RESEARCHERID
THOMSON REUTERS
International Journal of Management, IT & Engineering
Vol. 8 Issue 12, December 2018,
ISSN: 2249-0558
Impact Factor: 7.119Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Scope of CNN based Optimization and Block Chain Mechanism in IoT Based Distributed Environment

Mr. C. Sathish, Assistant Professor, Department of Computer Science and Engineering, Government College of Engineering, Bodinayakanur, Tamil Nadu, India

sathishgcebodi@gmail.com

ABSTRACT: CNNs are referred to as "metaheuristic optimisation" because to their utilisation of meta-heuristic methodologies in their search for optimal solutions. Heuristic refers to a "solution" and "meta" indicates "higher level" in this sense, when both goal function and the optimum solution are resilient. Cryptography ensures the integrity of the connections between the blocks of data on a blockchain. Since blockchains are a new kind of distributed database that makes use of CNN, they stand apart from relational databases, the

Connecting blocks after their contents have been recorded ensures that information is included in subsequent blocks in the right chronological sequence. Although blockchain technology may store any kind of data, its most notable usage so far has been as a distributed transaction ledger. To safeguard "smart" objects from hackers, blockchain-infused IoT with CNN offers a transparent and practically unchangeable solution. IoT devices may communicate securely via the blockchain since it records data in transactions and checks them with nodes. This makes it possible to identify which sensors were responsible for collecting a certain data set. Current IoT protocols may be enhanced by including blockchain data encryption. It is possible to make Internet of Things apps more private and safe using blockchain technology and CNN. The study of multi-node computer networks is known as distributed computing. In a distributed computing environment, several computers may collaborate to provide quicker results. Dependability, scalability, transparency, performance, geo-distribution, sharing of resources, adaptability, etc. are only a few of the many reasons for its extensive use.

Keywords: Optimization, Blockchain, IoT, Distributed Environment, CNN

1. INTRODUCTION

CNN Model-based metaheuristic optimisation yields optimum solutions. Meta is "higher" and heuristic "solution." These issues may have numerous objectives. Strong goal functions offer best solutions. CNN model encrypts blockchain blocks. Distributed blockchains differ from databases. A block is updated. To keep order, entire blocks are connected to the preceding one. Blockchain can store any data, although it's mostly used for transactions. Blockchain-infused CNN-based IoT prevents "smart" items from hackers. IoT communication is safe with blockchain data storage and verification. IoT protocols benefit from blockchain encryption. A blockchain can safeguard IoT applications. Multiple-node distributed computing. Multiple computers accelerate distributed computing. Many benefits come from distributed systems [1].

1.1 OPTIMIZATION MECHANISM

Optimisation solves tough problems by maximising or minimising an objective function. A

"hard" or "complex" optimisation task cannot be solved in a set time using deterministic methods. Optimisation is called metaheuristic optimisation because it uses meta-heuristics to identify optimum solutions. "Meta" means "upper level" and "heuristic" means "solution". That entails using more advanced ways to address uncertain problems. These problems may have one or several aims. Strong goal functions lead to strong optimum solutions. Single objectives ensure that all particles converge on one location, the optimal result [2]. Multi-objective particles converge at two or more sites, and the best solution must be selected. Metaheuristic algorithms iterate over solutions. Many algorithms search globally, some locally. An objective function is created using many metrics and parameters from the issue statement. Metaheuristics might be based on a single solution or a population. To narrow the answer, it searches just the nearby neighbourhood for the best option since it's focused on generating money. As demonstrated in figure 1, population-based approaches are discovery-oriented and confined to global searches for optimum solutions. Two methods that aim to find the best solution are simulated annealing and tabu search. Methods that rely on populations include swarm intelligence and evolutionary algorithms. GA and diversified evolution are two approaches of evolution. Cases of swarm intelligence include ant colony optimisation, particle swarm optimisation, and ABC. Also covered are cuckoo searches and the firefly method. Kennedy suggested particle PSO that flock "may profit from the experience of all other individuals," say sociobiologists. It considers Bird flocks may coordinate foraging. Sharing successful results' locations does it. Since each bird helps to finding the best answer, the flock's solution may be the best. In high-dimensional solution space, this solution is achieved. Heuristics are necessary since there is no proof otherwise. However, particle swarm optimisation solution often approaches global optimum. A global optimum or minimum is sought by PSO [3]. Here are ways to boost earnings and cut losses. This drives us to optimise by trying different function values. Some functions have several local maxima and minima. No matter what, Earth has one absolute maximum and low. Complex function global maxima are hard to find. Although imperfect, it got close to finding the world's maximum and lowest points. PSO belongs under heuristic modelling because of this.

Ant colony optimisation, among other techniques, is inspired by ant pheromones. The ants' plan all along was to exchange outputs for inputs in order to communicate over great distances. They use pheromones that are chemically similar while they hunt. Following this food trail can be a time and energy saver for the other ant species in the colony. To represent object edges, markers, and changes in surface orientation, an ideal edge detector produces a network of connected curves. Edge detection may simplify data processing without affecting image structure. Edge-finding algorithms are mostly search and zero-crossing-based. Many image analysis and machine vision programs struggle to locate moving object edges [4-10]. The ABC technique yields the best Cluster Heads. The first sensor node packet is "hello." After receiving a broadcast message, a sensor node adds the sender sensor's ID and RSSI value to a database. The nodes now notify the BS of their identification, neighbouring table status, and power. These algorithms lets the BS build CH. Nodes with energies over a threshold are CHs. After creating CH, network nodes' RSSI values may be compared to cluster. Then, wellness is assessed for the best results. Candidate algorithm ABC selects CH from pool. Bacterial Foraging Optimisation (BFO) begins with bacteria initialisation, which might be random. Bacterial cells are mostly CHs. Chemotaxis may locate a CH using node ids and current 2D coordinates. Additional swarming is directed using the formula. The microorganisms are ordered by their criterion compliance. Top half of population has to spread bacteria to bottom half to multiply. The technique may cease operating if the same cuckoo search settings are used again. We need a way to alter cuckoo search settings to fix this [11-19].

