Multi-layer Security and Power Efficiency Improvement with Blockchain Technology and NB-IoT

Chand Pasha Mohammed
Lovely Professional University
Sudan Jha
Kathmandu University
Shakti Raj Chopra
Lovely Professional University
Krishan Arora
Lovely Professional University
Rakesh Kumar
Punjab Technical University
Nihar Ranjan Pradhan
nihar.scitm@gmail.com

VIT AP University

Article

Keywords: Security, Narrowband Internet of Things, Smart Contract, Supply Chain Management

Posted Date: April 10th, 2024

DOI: https://doi.org/10.21203/rs.3.rs-4111246/v1

Additional Declarations: No competing interests reported.

Abstract

To increase the level of safety, precision, and openness of narrow-band IoT combined with blockchain. NB- IoT revolutionizes seamless connectivity for IoT devices in 3Gpp released 15, enabling long battery life and widespread coverage, its low-power consumption, enhanced penetration capabilities, promising a scalable and robust infrastructure for the future with integration of Blockchain technology presents a decentralized, immutable ledger system that ensures transparent and secure transactions across various industries, fostering trust without intermediaries and reducing fraud risks significantly. Its cryptographic principles and distributed nature empower industries by enabling traceability, enhancing data integrity, and revolutionizing traditional processes of supply chain management, our approach provides distributed data authentication while simultaneously creating a layer-based blockchain with NB- IoT proposing in this paper 16 QAM OFDM modulation technique optimizing Bit Error rate (BER), Symbol Error rate (SER), and Frame Error rate (FER) signal to noise ratio (SNR) at the maximum power of 25db using MAT Lab simulation graphical results in multi-layer, double-layer, and single-layer. Our mathematical model for optimizing business activities carried out at every stage of the intelligent supply chain facilitates revenue sharing among the entities of producers, distributors, and re-sellers who make up the proposed blockchain system and NB-IoT as it incorporates with additional traceability and review functions, it is the optimal solution for safe transportation of intelligent supply chain management.

Introduction

The Internet of Things connects millions of devices, heavily taxing the current communication infrastructures. Thousands of Smartphones can today fit within a radio cell [1, 5], but in the future, ordinary mobile networks could support millions of devices or sensors. Not surprisingly, there would be a sharp spike in both energy consumption [4] and network strain [5]. To address this issue, the NB-IoT standard was put into place. Radio waves of sufficient strength to pass through solid concrete and reach even the deepest, underground parts of a building power narrow-band machine sensor networks. As 5G networks have the potential to use very little energy and operate for many years without the need for new batteries, we are at the forefront of a major development in the field of communication. One layer of the network will make use of the machine's built-in sensor network [2].

The network of intelligence is divided into multiple tiers, or "slices," with distinct functions for each. All apps will be able to dependably communicate with each other according to their needs because of the various network levels [3].

A few examples are the ability for vending machines to report on their own inside the machine sensor network [2], the ability for permanently installed streetlights to only turn on or dim when necessary, and the ability for parking spaces to indicate if they are available. Numerous manufacturing potentials are presented by narrowband IoT [3].

When a significant number of narrowband IoT devices communicate with one another to increase city safety, the result is a smart city, which is an example of the Internet of Things. Your creative thinking in creating further interoperable devices could benefit us all [4]. Improve the way you convey your work.

Main Contributions

The main contributions of the paper:

1. In this paper combining both the technologies, blockchain and NB- IoT, the approach provides distributed data authentication while, simultaneously creating blockchain security with additional traceability and review functions, it is the optimal solution for safe transportation.
2. Unlike the existing conventional and proposed method of Intelligent supply chain with IoT and blockchain system facilitates the security, immutability, and authentication in the agriculture sector carried out revenue sharing profits among the entities; producer, wholesaler, and retailers are based on optimized business activities automatically without involving third parties using mathematical models are analysed every stage of the supply chain management.
3. Unlike conventional schemes the proposed multi-layered blockchain structure combined with Narrowband IoT explains the compatibility of various levels of security, scalability, power dissipation, and use cases in agriculture and supply

chain management.

4. Analysed and optimized multilayer simulation results in graphical representation of power versus bit error rate (BER), frame error rate (FER), and symbol error rate (SER) for OFDM over 16-QAM modulation technique is obtained for single-layer, two-layer, and multi-layer systems.

Paper Organization

The structure of the paper is as follows: Section I discussed IoT in the Introduction. Section II deals with Blockchain Technology and the NB-IoT Section. III deals with the Background of Literature. Section IV deals with Methodology. Section V. Deals with deals with a Mathematical model for supply-chain to implement smart contracts. VI Results and Analysis VII. Deals with the Results. Section VIII. Deals with Conclusion.

BLOCKCHAIN TECHNOLOGY WITH NB-IoT

Blockchain technology is an innovative technology that has gained pace over the past few years, with organizations in a wide range of sectors adopting it. It is a distributed and decentralized digital ledger [6-11] that operates an increasing number of records. Blockchain is just a digital decentralized database that allows for efficient and safe data exchanges [7].

Because of its intrinsic safety, blockchain is usually connected to the financial industry. However, there is still more to be discovered about the technology's numerous potential applications in other fields [12]. One area where blockchain has the potential to have a big influence is logistics in the food supply chain. Every block of transactions on a blockchain is connected to the block before it, creating a distributed ledger [13].

A flat file can be used instead of a complex database as one method of storing the blockchain. The task of the Sha256 cryptographic hashing method is to provide a distinct hash for the blockchain's block headers, enabling the identification of specific blocks [6]. The "prior block hash" element in the block header points to the parent block of a block. Stated differently, the hash of the parent block is contained in the header of each child block as shown in Fig.1 Generic blockchain. Every block's hash sequence is linked to its parents' hash sequences, creating a chain that can be traced back to the first block [6, 7]. The first stone of the foundation has been placed. The four primary categories of blockchain networks are hybrid, private, consortium, and public blockchains [13–20]. Encryption is used to safeguard sensitive data when it is being stored on a computer system, sent over the internet, or transferred over other computer networks. [9]. Decryption aims to make secret information understandable [9]. encrypting data to prevent unauthorized individuals from accessing it.

The study of techniques to guarantee that a message may only be read by the intended recipient and sender is known as cryptography. There are three types of these pieces. Certificate Authority Digital (CA) comes first. Furthermore, Accreditation Organizations Thirdly, a public key infrastructure (PKI) is made up of the Registrar's Office hardware, software, policies, procedures, and techniques for administering, distributing, utilizing, preserving, and canceling digital certificates and public keys [21].

