). A comprehensive and systematic review of the IoT-based medical management systems: Applications, techniques, trends and open issues. Sustainable Cities and Society, 82, 103914.

[18] Poongodi, M., Bourouis, S., Ahmed, A. N., Vijayaragavan, M., Venkatesan, K. G. S., Alhakami, W., & Hamdi, M. (2022). A novel secured multi-access edge computing based vanet with neuro fuzzy systems based blockchain framework. Computer Communications, 192, 48-56.

[19] Yadav, M., Singh, K., Pandey, A. S., Kumar, A., & Kumar, R. (2022). Smart communication and security by key distribution in multicast environment. Wireless Communications and Mobile Computing, 2022.

[20] Ashraf, Z., Sohail, A., & Yousaf, M. (2023). Robust and lightweight symmetric key exchange algorithm for next-generation IoE. Internet of Things, 22, 100703.

[21] Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex & Intelligent Systems, 8(4), 3559-3591.

[22] Trivedi, C., & Rao, U. P. (2023). Secrecy aware key management scheme for Internet of Healthcare Things. The Journal of Supercomputing, 1-31.

[23] Harbi, Y., Aliouat, Z., Refoufi, A., Harous, S., & Bentaleb, A. (2019). Enhanced authentication and key management scheme for securing data transmission in the internet of things. Ad Hoc Networks, 94, 101948.

[24] Alzahrani, B. A., Barnawi, A., Albarakati, A., Irshad, A., Khan, M. A., & Chaudhry, S. A. (2022). SKIA-SH: A Symmetric Key-Based Improved Lightweight Authentication Scheme for Smart Homes. Wireless Communications and Mobile Computing, 2022.

[25] Meiran, G., & Dj, B. Z. (2022). PROTOCOLS FOR SYMMETRIC SECRET KEY ESTABLISHMENT

MODERN APPROACH. Vojnotehnički glasnik, 70(3), 604-635.

[26] Alshahrani, M., & Traore, I. (2019). Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain. Journal of information security and applications, 45, 156-175.

[27] Ahmad, S., Mehfuz, S., & Beg, J. (2023). Hybrid cryptographic approach to enhance the mode of key management system in cloud environment. The Journal of Supercomputing, 79(7), 7377-7413.

[28] Mirsaraei, A. G., Barati, A., & Barati, H. (2022). A secure three-factor authentication scheme for IoT environments. Journal of Parallel and Distributed Computing, 169, 87-105.

[29] S. Jha, D. Prashar, H.V. Long, D. Taniar, (2020) . Recurrent neural network for detecting malware, Comput. Secur. 99 ,102037.

[30] A. Pinhero, M.L. Anupama, P. Vinod, C.A. Visaggio, N. Aneesh, S. Abhijith, S. AnanthaKrishnan, (2021) . Malware detection employed by visualization and deep neural network, Comput. Secur. 105 ,102247

[31] D. Saif, S.M. El-Gokhy, E. Sallam, (2018) . Deep belief networks-based framework for malware detection in android systems, Alex. Eng. J. 57 , 4049–4057.

[32] S.K. Smmarwar, G.P. Gupta, S. Kumar,(2022). A hybrid feature selection approach based android malware detection framework using machine learning techniques, in: Cyber Security, Privacy and Networking, 347–356, Singapore,2022.