The firefly method lets us find the optimum path between each cluster's CHs and BSs. Initial firefly testing is thorough. Several CH-BS routes are represented by flamingos. CH plus one space for BS determines the firefly's body size. It must complete a hop at each node before reaching the BS. To get optimal outcomes, we iterate. Considerations for fitness function

include following: people in next-hop CH, distance in Euclidean space between next-hop and BS, nodes between CH and hop, and hop's. When calculating the total number of CHs, genetic algorithms do the best. There is an initialisation phase and a steady-state operating phase to the method. BS arranges nodes according to the number of CHs. Communications between nodes and CHs are sent to back. After the BS creates chromosomes, genetic algorithm selects the best CH. Personal fitness may be assessed using the Fitness/Objective function. This study's target function is the sum of the hop counts [20] for each node, CH, and BS. To reduce data transmission time, maximise the target function. A third agent, CH, helps us achieve maximum separation. The agent CH with the most energy is usually chosen first.

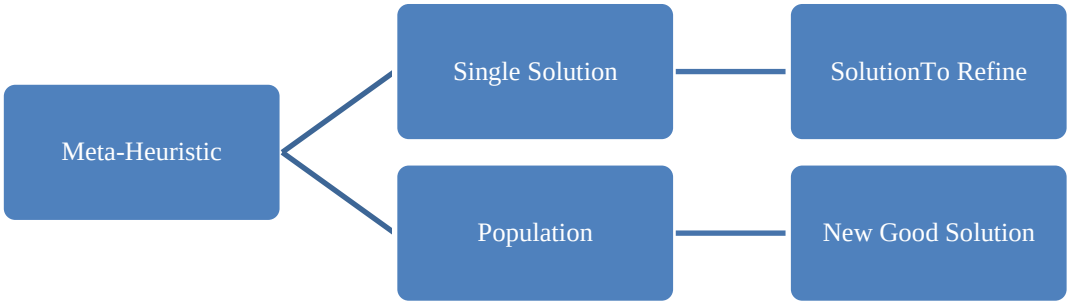


Fig 1 Types of Meta-Heuristic Optimization

1.2 BLOCKCHAIN

Blockchain data is kept in cryptographically linked blocks. Blockchains are a kind of distributed database, unlike relational databases. New blocks get information [21]. Full blocks are connected to the one preceding them so data is presented chronologically. Blockchain technology is most often employed as a distributed transaction ledger, although it may record any data. Bitcoin uses blockchain in a decentralised way so no user or group loses control and ownership is spread. Blockchain technology secures digital data storage and sharing. Thus, a blockchain creates immutable ledgers of transactions that cannot be altered, deleted, or destroyed. Therefore, blockchains are frequently called distributed ledger technology. Block-chain technology has grown more prominent in industry during the last several years. Consider block chains' purpose and need. Working of Block-Chain is shown in fig. 2.

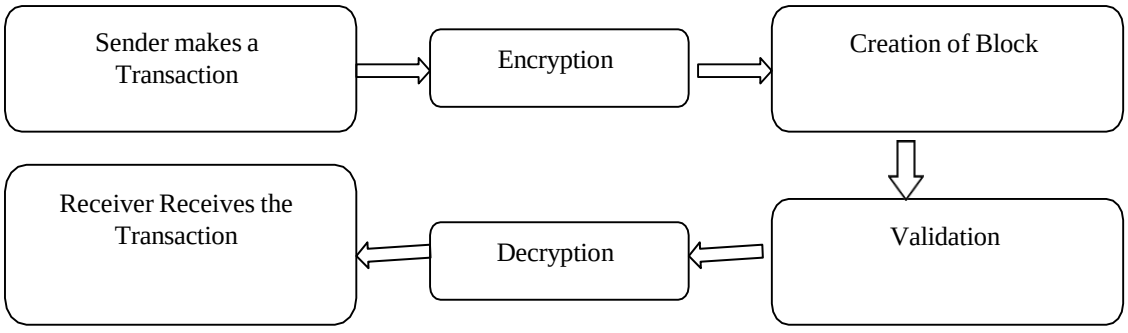


Fig 2 Working of Block-Chain

Blockchains are decentralised, therefore centralised entities cannot approve transactions or impose legitimacy standards. This demands a lot of trust from network members as they must agree to handle transactions. Risk-free is this feature's main benefit. New database entries may be added, but old ones cannot be changed.

1.3 IoT

The term IoT refers to system that allows various "things" (figure 3) to communicate with one another and share data acquired via various means such as sensors, software, processors,

and Internet. Despite the fact that most IoT adoption occurs in the utility and industrial sectors, the network has also discovered applications in the agricultural, infrastructure, and home automation industries, promoting digital transformation in these areas. A better existence for all sentient beings is the ultimate aim of IoT, which aims to connect and communicate everything in the world. The success of IoT is a result of the present technical mindset as well as advancements in hardware and software. Its innovative features caused a sea shift in product distribution. As time goes on, this technology will shape our future.

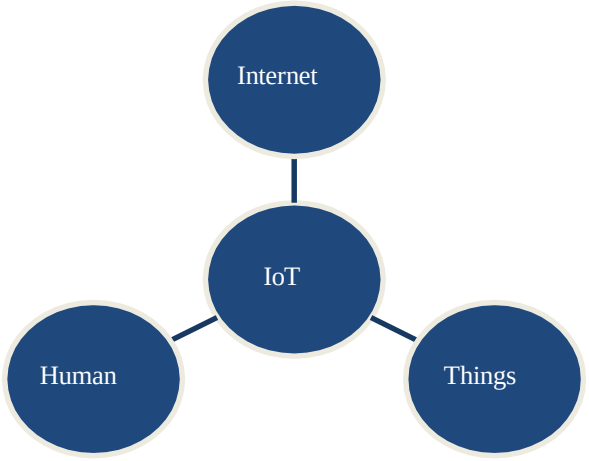


Fig 3 Interaction of Human, Internet and Things leading to IoT

Our insatiable need for knowledge and the dream of a more connected world inspired the creation of IoT. This is why we are developing smart devices to automate tasks and increase productivity. By linking devices to the internet and one another, researchers are able to use neural networks and machine learning to make complex decisions [27–32]. A.I., connectivity, sensors, active participation, and diminutive devices are the building blocks of IoT. Here are the characteristics (fig. 4) that we will briefly go over:

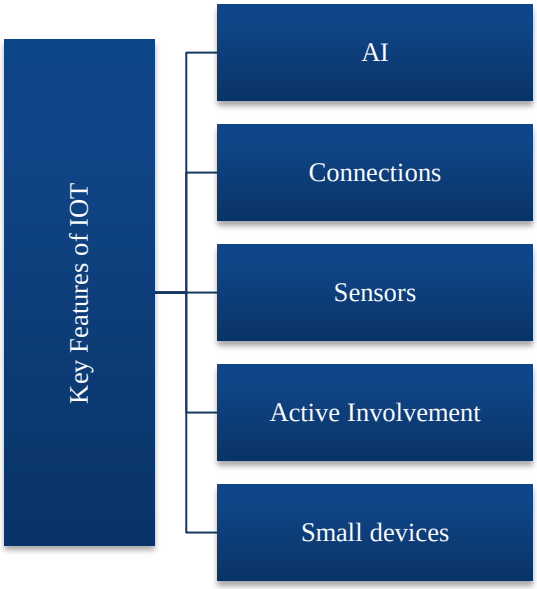


Fig 4 Key features of IoT

AI: Data collecting, AI algorithms, and network connection are the building blocks of AI and IoT, which improve every facet of life. They could put sensors in your cupboards and refrigerator to notify your preferred grocery store when you're low on essentials.

Connections: IoT networks are independent of established telecom companies thanks to new networking technologies like IoT networking.

Sensors: To begin with, sensors are essential to IoT, which is otherwise just a network of interconnected gadgets. IoT is transformed into a dynamic and functional system via a variety of methods.

Active Involvement: These days, we tend to be passive observers when we interact with our linked devices.

Small-Devices: The decreasing size, cost, and power of electronic gadgets is not surprising. The accuracy, scalability, and flexibility of IoT are supported by small, purpose-built devices [33–37].

1.4 Technology and Protocols of IoT

To function, the IoT must make heavy use of existing network protocols and equipment. Most of the technologies and protocols that make IoT possible are radio frequency identification. These technologies allow for the particular networking capabilities needed by an IoT system, as opposed to a standard uniform network of common systems.

NFC and RFID collaborate nicely. The advantages of RFID and NFC are well-suited to connection bootstrapping, identity and access tokens, and financial transactions.

Low-Energy Bluetooth Technology: This technology uses a standard that has a lot of support to fulfil the hard power and longevity requirements of Internet of Things applications.

Low-Energy Wireless: New technology is replacing most power-hungry component of IoT.

Radio Protocols: Protocols that may be used to build low-speed local area networks. Because of great data throughput and low power consumption, these technologies are unique.

LTE-A: Advanced protocol is improvement on original LTE protocol that increases throughput, lowers latency, and broadens coverage.

Wi-Fi-Direct: A central router is not necessary for Wi-Fi Direct to function. Now that P2P connection latency is so low, it can hold its own against Wi-Fi networks.

IoT safety and task performance problems might lead to legal action. Electronic device malfunctions, data theft, and infiltration are the top concerns. These difficulties may have many negative effects. Due to Technical Flaw: Once IoT is fully deployed, mission-critical and life-or-property-impacting systems will be managed more finely. IoT furnace control system failures might cause frozen pipes and water damage while no one is home. Thus, firms must find answers. Computer and network attacks: In short, an IoT attack may damage anything with network connectivity. Hacking a stove or sprinkler system may cause havoc without sufficient precautions. Monitoring, restricted access, and custom precautions are the best strategies to prevent this. Complex defences aren't necessary. Hardened devices are designed with security in mind at every stage. Both manufacturer and user systems must encrypt. Organisations and people must consider all dangers when designing or implementing a new system. Devices should have privileged rules and access wherever feasible. One potential drawback of the Internet of Things is the ease with which sensitive information might be stolen. Their dark desire for revenge, stalking, identity theft, selling and advertising based on personal data, and shaming others into confessing are all examples of their perverted curiosity. Dealing with this danger is like defending against assaults. As the IoT sector grows, hackers will have access to more personal data via smart home devices like Amazon Alexa and smart thermostats. A Blockchain-infused Defending “smart” device against hacking requires transparent, incorruptible technologies like the Internet of Things. Since it records and validates transactions with nodes, the blockchain can safeguard IoT device communication. Blockchain data encryption may improve IoT protocols. Blockchain technology makes IoT apps safer and more private.

1.5 Distributed Environment

Distributed systems employ numerous computers to execute a job. Multiple computers accomplish the job. Distributed computing studies multi-node computer networks. Distributed computing accelerates tasks using a network of computers. Distributed systems offer several benefits that are well known. Distributed Systems advantages cannot be completely realised without the necessary infrastructure for operating and building Distributed Applications. Distributed applications run on numerous machines and communicate over a network. Its modules operate separately on network nodes but work together to achieve a purpose. The system is client-server. Resources required to generate and maintain distributed software are called "distributed computing environment". It is a collection of interoperable software components/frameworks that operate on an OS and provide Decentralised Application development and deployment. DCE applications let user's access distant server data and programs.

1. Networks: Ethernet and LAN were developed in the 1970s to facilitate localized computer networking. Distributed systems like internet and e-mail are the most well-known results of the rise of peer-to-peer networking.

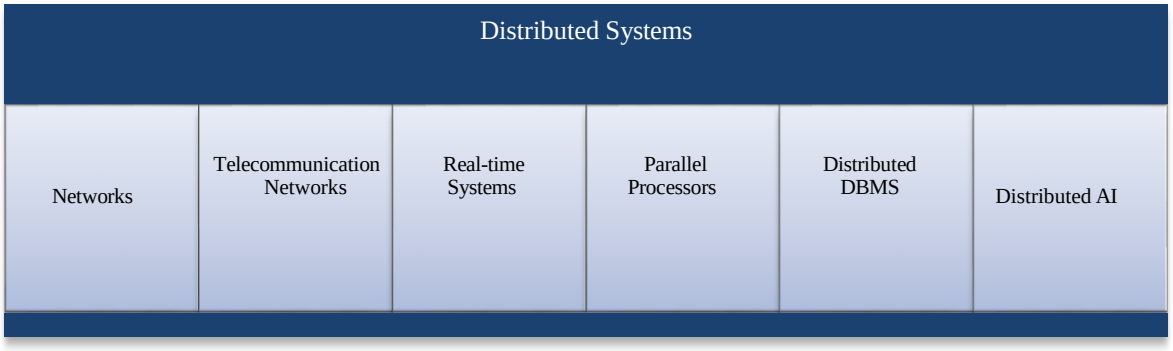


Fig 5 Major examples of Distributed Systems

2. Telecommunication networks: P2P networks also include traditional telephone and mobile phone networks. The first telephone networks were also early examples of distributed communication systems; today's cellular networks are similarly descended from the original telephone network.