In asymmetric encryption, communication is encrypted and decrypted with the aid of two keys: a public key and a private key [19]. Symmetric encryption uses a single key for both the encryption and decryption procedures (a secret key).

Narro Band IoT

The Radio technology created especially for Internet of Things applications is called NB-IoT, or narrowband Internet of Things. It can be immediately installed in GSM or LTE networks to reduce implementation expenses [8]. However, advancements in wireless connectivity make the Internet of Things possible.

Repeatedly sending the same control signals and data is the main way that the 3GPP plans to expand NB-coverage IoTs. Other NB-IoT proposals consider this new capacity of repeating. The strategy will consider a two-dimensional space, much like standard

LTE systems do. Specifically, it will consider the modulation and coding scheme (MCS) level and repetition number gumption to perform a link adaptation for resource management, which will improve energy data rate and coverage efficiency.

Operation at Low Power

To cut down on upkeep costs, battery powered IoT sensors should last at least a decade before needing to be replaced. This is an essential requirement for the Internet of Things and Machine-to-Machine designs. Most studies show that battery life is significantly affected by several factors, including comparison of various IoT and progress towards 5G technology seen in Fig. 3. including network design, duty cycle, and workload distribution between end devices and base stations. When the NB-IoT system contains a large number of widely dispersed nodes, the "bottleneck problem" shows congestion at any one node in the network. This is because traffic directed to a gateway over many hops leads certain devices, depending on their location or network traffic patterns, to become increasingly crowded than others. Due to dwindling battery life, the network has a finite number of remaining months or years until it ceases to function entirely. Because the majority of NB-IoT systems feature a star network topology, where end devices link directly to base stations, there is often no need for a substantial and expensive switch and gateway deployment. This strategy conserves a great deal of energy. In a star topology, nodes conserve energy by not checking for incoming connections to relay continuously.

Most LPWAN techniques, and NB-IoT systems in particular, employ a major(star) topology in which the base station is always on and ready to provide immediate access to end devices anytime they request it. Even though the vast majority of LPWA technologies use a star topology, it’s crucial to note that certain LPWA technologies employ a tree or mesh topology. To attain the same energy efficiency performance as a star network architecture, however, these latter network architectures often require substantially more sophisticated protocol designs. Duty Cycle Management: To make NB-IoT systems run more efficiently on power, this method involves opto- tonetically turning off high-power M2M/IoT components, the radio transceiver circuit, for instance. By turning on the radio transceiver circuit only when data has to be sent or received, it has proven possible to significantly reduce the network’s power usage. Several studies on NB-IoT systems have looked at the effects of extra PHY layer parameters based on how much energy the system uses. This study suggests more research into how channel coding and modulation scheme selection affect the NB-IoT system’s overall energy usage and comparison of various IoT and progress towards 5G technology shown in Fig.2.

Blockchain Technology with Supply Chain Management

A blockchain is a distributed ledger that links several data blocks chronologically utilizing cryptographic techniques to pro- duce amazing outcomes. Blockchain was created to solve two main problems with digital currency: the double spending problem and the Byzantine generals’ dilemma. Supply chain blockchain applications have to be valued right away [12].

Blockchain technology makes it possible for the supply chain to expand, strengthen, and grow quickly. Think of it like a massive ledger. Unlike conventional databases, a central authority does not own the blockchain. However, the blockchain can accept new additions or upgrades if a majority of its members, or more than half of them, concur. Other benefits of a blockchain include its capacity to handle enormous amounts of documents and its ability to expedite procedures while maintaining uniform control over all parties involved [21]. Blockchain can change several aspects of the supply chain. Every transaction on the blockchain is kept on a block. These entries are subsequently spread over a larger number of devices as a

result of the enormous number of copies on the ledger, improving accessibility [22]. Only the block that comes before it is related to every other block, and so forth. Blockchain security is therefore difficult to breach. The goods’ data is moved and stored by the supply chain. Blockchain technology is an open, secure, and private way to store data.

According to Decker and Yeomans (2018), the blockchain is made up of blocks that hold transaction data and can only be modified by user consensus. The adoption of blockchain technology has the potential to revolutionize the supply chain by enabling companies to track their goods more effectively and guarantee that they reach their destination without incident. Businesses in the grocery market are required to monitor their items from their origins to the final consumer due to their extreme perishability and enhanced transparency [19]. For example, the supply chain management system enhanced by blockchain technology can easily monitor the source, handling, and delivery of every item [22].

Additionally, the operation becomes more efficient overall when it is sold. As a result, the final consumer benefits from higher quality service. In "Blockchain: The Future of Supply Chain Management," author Kate Mitchelmore explains how tracking an item's lifecycle can be done using blockchain technology.

"Using blockchain technology, manufacturers may promptly identify product faults and communicate them directly to suppliers, who can then recall products without waiting for government regulators to intervene or for consumers to report issues." Using blockchain technology for supply chain management can lower costs by eliminating intermediaries, which is the first advantage12]. For instance, if you wanted to purchase flowers from a flower store, you would be required to pay for this service, as someone would have to deliver it. However, if you were utilizing blockchains, there would be no need for a third party to supply this service because everything is provided by the network itself (Peirce, 2016). inapparency is increased among all system participants, which is an additional advantage of utilizing blockchain technology in supply chain management. This means that all parties will know precisely where and when their products were generated or made (Ramirez-Lopez & Soto-Acosta, 2018). Customers will be able to see exactly what they are purchasing, as opposed to depending on someone else's word on the product's ingredients and manufacturing process (Ramirez-Lopez & Soto-Acosta, 2018) Included among the downsides is the difficulty of scaling a blockchain. There may be an absence of data access limitations, and the blockchain may not be fully compliant with the laws of some nations [24]. Converting a conventional supply chain into a global supply chain is effortless. Since it relies on a network of computers having access to the same database, the technology may not be as safe as it seems [25].