3. Real-time systems: It's not just one industry that can benefit from real-time technologies. The global airline, ridesharing, logistics, financial trading, MMORPG, and ecommerce businesses all make use of and benefit from such platforms.

4. Parallel processors: When numerous computers work together, they divide up specialized jobs. This then generates data that can be assembled into a large computing problem.

5. Distributed database systems: Information can be copied and pasted between other systems. In the world of distributed databases, things might go either way: homogeneous or heterogeneous. Systems in a homogenous distributed database employ the same database administration framework and data model.

6. Distributed artificial intelligence: To complex learning algorithms, decision-making, & large-scale systems, distributed AI is just one of the various AI learning methodologies. As can be seen in Figure 6, the applications for distributed systems are almost endless, ranging from online banking to massively multiplayer gaming.

Distributed systems drive modern computer architectures by improving performance and scalability. Wireless networks, cloud computing, and the internet need dispersed systems. Pooling the processing capacity of numerous computers to accomplish goals that would be difficult or impossible with a single computer has made distributed systems exceedingly dependable.

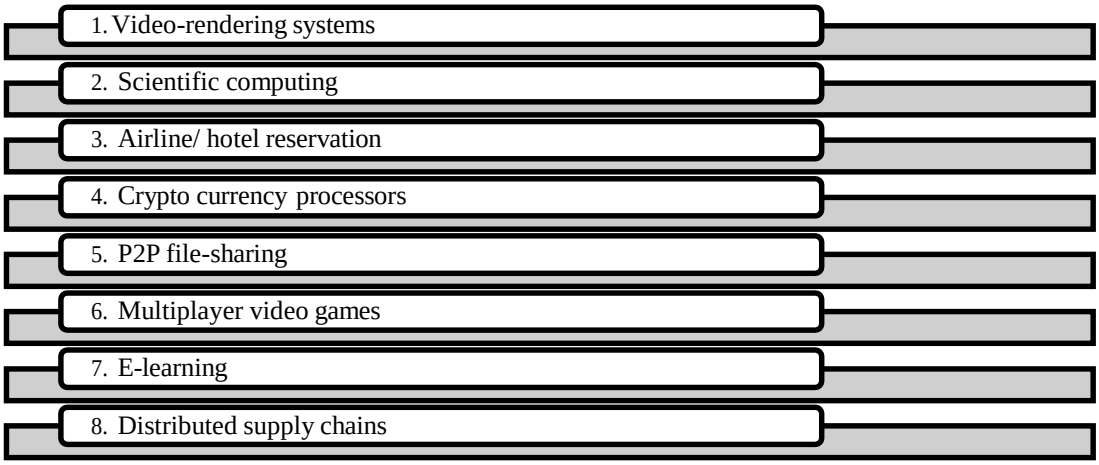


Fig 6 Real-world examples of distributed systems

1.6 Role of CNN for Optimization and Blockchain Mechanism in IoT-Based Distributed Environment

An IoT-based distributed system must be secure and functional due to the amount of data created, managed, and exchanged by associated devices. We can improve system efficiency and security by combining blockchain technology, which manages data securely and decentralised, with CNNs, which can analyse complicated patterns.

Role of CNN in Optimization: CNNs improve data analysis and decision-making, making them vital for IoT system optimisation. Pattern identification and anomaly detection would improve dynamic resource allocation. CNNs analyse consumption patterns to reduce latency and improve system efficiency, optimising IoT device resource utilisation. They also excel in detecting device or network failures, ensuring system reliability. CNN analysis may optimise busy network traffic, improving IoT connectivity and data flow.

Role of Blockchain Mechanism: IoT devices, which complement CNNs, will benefit from blockchain's decentralised and secure data management. Unchangeable data storage ensures the authenticity of data exchanged between IoT devices and avoids manipulation. Decentralised trust management in blockchain enables devices to independently authenticate and verify transactions, avoiding centralised power needs. Smart contracts can automate security policy execution and resource allocation, improving efficiency. For IoT networks to be secure and open, blockchain technology is important.

Integration of CNN and Blockchain in IoT: Blockchain and CNNs provide a secure and optimised foundation for IoT-based distributed ecosystems. Blockchain validates and securely records all transactions and decisions, but CNNs analyse data in real time to find cyber threats and abnormalities. CNNs can spot potential problems, whereas blockchain can provide a secure solution. Blockchain's distributed ledger allows frictionless data sharing, but CNNs preprocess and analyse data for educated decision-making. Combining technologies creates a secure, scalable IoT.

2. LITERATURE REVIEW

Interest in the possible uses of new technology across a range of sectors, including the IoT, blockchain, big data, and deep learning, has exploded recently. The Internet of Things has upended various industries by allowing smart devices to communicate constantly and instantly share data. As Dorri et al. (2017) stress, optimising blockchain for Internet of

Things applications depends on addressing problems with scalability, latency, and security. Conti et al. (2017) have proposed an energy-efficient and secure IoT system-on-chip for near-sensor analytics to help real-time data processing.

The purpose of distributed computing in IoT has been much under investigation. Sharma and Dutta (2015) introduced a middleware architecture based on distributed DNNs to detect cyberattacks in smart IoT ecosystems. Further underlining the use of artificial intelligence in IoT security, Han and Kim (2016) proposed a back-end offload architecture for protecting resource-limited networks. Yuan, Zhang, and Liu's (2015) study on automated forest fire monitoring utilising UAVs and remote sensing techniques provides even another IoT-integrated environmental monitoring system example.

Blockchain technology has recently emerged as a potent new tool for increasing online transaction security and dependability. Atzori (2017) put forward a transparent and distributed type of governance for the eSociety using blockchain technology. Killeen's (2015) study of how the two have come together in the global sharing economy highlighted how blockchain can upend conventional commercial and financial organisations.

Furthermore emphasised by Czepluch, (2015) who looked at its many applications across industries was the adaptability and revolutionary potential of blockchain. Furthermore much attention has been paid to researching how blockchain technology interacts with big data. Examining big data analytics for cloud computing, IoT, and cognitive computing, Hwang and Chen (2017) sought to demonstrate how data-driven insights may maximise system efficiency. Mahjabin et al. (2017) studied strategies for stopping DDoS attacks in order to address significant security concerns in big-scale networks. As Pena, Rodriguez (2017) highlight, reconfigurable platforms are also quite crucial for IoT. This promotes adaptability in evolving environments and scalability.

Deep learning models, especially CNNs, have been examined in several research for possible application in cryptographic analysis and cybersecurity. Hill and Bellekens (2017) demonstrated using a deep learning-based technique for cryptographic basic categorisation that neural networks can successfully identify security issues. Furthermore, Khan (2017) looked at the challenges of computer security in applications targeted on people, stressing the requirement of threat detection methods driven by artificial intelligence. Thangarasu and Alla (2017) propose a whale optimisation technique to raise the accuracy of intrusion predictions within the domain of Internet of Things security. Many have considered how blockchain technology may be used with the internet of things to provide secure and efficient data transfers. Thakur (2017) looked on accounting, authorisation, and authentication techniques on the Ethereum blockchain in order to ensure data integrity and access control. Han and Yang (2016) investigated privacy, anonymity, and security in computing and communication systems underlining the necessity of distributed security frameworks. Vo-Huu and Noubir (2014) developed the crypto-coded modulation technique in order to boost cyber attack resistance.

Edge computing and new advancements in mobile connection have tremendously expanded the spectrum of potential IoT applications. AI-driven Bayesian game-theoretic solution to resource optimisation in 6G-IoT networks enabled intelligent and adaptive network management. Several researchers investigated ways to safely implement mobile services in edge computing environments in response to concerns regarding data privacy and security. IoT, blockchain, distributed computing, big data, and deep learning have all been discussed extensively on how they will interact to provide digital ecosystems that are both smart and secure moving forward. Further research is needed to tackle present issues with scalability, energy economy, and processing data in real-time so that various technologies cooperate and operate at their best.

Table 1 Literature Survey

S. No.	Author / Year	Title	Methodology	Limitations
1	Dorri et al., 2017	Towards an optimized blockchain for IoT	Proposed an optimized blockchain framework for IoT networks to enhance security	Limited scalability due to computational constraints
2	Meelu & Anand, 2010	How Effective Cluster-based Routing Protocols Are for WSN in Terms of Energy Efficiency	Analyzed cluster-based routing protocols for energy-efficient communication in WSNs	Lacks real-time implementation and validation
3	Conti et al., 2017	Secure and Energy-Efficient IoT Endpoint System-on-Chip for Near-Sensor Analytics	Designed an energy-efficient IoT SoC for secure data processing	Security aspects require further enhancement
4	Sharma & Dutta, 2015	Distributed DNN-based Cyberattack Detection Middleware for Smart IoT	Utilized deep neural networks for detecting cyberattacks in IoT environments	High computational cost for real-time processing
5	Hill & Bellekens, 2017	Classification of Cryptographic Primitive Encryptions Using Deep Learning	Developed a deep learning model for classifying cryptographic primitives	Model performance depends on training data quality
6	Mahjabin et al., 2017	A Comprehensive Review of DDoS Attacks, Their Prevention, and Mitigation Strategies	Reviewed various DDoS attack mitigation techniques in distributed networks	Lack of implementation details for real-world use
7	Khan, 2017	Computer Security in Human Life	Discussed security threats in computing environments and proposed countermeasures	Does not cover emerging threats like AI-driven cyberattacks
8	Ambrosin et al., 2014	Updaticator: Secure Software Update Distribution in Untrusted Networks	Proposed a scalable software update mechanism for IoT devices	Scalability concerns in large-scale networks
9	Killeen, 2015	Bitcoin at the Crossroads with Global Sharing Economy	Analyzed the impact of Bitcoin on the global economy	Limited focus on regulatory challenges
10	Czepluch et al., 2015	Exploring Many Use Cases of Blockchain	Explored the applicability of blockchain in various domains	Lacks implementation details in real-world use cases
11	Atzori & Ulieru, 2017	eSociety on Blockchain: An Architectural Framework	Proposed a blockchain-based societal architecture	Ethical concerns and scalability remain unresolved
12	Thakur, 2017	Verification, Permission, and Record Keeping with Ethereum Network	Used Ethereum smart contracts for AAA in distributed networks	Limited experimental evaluation
13	Thangarasu & Alla, 2017	Whale Optimization Algorithm for Intrusion Detection in IoT	Applied Whale Optimization Algorithm to enhance IoT security	Algorithm performance varies with different attack types
14	Pena et al., 2017	Role of Reconfigurable Platforms in IoT	Examined the role of reconfigurable computing	Lacks real-world validation

			in IoT applications	of proposed methods
15	Menapace, 2017	Clustering Blockchain Protocols with Regards to Security Testing	Categorized blockchain security testing approaches	Does not evaluate performance metrics in depth
16	Yu et al., 2017	Protecting Data in Cyber-Physical Environments	Special issue discussing security challenges in CPS	Lacks practical implementation details
17	Dhawan, 2012	Advanced Sensing in Image Processing and IoT	Discussed IoT-enabled image processing techniques	Does not address security risks in depth
18	Han & Kim, 2016	A Secure Backend Offload Architecture for Networks with Limited Resources	Proposed an offloading strategy for securing IoT networks	High latency in real-world scenarios
19	Han & Yang, 2016	Security, Privacy, and Anonymity in Computing	Explored security and privacy challenges in computing systems	Limited coverage of blockchain-based solutions
20	Vo-Huu & Noubir, 2014	Crypto-Coded Modulation for Rate Information Concealing	Proposed a novel cryptographic modulation scheme	Complexity in implementation
21	Yuan et al., 2015	Survey on UAV-based Forest Fire Monitoring	Reviewed UAV technologies for forest fire detection	Energy efficiency remains a challenge
22	Jover, 2013	Security Attacks in LTE Mobility Networks	Examined security threats in LTE mobility networks	Lacks discussion on mitigation strategies
23	Chaudhary et al., 2016	Deep Learning-Based IoT Network Intrusion Detection	Used deep learning for IoT security monitoring	High computational requirements
24	Hwang & Chen, 2017	Analytics on Big Data for Cloud, IoT, and Cognitive Computing	Reviewed big data analytics applications in IoT and cloud	Scalability issues in real-world applications
25	Monika Singh et al., 2017	Blockchain in Cybersecurity	Discussed the role of blockchain in enhancing cybersecurity	Lacks experimental validation
26	Ki et al., 2015	API Call Sequence Analysis for Malware Detection	Proposed an API-based approach for detecting malware	High false-positive rates in detection
27	G. D. Hill, 2017	Deep learning , cryptography	Explored cryptography that is based on deep learning	Limited real-world applications discussed
28	T. Mahjabin, 2017	Denial of service, attack	Discussed privacy and security issues	No experimental validation of countermeasures
29	R. Tzezana, 2016	Future crime, terror attack using IoT	Examined security vulnerabilities in IoT	Does not propose concrete mitigation strategies
30	M. N. Semeria, 2016	Smart and secure technology, Hyperconnectivity	Considered secure technology in age of hyper connectivity	Limited real-world case studies provided