Background of Literature

Numerous researchers have developed IoT networks that use blockchain technology to increase the efficiency of standard IoT architectures. In [11], the advantages of attribute-based encryption (ABE) and blockchain enhance the anonymity of IoT applications. Numerous researchers have developed IoT networks that use blockchain technology to increase the efficiency of standard IoT architectures. For example, in a paper published in the IEEE Internet of Things Journal, researchers at the University of Illinois at Urbana-Champaign used blockchain technology to create an IoT network for smart buildings. They built their system using the Ethereum platform and an open-source smart contract framework called Truffle. The researchers were able to create a decentralized system for managing access control policies, user authentication, and device authorization within buildings. They also showed how they could leverage this framework to allow users to track their energy usage. In a study by Kwon and Lee (2019), it was found that blockchain technology can be used to improve the efficiency of IoT networks. The researchers developed an IoT network that used blockchain technology to more effectively process data sent between devices. Additionally, the cost of computation suitable for IoT terminal computers is discussed in [12]. A blockchain-based IoT framework for agri-food supply chain management that enables traceability in the logistics phase is discussed [13]. Additionally, simulations on many IoT computers to demonstrate the scheme's advantages and disadvantages in terms of time delay and network consumption are also discussed. The shortcomings in the existing IoT platform and the necessary suggestions for a new scheme for managing IoT devices with greater flexibility are identified in [14]. A practical cryptographic mechanism built on blockchain technology with confidentiality and verification, their scheme was well-suited for data security in IoT systems developed in [15]. The features of IoT and blockchain before proposing ways to address IoT protection issues and how blockchain-based IoT can be extended to a variety of vertical sectors, including intelligent transportation and Knowledge tourism [16]. An architecture that incorporates the functionality of software-defined networking (SDN), and blockchain establishes a trust structure for IoT devices [17]. The blockchain-based IoT in the medical distribution sector includes the capability of monitoring real-time temperature during the logistic process's lifetime dealt in [18]. In [19], first-time authors developed the "Alky lVM" split-virtual machine and later integrated it into IoT and blockchain networks. Their concepts developed novel links between blockchain and resource constrained IoT devices. A blockchain-based, cloud- based authorization and proxy computation model for IoT is created in [20]. In [21], a lightweight framework for securing IoT devices via blockchain, and their experimental findings indicated that the design was decentralized and transparent, allowing everyone to participate in the validation mechanism and add to the blockchain based on blockchain technology in [22], authors have proposed a modern approach for achieving fine-grained access control over IoT applications. In [23], The computational costs of cryptographic algorithms used in blockchain, and which are applied to real-world IoT computers are examined. How a blockchain can be used to improve the overall protection of blockchain is discussed in [24]. The coordination process in the IoT devices examines the traffic between the blockchain network and IoT computers examined in [25]. Their research indicated that the uplink traffic generated by blockchain protocols necessitated a significant allocation of the downlink. Finally, [26] pioneered the creation of a shared network that leveraged blockchain technologies to facilitate data retrieval in IoT devices. Reference to Table 2. Proposed scheme comparing among all the above references.

Methodology

The integration of blockchain technology and IoT devices in supply chain management begins with understanding the existing supply chain challenges and requirements. Selection of appropriate IoT devices follows, ensuring they can efficiently capture relevant data points. Choosing a suitable blockchain platform based on scalability and security is pivotal. Integration involves developing communication protocols between IoT devices and the blockchain network, focusing on secure data transmission. Captured IoT data, such as shipment details or environmental conditions, is stored securely on the blockchain using smart contracts for validation and immutability. Implementing unique identifiers enables traceability, providing stakeholders with real-time access to product history and location. Smart contracts automate actions triggered by IoT events, ensuring contract terms' enforcement or triggering actions based on predefined conditions like delivery confirmation or temperature deviations. Testing, scalability planning, and stakeholder training ensure a seamless and efficient adoption of this integrated system, fostering transparency, data accuracy, and streamlined processes within the supply chain.

Blockchain eliminates the need for a centralized governing body [6]. All transactions must be robustly secured, and data must be maintained securely on a distributed ledger [7]. Blockchain is one of the architectures in the layered network depicted in Fig. 3 that enables them to authenticate transactions uniquely. Blockchains are peer-to-peer networks [8] that enable clients to connect with peer clients to expedite and simplify data sharing. A distributed ledger is created by a wide network of devices connecting [9].

This layer executes the protocol that needs a particular number of nodes to verify a single transaction; therefore, every transaction is handled by many nodes that must concur on its validity. This approach preserves the blockchain's decentralized nature [10] by ensuring that no node has exclusive authority over transaction data and by distributing the role itself. The application depicted in Fig. 3, is where smart contracts and decentralized applications should run. Contracts with artificial intelligence make judgments depending on triggers such as contract expiration dates, spot pricing, etc. The application layer also supports user device interactions with the blockchain. Each device connecting to a network is a node, and each node checks transaction data at random.

This digital signature also maintains the owner's encrypted identity, ensuring optimum network security and anonymity. The application is the front end, while the core blockchain is the back end where data is securely stored. This Five-tier blockchain contains the hardware and equipment necessary for the network's seamless operation and consensus procedures, as well as the internet connection used for blockchain network communication. Layer 1, depicted in Fig. 3, regulates blockchain security methods and consists of the consensus process, coding languages, and all the rules encoded in the blockchain's operations; it is also known as the implementation layer. Layer 2 increases processing power and nodes to enhance the entire blockchain. Layer 1 permits integration with third parties. Layer 2 is a new network that administers authentication, decongests Layer 1, and generates and adds blocks to the blockchain. The third layer consists of the smart contracts depicted in Fig. 3 and applications that govern decision-making and subsequent operations. Since the maximum functionality of the blockchain is the layer that interfaces between real-world applications and the underlying layers that sup- port everything depicted in Fig. 3, in the distributed network of the blockchain architecture, each member maintains, approves, and updates new entries, resulting in blocks containing transactions in a particular order. The design of blockchains may employ public-private and consortium structures as necessary. Blockchain is a service layer consisting of a multi-layered architecture with blockchain technology and NB-IoT illustrated in Fig. 4 consuming less power as compared to the single- and two-layer architectures given in the conclusion.