Table 2 Comparison of feature chart

Citation	Blockchain	Optimization	Distributed Environment	IoT	CNN
[1]	Yes	Yes	No	Yes	No
[2]	Yes	No	No	Yes	No
[3]	Yes	No	No	Yes	No
[4]	Yes	Yes	No	Yes	No
[5]	Yes	Yes	Yes	Yes	Yes
[6]	Yes	No	No	Yes	No
[7]	Yes	No	No	Yes	No
[8]	Yes	No	No	Yes	No
[9]	No	No	Yes	Yes	Yes
[10]	No	No	Yes	No	No
[11]	Yes	No	No	Yes	No
[12]	Yes	Yes	No	No	Yes
[13]	Yes	No	No	No	No
[14]	Yes	No	No	Yes	No
[15]	Yes	No	No	Yes	No
[16]	Yes	No	No	Yes	No

3. ROLE OF OPTIMIZATION IN BLOCK CHAIN USING CNN

Optimising blockchain technology greatly improves performance, especially in distributed systems built on IoT, where scalability, efficiency, and speed are of the utmost importance.

better resource management, decreased latency, and higher data processing capacity. CNNs are perfect for blockchain optimisation because to their remarkable pattern detection and trait extraction capabilities. Utilising CNNs to analyse network traffic patterns and optimise transaction validation procedures is one way to enhance the consensus and performance of blockchain systems. Because IoT devices produce massive volumes of data that need real-time processing, this is crucial. Blockchain optimisation in the realm of energy efficiency is another potential use of CNNs. Particularly blockchain networks that rely on proof-of-work techniques may be rather demanding on system resources. To make these processes go more smoothly, CNNs can predict and adjust how much resources will be used, cut down on unnecessary calculations, and ensure that jobs that use a lot of energy are properly managed. Additionally, by dynamically managing the allocation of resources, CNNs improve the scalability of blockchain systems. Predicting future workload needs and adjusting blockchain operations appropriately, they make sure the network keeps running smoothly even as it grows. Given the exponential growth potential of connected devices and data exchanges, these qualities are essential for Internet of Things applications. IoT devices may benefit from blockchain technologies better performance, scalability, and energy economy thanks to CNNs. The continued viability and effectiveness of blockchain as a solution for managing trust, transparency, and security in complex data-driven systems is guaranteed by this relationship.

4. ISSUES IN EXISTING RESEARCH

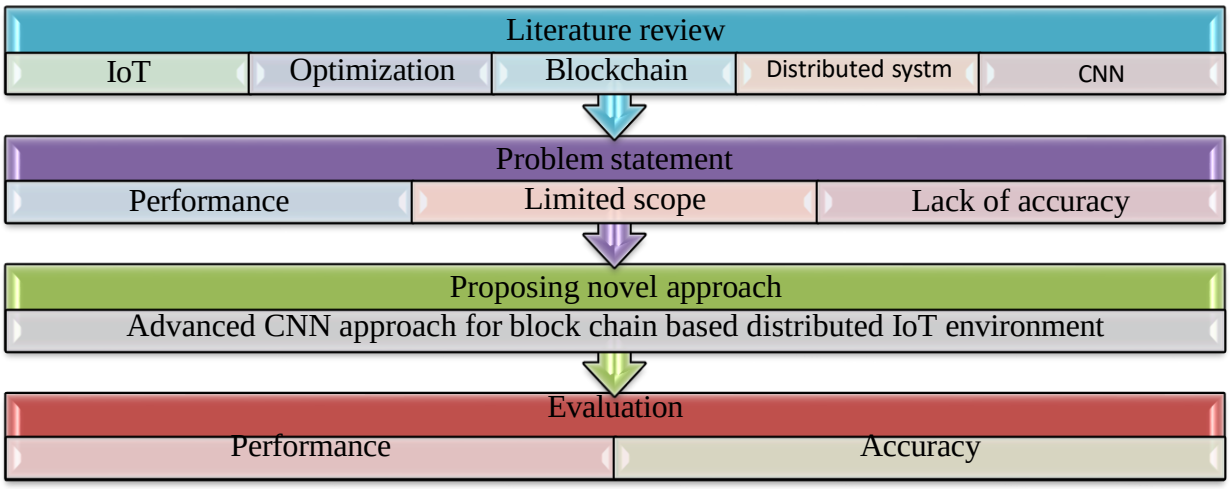
Data security, operational efficacy, and encrypted communication are three issues that are becoming more prevalent with the proliferation of IoT devices. The enormous amounts of data generated by IoT devices need secure ways of data storage, processing, and protection against hackers and unauthorised access. Concerning these systems, existing security designs can be vulnerable since they can't handle the scalability and real-time requirements. Distributed ledger technology, more commonly known as blockchain, may address these issues due to its cryptographically secured design. Traditional blockchain implementations struggle with scalability, energy efficiency, and transaction speed, particularly when integrated with IoT networks. Due to the high processing demands of blockchain security maintenance, resource-constrained IoT devices may also be inefficient. One novel approach to overcoming these limitations is metaheuristic optimisation, which use CNNs and other higher-level heuristic approaches to discover enduring solutions. With CNNs, distributed systems powered by IoT may make the most of blockchain operations by enhancing pattern recognition efficiency, decreasing energy consumption, and guaranteeing scalability. A universal framework integrating blockchain technology, metaheuristic optimisation, and CNNs is lacking in existing solutions for the specific security and performance issues with IoT networks, despite the obvious advantages. This study aims to investigate how incorporating CNNs and metaheuristic optimisation techniques into blockchain systems might improve the scalability, efficiency, and security of distributed systems that rely on IoT. By developing a robust and adaptable framework for safe data processing and transmission among IoT devices, this project aims to fill these gaps.

5. PROPOSED RESEARCH WORK

Both IoT and blockchain have previously been studied in relation to distributed ecosystems. After that, investigating the issues related to an IoT-based dispersed environment is considered. There have been reports of performance and accuracy issues from researchers concentrating on this area. It would be used in the process of developing an effective blockchain model after the level of security had been increased. An evaluation of the validity and performance of the suggested model is the final remaining task. The research methodology is shown in Figure 7.

The ways in which applications use block chain and IoT with a CNN model have been examined in several researches. Subsequently, an examination of these discoveries was

carried out. Research conducted in a distributed environment is not as accurate as it might be in terms of the amount of performance it is capable of achieving. A company's ability to adapt to changing security threats is a key factor in determining the level of satisfaction its



customers have with the products and services it offers via CNN.

Fig 7 Research Methodology

6. FUTURE SCOPE AND CONCLUSION

One term for optimisation that employs meta-heuristic approaches to discover optimum solutions is metaheuristic optimisation. Together, the words "meta" and "heuristic" mean "upper level" and "solution," respectively. When the objective function is robust, the optimal solution is also robust. Distributed ledger technology known as a blockchain stores information in encrypted blocks with cryptographic protections applied to both the blocks themselves and the links between them. In contrast to the more common relational databases, this is what distinguishes blockchain as a distinct kind of distributed database. Each new block of data is appended to the end of the one that was most recently processed. Ensuring that data in following blocks is collected in the correct chronological order requires linking each block once its data is taken. Even though it can store any kind of data, blockchain technology has mostly been employed as a distributed ledger for transactions thus far. IoT is perfect for use in hack-proofing "smart" items because of its blockchain-infused transparency and almost incorruptibility. Blockchain has the potential to make IoT connections more secure by recording and validating transactions. This allows us to determine which sensors were responsible for collecting a certain data set. The use of blockchain technology to encrypt data could result in safer protocols for the IoT. A more private and secure IoT application could be possible with blockchain technology. The study of multi-node computer networks is known as distributed computing. To speed up data processing, distributed computing makes use of a network of computers.

Distributed systems developed on the IoT may greatly benefit from combining blockchain technology with CNNs in order to increase operational efficiency, data security, and scalability. The need for safe, decentralised systems that can handle massive volumes of data will only grow in response to the proliferation of interconnected gadgets. For IoT devices with limited resources, future studies may investigate ways to optimise blockchain algorithms for faster transactions with less power usage. To further enhance pattern recognition, anomaly detection, and system reliability, it would be helpful to investigate enhanced CNN architectures and hybrid metaheuristic approaches. Blockchain technology, CNNs, and optimisation methods have finally come together to provide a strong answer to the security problems plaguing IoT settings. This research should inform the development of safe, scalable systems to ensure the integrity and preservation of data. An effective and long-lasting IoT infrastructure that can adapt to the changing needs of today's dispersed settings is within reach, according to the groundwork laid forth by this study.

REFERENCES

1. Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for IoT. Proceedings - 2017 IEEE/ACM 2nd International Conference on Internet-of-Things Design and Implementation, IoTDI 2017 (Part of CPS Week), October, 173–178. https://doi.org/10.1145/3054977.3055003
2. Meelu, R., & Anand, R. (2010, November). Energy Efficiency of Cluster-based Routing Protocols used in Wireless Sensor Networks. In AIP Conference Proceedings (Vol. 1324, No. 1, pp. 109-113). American Institute of Physics.
3. Conti, F., Schilling, R., Schiavone, P. D., Pullini, A., Rossi, D., Gürkaynak, F. K., ... & Benini, L. (2017). An IoT endpoint system-on-chip for secure and energy-efficient near-sensor analytics. IEEE Transactions on Circuits and Systems I: Regular Papers, 64(9), 2481-2494.
4. Sharma, S., & Dutta, N. (2015). Distributed DNN-based Middleware for Cyberattack Detection in the Smart IOT Ecosystem: A Novel Framework and Performance Evaluation Technique.
5. Hill, G. D., & Bellekens, X. J. (2017). Deep learning based cryptographic primitive classification. arXiv preprint arXiv:1709.08385.
6. Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 13(12), 1550147717741463.
7. Khan, M. (2017). Computer security in the human life. Int. J. Comput. Sci. Eng, 6.
8. Ambrosin, M., Busold, C., Conti, M., Sadeghi, A. R., & Schunter, M. (2014). Updaticator: Updating billions of devices by an efficient, scalable and secure software update distribution over untrusted cache-enabled networks. In Computer Security-ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part I 19 (pp. 76-93). Springer International Publishing.
9. Killeen, A. (2015). The confluence of bitcoin and the global sharing economy. In Handbook of digital currency (pp. 485-503). Academic Press.
10. Czepluch, J. S., Lollike, N. Z., & Malone, S. O. (2015). The use of block chain technology in different application domains. The IT University of Copenhagen, Copenhagen.
11. Atzori, M., & Ulieru, M. (2017). Architecting the eSociety on blockchain: A provocation to human nature. Social Science Research Network. https://papers. ssrn. com/abstract, 2999715.
12. Thakur, M. (2017). Authentication, authorization and accounting with Ethereum blockchain. Helsingfors universitet.
13. Thangarasu, G., & Alla, K. R. (2017, April). Wagging-Based Whale Optimization Algorithm to Enhance the Prediction of Intrusions in IoT Network. In International Conference on Engineering, Applied Sciences and System Modeling (pp. 459-470). Singapore: Springer Nature Singapore.
14. Pena, M. D. V., Rodriguez-Andina, J. J., & Manic, M. (2017). The internet of things: The role of reconfigurable platforms. IEEE Industrial Electronics Magazine, 11(3), 6-19.
15. Menapace, T. (2017). Clustering Blockchain Protocols With Regards To Security Testing (Doctoral dissertation, University of Applied Sciences Leipzig).
16. Yu, W., Fu, X., Song, H., Economides, A. A., Jo, M., & Zhao, W. (2017). Guest editorial special issue on security and privacy in cyber-physical systems. IEEE Internet of Things Journal, 4(6), 1798-1801.
17. Dhawan, S. (Ed.). (2012). Advanced sensing in image processing and IoT/edited by Rashmi. International Journal of Computer Applications, 58(18), 13-16.
18. Han, J., & Kim, D. (2016, October). A back-end offload architecture for security of resource-constrained networks. In 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA) (pp. 383-387). IEEE.
19. Han, W., & Yang, X. (2016). Security, privacy, and anonymity in computation, communication, and storage. Springer, 10066, 1-11.