Table 1
Notations for Math Formula

Symbols	Definitions
Z	Required quantity of retailers to distributors
Y1	The quantum of wholesale price of products for the distributor
y2	The amount of the manufacturer's wholesale price of products
r	Prices at retail
d1	The order cost for the store
d2	The order cost for the distributor
d3	The manufacturer's marginal order cost
d4	The Costs of the Internet of Things (IoT)
d5	RFID tags are priced per unit.
d6	IoT unit maintenance costs
d7	The cost of IoT hardware and software
d8	Another cost to consider (in terms of business processes, services, timing, and education)
y1	Product wholesale price per unit for the distributor
y2	For the manufacturer, one unit wholesale price of products
d(θ)	Freshness control costs money.
α·c(θ) and β·c(θ)	Freshness control costs are shared by the retailer and distributor.
τ	The IoT application's complexity (0, 1)
	Rate of radio frequency identification tag recycling
λ	Total supply chain profits
υ1	Retailer revenue distribution rate (0, 1)
Y2	The distributor's revenue distribution rate (0, 1)
μRS	Retailer profit
μDS	Distributor profit
μMS	Manufacturer profit

Table 2
Proposed scheme comparing among the references.

Sloe.	Description of Features	Refn. et. al in [1] 2016	Refn. et. al in [2] 2017	Refn. et. al in [3] 2016	Refn. et. al in [4] 2016	Refn. et. al in [5] 2017	Refn. et. al in [19] 2017	Refn. et. al in [20] 2018	Proposed Scheme Supply Chain Using Black Chain with NB-IoT
1	Base Station Gain			×	×	×	×		
2	Base Station Coverage			×	×	×	×		
3	Short Term Standby			×	×	×	×		
4	Connectivity Performance			×	×	×	×		
5	Power Consumption			×	×	×	×		
6	Longer Durability of Battery			×	×	×	×		
7	Cost of Implementation Low			×	×	×	×		
8	Deep Signal Access Possibility			×	×	×	×		
9	Scalability (Upgradation)		×	×	×	×	×		
10	Tx-Throughput High		×	×	×	×	×		
11	De-Centralized Infra Ledger		×						
12	Confidentiality (Trust)		×						
13	Privacy		×						
14	Accuracy		×						
15	Authentication		×						
16	Transparency		×						
17	Traceability		×					×	
18	QR Code for Product History	×	×	×	×	×	×	×	

Mathematical model for supply-chain implementation for smart contracts

The use of smart contracts in the management of supply chains, farming, and the Internet of Things is growing quickly (IoT). Digital contracts known as "smart contracts" can be automatically recorded and carried out on a blockchain database shown in Fig. 4 model for supply chain management with blockchain technology and NB-IoT. Without the involvement of a third entity, such as an escrow company or lawyer, smart contracts allow the exchange of money, assets, shares, or anything else of value between two parties. Smart contracts automatically execute when specific circumstances are satisfied.

As more organizations implement blockchain technologies for supply chain management, smart contracts will also become more common. The agricultural industry could also benefit from the use of smart contracts to assist farmers in

tracking their produce from seed to sale to earn just remuneration for their labor. In addition, IoT devices might employ smart contracts to ensure that payment is only made when particular criteria are met, such as when items are delivered or when customers have paid for them through an online retailer. Table No.2 symbols and definitions mentioned for the mathematical formulas as given below with reference to the Table 1 Notations for Math Formula.

Mathematical model of Agri products using supply chain management

$$x = y(p,\theta) + n, p \in (c, p_{o)},\theta \in (\theta_o, 1)$$

1

where P_o $\rightarrow$maximum retailer price.

$$y\left(P_o,\theta\right) = 0$$

2

θ_o $\rightarrow$ The lowest quality of freshness in Agri products.

$\theta < \theta_o, y\left(P,\theta\right) = 0 \rightarrow$ acceptable to customers.

$$f\left(\eta\right) = \lambda e^{-\lambda\eta}$$

3

$$F\left(\eta\right) = 1 - e^{-\lambda\eta}$$

4

Here η is the exponential distribution.

$$F^{-1}\left(z\right) = -\left(\frac{1}{\lambda}\right) lnln(1-z), -\lambda > 0{,}0 < z < 1$$

5

Now the fresh Agri product sale monetization can be given as below.

$$S(r,z,\theta) = E[min(z,x)] = \int_0^x xf(x - y(r,\theta))\,dx + r\int_q^{+\infty} f(x - y(r,\theta))\,dx$$

6

$$= r - \int_{y(p,\theta)}^{q} F(x - y(r,\theta)dx = z - \int_0^{q-y(p,\theta)} F\left(x\right)dx \quad \textbf{(7)}$$

The total gain or profit in modern Agri products in supply chain management can be expressed as

$$.S(r,z,\theta)-(d_1+d_2+d_3).$$
$$z-r.\left(d_6+d_7+d_8+d_5.\left(1-\gamma\right)\right).z-d\left(\theta\right) \textbf{ (8)}$$

Were,

R $S(r,z,\theta)$ is sale revenue, $(d_1+d_2+d_3)$ is producing and ordering cost, $R(d_6+d_7+d_5(1-\omega)].q$ is IoT maintenance cost, $d$is freshness control cost, $d_4=r(d_6+d_7+d_5(1-\omega)$ is demand, and r is complexity in IoT technical application

$$\text{Assume}, d=d_2+d_3+d_4+d_1.\mu_1=r$$

$$S\left(r,z,\theta\right)-C.z-d\left(\theta\right)$$

9

The total profit of supply chain management of modern Agri products can be given by

$$\frac{\partial\mu_z}{\partial\theta_1^*}=r(\frac{\partial S\left(r,z_1\theta_1^*\right)}{\partial\theta_1^*}-d^1(\theta_1^*)=0$$

10

$$\frac{\partial\mu_1}{\partial{r_1}^*}=S\left({r_1}^*,z,\theta\right)+{p_1}^*.\frac{\partial s\left({r_1}^*,z,\theta\right)}{\partial{r_1}^*}=0$$

11

$$\frac{\partial\mu_1}{\partial r_1^*}=r(\frac{\partial S\left(r,z_{1,}^*\theta\right)}{\partial z_1^*}-d=0$$

12

The centralized decision for optimal order is calculated as $z_{1,}^*=F_{,}^{-1}\left(1-\frac{C}{r}\right)+y\left(r,\theta\right)$ (13)

The value of μ_i is generalized as

$$\mu_i=(r-d)\left(a-k^2\frac{(r-d)}{2a}-lr\right)+\frac{r-d+(lnr-lnd)\,d}{\lambda}$$

14

Now,

$$\frac{\partial\mu_1}{\partial r_1^*}=a+\frac{1}{\lambda}-\left(\frac{k^2}{a}-l\right)d+\left(\frac{k^2}{a}-2l\right)r_1^*+\frac{d}{\lambda}.\frac{1}{r_1^*}=0$$

15

Therefore, now the optimal retailer price can be calculated.

as $r_1^*=\frac{-\left[a+\frac{1}{\lambda}\left(l-\frac{k^2}{a}\right)d\right]\pm\sqrt{[a+\frac{1}{\lambda}-(l-\frac{k^2}{a})d]^2-4(\frac{k^2}{a}-2l)\frac{d}{\lambda}}}{2\left(\frac{k^2}{a}-2l\right)}$ (16)

The freshness of agriproducts impacts on retailer profit is shown in Fig. 5, distributor price and $\phi1$ coefficient shown in Fig. 6, and revenue sharing Co- Co-Efficient combined range between $\phi1$ and $\phi2$ in Fig. 7.

The Agri product's quality is analyzed by the farmer and the maximum retail price is calculated by fixing the base price on the different qualities of the product with expenditure and charges mentioned in the above mathematical model records are stored in a decentralized and distributed manner in the cloud called public ledger by implementing in smart contract revenue sharing model among the producer, distributer and retailer using blockchain technology shared in publicly using NB-IoT.

This mathematical model details are mentioned in the centralized and decentralized decision-making for profit margin in supply chain management of modern Agri products. The Profit of the Agri Product earned by the farmer in the above mathematical model analyzed and given is the maximum retailer price fixed by the former based on the supply and demand after analyzing the quality of the product and other parameters as mentioned below.

Where $rs\ (r, z, \theta)$ is sale revenue. $(d_1 + d_2 + d_3)$ producing and ordering costs.

$R\ (d_6 + d_7 + d_5(1 - \omega)]$. q is IoT maintenance cost.

$d(\theta) \rightarrow$ freshness control cost.

$d_4 = R\ (d_6 + d_7 + d_5(1 - \omega) \rightarrow$ demand

RESULTS AND ANALYSIS

Signal-to-noise ratio (SNR) in terms of 16 QAM in OFDM modulation technique optimizing Bit Error rate (BER), Symbol Error rate (SER), and Frame Error rate (FER) at the maximum power of 25db using MAT Lab simulation graphical results in multi-layer, double-layer and single-layer.

The following Error Rate calculations as mentioned below:

1. **Bit Error Rate (BER)**: This measures the probability of an incorrect bit reception. For 16-QAM, the BER can be mathematically expressed as:
2. **Symbol Error Rate (SER)**: SER is the probability that a transmitted symbol is received incorrectly. The formula for SER depends on the modulation scheme and the SNR. For 16-QAM, the SER formula is complex and involves the Q-function.
3. **Frame Error Rate (FER)**: FER indicates the likelihood of errors within a frame of symbols. It's influenced by the number of symbols per frame and the error rates of individual symbols.

The below equations provide an estimate of the Bit error rate, Symbol Error Rate, and Frame Error Rate for a 16-QAM

modulation scheme. They are derived based on statistical models and are used to analyze and predict the performance of communication systems using this modulation scheme under specific signal-to-noise conditions.

The following Error Rate calculations as mentioned below:

1. **Bit Error Rate (BER)**: This measures the probability of an incorrect bit reception. For 16-QAM, the BER can be mathematically expressed as:
2. **Symbol Error Rate (SER)**: SER is the probability that a transmitted symbol is received incorrectly. The formula for SER depends on the modulation scheme and the SNR. For 16-QAM, the SER formula is complex and involves the Q-function.
3. **Frame Error Rate (FER)**: FER indicates the likelihood of errors within a frame of symbols. It's influenced by the number of symbols per frame and the error rates of individual symbols.

The below equations provide an estimate of the Bit error rate, Symbol Error Rate, and Frame Error Rate for a 16-QAM modulation scheme. They are derived based on statistical models and are used to analyze and predict the performance of communication systems using this modulation scheme under specific signal-to-noise conditions.

1) **Bit Error Rate (BER) Calculation**:

The formula for BER in 16-QAM at an SNR of 25 dB is:

$$BER = \frac{3}{2}\frac{erfc(\sqrt{\frac{0.8SNR}{log_2(M)}}}{log_2(M)}$$

23
For 16-QAM (M = 16) and SNR of 25 dB

$$BER = \frac{3}{2}.\frac{erfc(\sqrt{\frac{0.8(25)}{log_2(M)}}}{log_2(16)}$$

24
Solving this equation will give you the Bit Error Rate at 25 dB SNR in Fig. 8.

2) **Symbol Error Rate (SER) Calculation**:

The SER formula for 16-QAM involves the Q-function and is:

$$SER = \frac{3}{2}.\frac{2}{log_2(M)}erfc\left(\sqrt{\frac{3(SNR)}{2(M-1)}}\right) - \frac{3}{2}\left(\frac{2}{log_2(M)}\right)^2 erfc^2\left(\sqrt{\frac{3(SNR)}{2(M-1)}}\right)$$

(25)

For 16-QAM (M = 16) and an SNR of 25 dB, plug in these values to find the Symbol Error Rate in Fig. 9.

3) **Frame Error Rate (FER) Calculation**:

The FER depends on the SER and the number of symbols per frame. The equation is:

$$FER = 1 - (1 - SER)^N$$

(26)

Here, (N) represents the number of symbols per frame. To determine the Frame Error Rate at an SNR of 25 dB, you'll need to know the number of symbols per frame in your system in Fig. 10

These calculations will provide you with estimates of the error rates (BER, SER, FER) at a signal-to-noise ratio of 25 dB in a 16-QAM system. Simulation Parameters of energy consumption rate as shown in Table 3.

Simulation Environment

Simulation Parameters Energy Consumption Rate at 25(dB) Value

Parameter Bit Error Rate (BER) Symbol Error Rate (SER) Frame Error Rate (FER) Multi-Layer 10 −2.5 10 −8 10 −8

Two Layer 10 −2 10 −7 10 −6

Simulation Environment			
Simulation Parameters	**Energy Consumption Rate at 25(dB) Value**		
Parameter	Bit Error Rate (BER)	Symbol Error Rate (SER)	Frame Error Rate
(FER) Multi-Layer	$10^{-2.5}$	10^{-8}	10^{-8}
Two Layer	10^{-2}	10^{-7}	10^{-6}
Single Layer	$10^{-1.5}$	10^{-5}	10^{-4}

Table 3. Simulation Parameters

As shown in Fig. 8, among the three layers, multi-layer security consumes the least bit error rate and produces the least energy consumption rate. Two-layer security is the second least security which consumes a moderate bit error rate and produces a moderate energy consumption rate. Single-layer security consumes the highest bit error rate and produces the highest energy consumption rate compared to the other two layers: single-layer security and two-layer security in graph Fig. 8 with increasing energy consumption rate. But it is saturated for low values of energy consumption rate, i.e., the Bit error rate converges to the maximum value.