20. Vo-Huu, T. D., & Noubir, G. (2014). CBM: A crypto-coded modulation scheme for rate information concealing and robustness boosting. arXiv preprint arXiv:1411.5078.
21. Yuan, C., Zhang, Y., & Liu, Z. (2015). A survey on technologies for automatic forest fire monitoring, detection, and fighting using unmanned aerial vehicles and remote sensing techniques. Canadian journal of forest research, 45(7), 783-792.
22. Jover, R. P. (2013, June). Security attacks against the availability of LTE mobility networks: Overview and research directions. In 2013 16th international symposium on wireless personal multimedia communications (WPMC) (pp. 1-9). IEEE.
23. Chaudhary, D. K., Yadav, P., & Jha, K. (2016). Deep Learning and Elephant Herd Based IOT Network Intrusion Alarming System.
24. Hwang, K., & Chen, M. (2017). Big-data analytics for cloud, IoT and cognitive computing. John Wiley & Sons.
25. T. Monika Singh, C. Kishor Kumar Reddy, and K. Lippert, "The revolution and future of blockchain technology in cybersecurity," Artificial Intelligence for Blockchain and Cybersecurity Powered IoT Applications. CRC Press, pp. 71–98, Nov. 06, 2017. doi: 10.1201/9781003497585-5.
26. Y. Ki, E. Kim, and H. K. Kim, "A Novel Approach to Detect Malware Based on API Call Sequence Analysis," International Journal of Distributed Sensor Networks, vol. 11, no. 6. SAGE Publications, p. 659101, Jun. 01, 2015. doi: 10.1155/2015/659101.
27. G. D. Hill and X. J. A. Bellekens, "Deep Learning Based Cryptographic Primitive Classification," 2017, arXiv. doi: 10.48550/ARXIV.1709.08385.
28. T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," International Journal of Distributed Sensor Networks, vol. 13, no. 12. SAGE Publications, p. 155014771774146, Dec. 2017. doi: 10.1177/1550147717741463.
29. R. Tzezana, "High-probability and wild-card scenarios for future crimes and terror attacks using the Internet of Things," foresight, vol. 19, no. 1. Emerald, pp. 1–14, Mar. 13, 2017. doi: 10.1108/fs-11-2016-0056.
30. M. N. Semeria, "Symbiotic low-power, smart and secure technologies in the age of hyperconnectivity," 2016 IEEE International Electron Devices Meeting (IEDM), San Francisco, CA, USA, 2016, pp. 1.3.1-1.3.14, doi: 10.1109/IEDM.2016.7838027.
31. K. Bheemaiah, "Why Business Schools Need to Teach About the Blockchain," SSRN Electronic Journal. Elsevier BV, 2015. doi: 10.2139/ssrn.2596465.
32. Ali. M. A. Ibrahim et al., "Advancing 6G-IoT networks: Willow catkin packet transmission scheduling with AI and bayesian game-theoretic approach-based resource allocation.," Internet of Things, vol. 25. Elsevier BV, p. 101119, Apr. 2017. doi: 10.1016/j.iot.2017.101119.
33. M. Bhandarkar, P. Bansal, and B. Dewan, "Introduction to Application of Artificial Intelligence in Agricultural Industry," Artificial Intelligence and Communication Techniques in Industry 5.0. CRC Press, pp. 289–305, Sep. 17, 2017. doi: 10.1201/9781003494027-18.
34. J. Wurm et al., "Introduction to Cyber-Physical System Security: A Cross-Layer Perspective," in IEEE Transactions on Multi-Scale Computing Systems, vol. 3, no. 3, pp. 215-227, 1 July-Sept. 2017, doi: 10.1109/TMSCS.2016.2569446.
35. G. Wang, J. Feng, M. Z. A. Bhuiyan, and R. Lu, Eds., Security, Privacy, and Anonymity in Computation, Communication, and Storage. Springer International Publishing, 2017. doi: 10.1007/978-3-030-24900-7.
36. J. Han and D. Kim, "A back-end offload architecture for security of resource-constrained networks," 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 2016, pp. 383-387, doi: 10.1109/NCA.2016.7778645.
37. P. William, P. B. Khatkale, and N. Yogeesh, "A Study of Secure Deployment of Mobile Services in Edge Computing," Edge Computational Intelligence for AI-Enabled IoT

Systems. CRC Press, pp. 155–170, Jan. 23, 2017. doi: 10.1201/9781032650722-11.
38. R. Altawy and A. M. Youssef, “Security, Privacy, and Safety Aspects of Civilian Drones,” ACM Transactions on Cyber-Physical Systems, vol. 1, no. 2. Association for Computing Machinery (ACM), pp. 1–25, Nov. 09, 2016. doi: 10.1145/3001836.
39. A. Ometov, A. Levina, P. Borisenko, R. Mostovoy, A. Orsino and S. Andreev, "Mobile Social Networking Under Side-Channel Attacks: Practical Security Challenges," in IEEE Access, vol. 5, pp. 2591-2601, 2017, doi: 10.1109/ACCESS.2017.2665640.
40. A. Devulkar and M. Awwad, “Blockchain and the internet of things: A literature review,” Proc. Int. Conf. Ind. Eng. Oper. Manag., vol. 59, no. 2011, pp. 1079–1090, 2017.
41. Meelu, R., & Anand, R. (2010, November). Energy Efficiency of Cluster-based Routing Protocols used in Wireless Sensor Networks. In AIP Conference Proceedings (Vol. 1324, No. 1, pp. 109-113). American Institute of Physics.