Among the three layers, multi-layer security consumes the symbol error rate and produces the least energy consumption rate. Two-layer security is the second least security which consumes a moderate and produces a moderate energy consumption rate.

Single-layer security consumes the highest symbol error rate and produces the maximum energy consumption rate com- pared to the other two layers: single-layer security and two-layer security in graph Fig. 9 with increasing energy consumption rate. But it is saturated for low values of energy consumption rate, i.e., the symbol error rate converges to the maximum value.

The Frame error rate that is presented in Fig. 10 is for different values of the Energy Consumption Rate. As seen among the three layers, multi-layer security consumes the least frame error rate and produces the least energy consumption rate. Two-layer security is the second least security which consumes a moderate frame error rate and produces a moderate energy consumption rate.

Single-layer security consumes the highest frame error rate and produces the maximum energy consumption rate compared to the other two layers: single-layer security and two-layer security in the graph Fig. 10 with increasing energy consumption rate. But it is saturated for low values of energy consumption rate, i.e., the frame error rate is converged to the maximum value.

Weakness of the Blockchain Technology with NB-IoT There are still unanswered security concerns, despite the enormous benefits given by systems like blockchain technologies. Transactions explore and draw attention to several unresolved issues, including resource constraints, device heterogeneity, single points of failure, hardware and firmware vulnerabilities, trusted updates, administration, and blockchain vulnerabilities. These open questions provide openings for investigations into how NB-IoT network security management might be improved.

CONCLUSION

This study investigates analyses and discusses the various problems with network resource efficiency in NB-IoT design and implementation. Data rates, network dependability, and performance scalability have all been taken into account. The analysis also included recommendations for future studies that could help solve the serious problems plaguing existing NB-IoT models. We suggest an energy-efficient technique for MCS selection, and we will simulate the PHY layer of an NB-IoT network in future research. This paper provides an accessible and concise review of the most important network resource factors, making it a helpful tool for any researcher interested in studying the evolution of NB-IoT network performance with mathematical models, an intelligent smart contract revenue-sharing model has been developed, which authenticates data displayed in graphical representations, generates blockchain in a decentralized and distributed manner using blockchain technology and NB-IoT, and maximizes profits for all parties involved in the supply chain, from manufacturer to distributor to retailer. For single-layer, two-layer, and multi-layer transmissions over AWGN channels modulated with 16-Qam, optimal simulation results of power versus bit error rate (BER), frame error rate (FER), and symbol error rate (SER) are obtained for the OFDM scheme. Power losses are seen to be minimized in multi-layer systems in (Figs. 8, 9, and 10) as compared to single-and double -layer systems.

Declarations

ACKNOWLEDGMENT

We would like to express our heartfelt gratitude to the esteemed Lovely Professional University for their contribution to the achievement of this initiative. It is a knowledge center where anyone may learn and upgrade their expertise in any field. Second, we worked together as a team to accomplish this project successfully. As a result, we are pleased to say that our collaboration is good and that we will continue to have tremendous success in the future.

Data Availability

Data is provided within the manuscript or supplementary information files.

References

1. Ratasuk R, Vejlgaard B, Mangalvedhe N, et al. NB-IoT system for M2M communication. In: Proceedings of the IEEE Wireless Communications and networking conference workshops (WCNCW), Doha, Qatar, 3–6 April 2016, pp.428–432. New York: IEEE.
2. Kim H, Cho S, Oh J, et al. Analysis of LTE and NB-IoT coexistence. In: Proceedings of the International Conference on information and Communication Technology Convergence (ICTC), Jeju, South Korea, 18–20 October 2017, pp.870–872. New York: IEEE.
3. Mangalvedhe N, Ratasuk R and Ghosh A. NB-IoT deployment study for low power wide area cellular IoT. In: Proceedings of the 27th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), Valencia, 4–8 September 2016, pp.1–6. New York: IEEE.
4. Chang YCP, Chen S and Wang T-J. Fog computing node system software architecture and potential applications for NB-IoT industry. In: Proceedings of the International Computer Symposium (ICS), Chiayi, Taiwan, 15–17 December 2016, pp.727–730. New York: IEEE.
5. Shin E and Jo G. Structure of NB-IoT Node system. In: Proceedings of the international conference on information and communication technology convergence (ICTC), Jeju, South Korea, 18–20 October 2017, pp.1269–1271. New York: IEEE.
6. Henry R, Herzberg A and Kate A. Blockchain access privacy: challenges and directions. IEEE Securer 2018; 16(4): 38–45.
7. Ehmke C, Wessling F and Friedrich CM. Proof-of-property—a lightweight and scalable blockchain protocol. In: Proceedings of the IEEE/ACM 1st international workshop on emerging trends in software engineering for blockchain (WETSEB), Gothenburg, 27 May–3 June 2018, pp.48– 51. New York: IEEE.
8. Khatri N. Can blockchain strengthen the Internet of Things? IT Prof 2017; 19(4): 68–72.
9. Hong H and Sun Z. Towards secure data sharing in cloud computing using attribute-based proxy re-encryption with keyword search. In: Proceedings of the IEEE 2nd international conference on cloud computing and big data analysis (ICCCBDA), Chengdu, China, 28–30 April 2017, pp.218–New York: IEEE.
10. Hong H and Sun Z. sharing your privileges securely: a key-insulated attribute-based proxy re encryption scheme for IoT. Worldwide Web 2018; 21(3): 595–607.
11. Rahulamathavan Y, Phan RC-W, Rajarajan M, et al. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In: Proceedings of the international conference on advanced networks and telecommunications systems (ANTS), Bhubaneswar, India, 17–20 December 2017, pp.1–6. New York: IEEE.
12. Caro MP, Ali MS, Vecchio M, et al. Blockchain-based traceability in agri-food supply chain management: a practical implementation. In: Proceedings of the IoT vertical and topical summit on agriculture—Tuscany (IOT Tuscany), Tuscany, 8–9

May 2018, pp.1–4. New York: IEEE.

13. Huh S, Cho S and Kim S. Managing IoT devices using blockchain platform. In: Proceedings of the 19th international conference on advanced communication technology (ICACT), Tongyeong, South Korea, 19–22 February 2017, pp.464. New York: IEEE.
14. Kravitz DW and Cooper J. Securing user identity and transactions symbiotically: IoT meets blockchain. In: Proceedings of the global Internet of Things summit (Griots), Geneva, 6–9 June 2017, pp.1–6. New York: IEEE.
15. Jha, Sudan, Sultan Ahmad, Hikmat AM Abdeljaber, Nashwan Adnan Othman, Jabeen Nazeer, Kusum Yadav, and Ahmed Hussein Alkhayyat. "Enabling Resilient Wireless Networks: OFDMA-Based Algorithm for Enhanced Survivability and Privacy in 6G IoT Environments." IEEE Transactions on Consumer Electronics (2024).
16. Li S. Application of blockchain technology in smart city infrastructure. In: Proceedings of the international conference on smart Internet of Things (Smartt), Xi'an, China, 17–19 August 2018, pp.276–382. New York: IEEE.
17. Kataoka K, Gangway S and Podila P. Trust list: Internet wide and distributed IoT traffic management using blockchain and SDN. In: Proceedings of the fourth world forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018, pp.296–301. New York: IEEE.
18. Bocek T, Rodrigues BB, Strasser T, et al. Blockchains everywhere—a use-case of blockchains in the pharma supply-chain. In: Proceedings of the 2017 IFIP/IEEE
19. Bocek T, Rodrigues BB, Strasser T, et al. Blockchains everywhere—a use-case of blockchains in the pharma supply-chain. In: Proceedings of the 2017 IFIP/IEEE symposium on integrated network and service management (IM), Lisbon, 8–12 May 2017, pp.772–777. New York: IEEE.
20. Ellul J and Pace GJ. Alkyl: a virtual machine for smart contract blockchain connected Internet of Things. In: Proceedings of the 9th IFIP international conference on new technologies, mobility and security (NTMS), Paris, 26–28 February 2018, pp.1–4. New York: IEEE.
21. Son LH, Jha S, Kumar R, Chatterjee JM, Khari M. Collaborative handshaking approaches between internet of computing and internet of things towards a smart world: a review from 2009–2017. Telecommunication Systems. 2019 Apr 15;70:617-34.
22. Tapas N, Merlino G and Longo F. Blockchain-based IoT-cloud authorization and delegation. In: Proceedings of the ninth international conference on smart computing (SMARTCOMP), Taormina, 18–20 June 2018, pp.411– 416. New York: IEEE.
23. Awasthi S, Johri P and Khatri SK. IoT based security model to enhance blockchain technology. In: Proceedings of the international conference on advances in computing and communication engineering, Paris, 22–23 June 2018, pp.133–137. New York: IEEE.
24. Shakya, S.R. and Jha, S., 2022. Challenges in Industrial Internet of Things (IIoT). In *Industrial Internet of Things* (pp. 19-39). CRC Press.
25. Ouida A, El kalam AA and Oakman AA. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In: Rocha A', Serhii M and Felgueiras C (eds) Europe and MENA Cooperation advances in information and communication technologies (Advances in Intelligent Systems and Computing, vol. 520). Cham: Springer, pp.523–533.
26. Urien P. Towards secure elements for trusted transactions in blockchain and blockchain IoT (Biota) platforms. In: Proceedings of the 2018 fourth international conference on mobile and secure services (Moiseev), Miami Beach, FL, 24–25 February 2018. New York: IEEE.
27. Miraz MH and Ali M. Blockchain enabled enhanced IoT ecosystem security. In: Proceedings of the international conference on advances in computing and communication engineering, Paris, 22– 23 June 2018, pp.133–137. New York: IEEE.
28. Puri, V., Jha, S., Kumar, R., Priyadarshini, I., Abdel-Basset, M., Elhoseny, M. and Long, H.V., 2019. A hybrid artificial intelligence and internet of things model for generation of renewable resource of energy. *Ieee Access*, *7*, pp.111181-111191.
29. Danzi P, Kalør AE, Stefanovic´ C, et al. Analysis of the communication traffic for blockchain synchronization of IoT devices. In: Proceedings of the IEEE international conference on communications (ICC), Kansas City, MO, 20–24 May 2018, pp.1–7. New York: IEEE.
30. Jha, S., Jha, N., Prashar, D., Ahmad, S., Alouffi, B. and Alharbi, A., 2022. Integrated IoT-based secure and efficient key management framework using hashgraphs for autonomous vehicles to ensure road safety. *Sensors*, *22*(7), p.2529.

31. Opiate O, Lomotil RK and Deters R. Using blockchain to support data and service management in Io/IoT. In: Peng SL, Wang SJ, Balas V, et al. (eds) Security with intelligent computing and big-data services. SICBS 2017 (Advances in Intelligent Systems and Computing, vol. 733). Cham: Springer, pp.344–362.
32. Jha, S., Routray, S. and Ahmad, S., 2022. An expert system-based IoT system for minimization of air pollution in developing countries. *International Journal of Computer Applications in Technology*, *68*(3), pp.277-285.

Figures

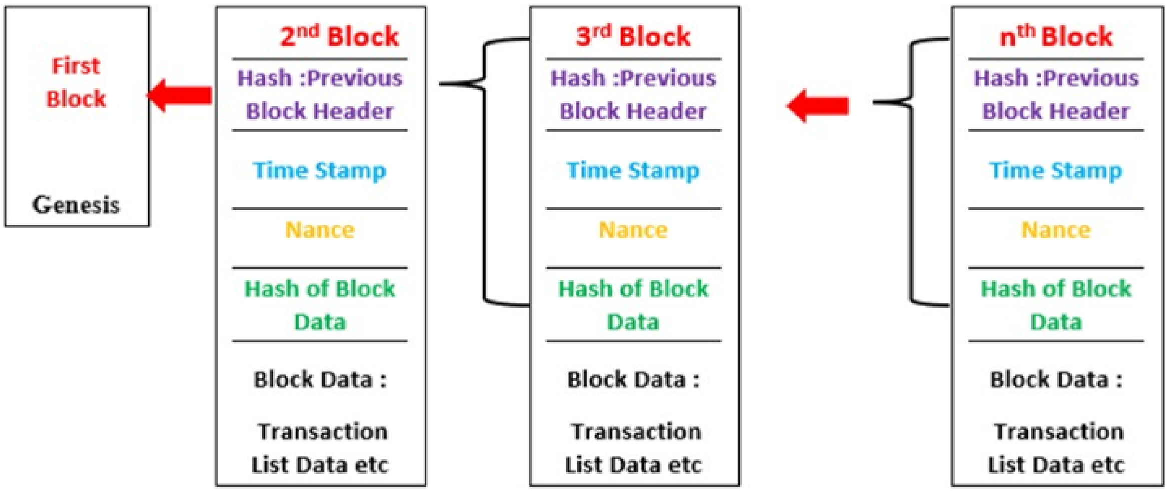

Figure 1

Generic blockchain

	NB-IoT	WIFI	BLUETOOTH	SIGFOX	LoRa	LTE-M/ (eMTC) (Rel 13)	EC-GSM (Rel. 13)	ZIGBEE Pro	5G (targets)
	Lte NB-IoT	WiFi	Bluetooth	SIGFOX	LoRa	Lte eMTC	GSM	ZigBee Alliance	5G
Coverage Area	<15 km 164 dB	17-30+ (meters)	1-10+ (meters)	<12km 160 dB	<10 km 157 dB	<10 km 156 dB	<15 km 164 dB	1-100+ (meters)	**<12km 160 dB**
Spectrum Bandwidth	Licensed 7-900MHz 200 kHz shared	2.4 GHz 802.11	2.4 GHz 802.15.1	Unlicensed 900MHz 100kHz	Unlicensed 900MHz <500kHz	Licensed 700MHz-900MHz 1.4 MHz shared	Licensed 800MHz-900MHz shared	2.4G 802.15.4	Licensed 700MHz-900MHz shared
Rate	<50 kbps	150Mbps	1Mbps	<100bps	<10 kbps	<1 Mbps	10 kbps	250kbps	<1 Mbps
Terminal cost	4.00$ (2015) 2-3$ (2020)	4.00$ (2016)	4.00$ (2016)	4.00$ (2015) 2.64$ (2020)	4.00$ (2015) 2.64$ (2020)	5.00$ (2015) 3.30$ (2020)	4.5$ (2015) 2.97$ (2020)	3.00$ (2016)	<2$
Network Reforming	Small to moderate	None	None	Large	Large	Small	Moderate (LTE reuse)	None	Requires 5G NWs

Figure 2

Comparison of various IoT and progress towards 5G technology.

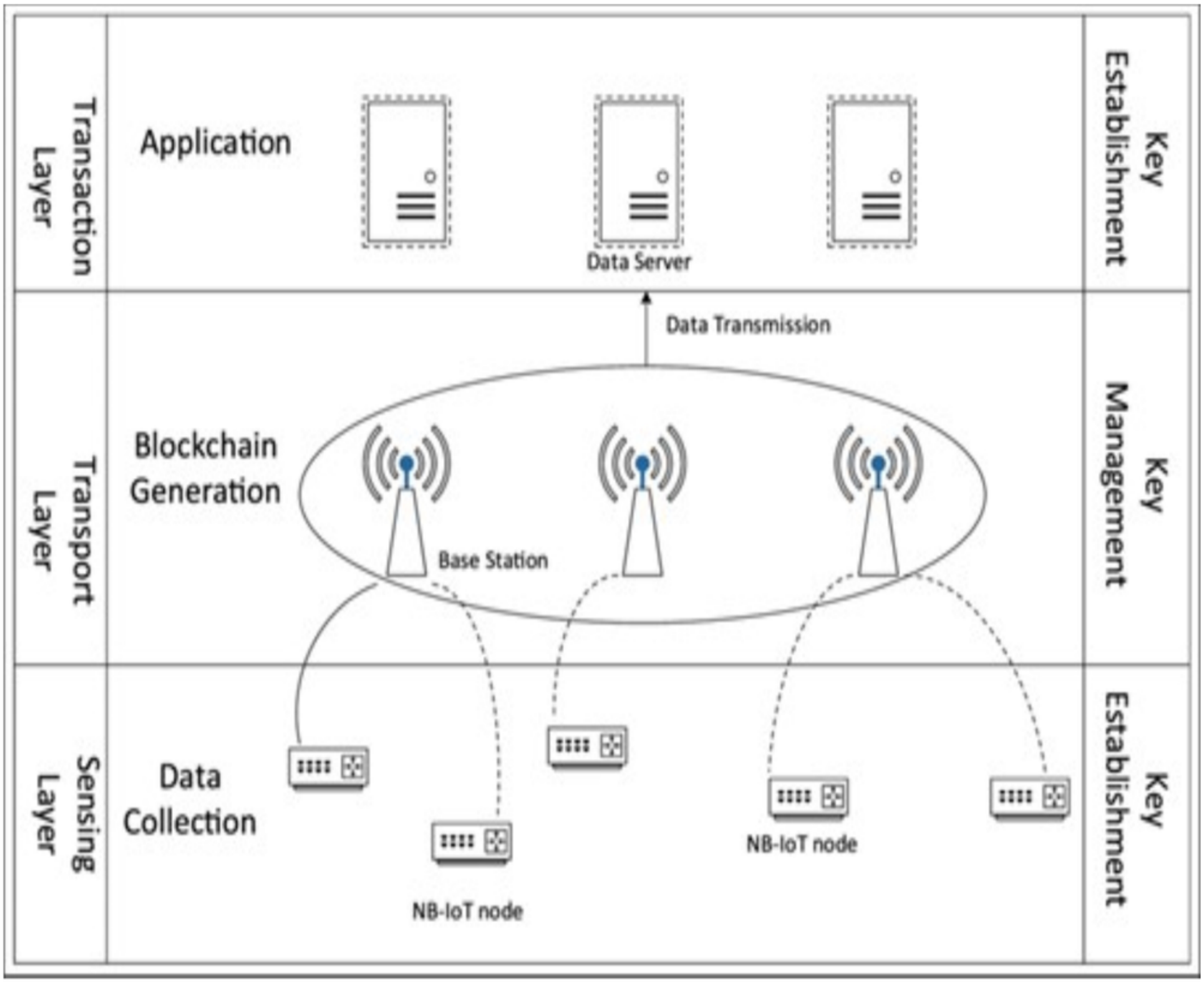

Figure 3

Multi-layer-based architecture with blockchain Technology and NB-IoT

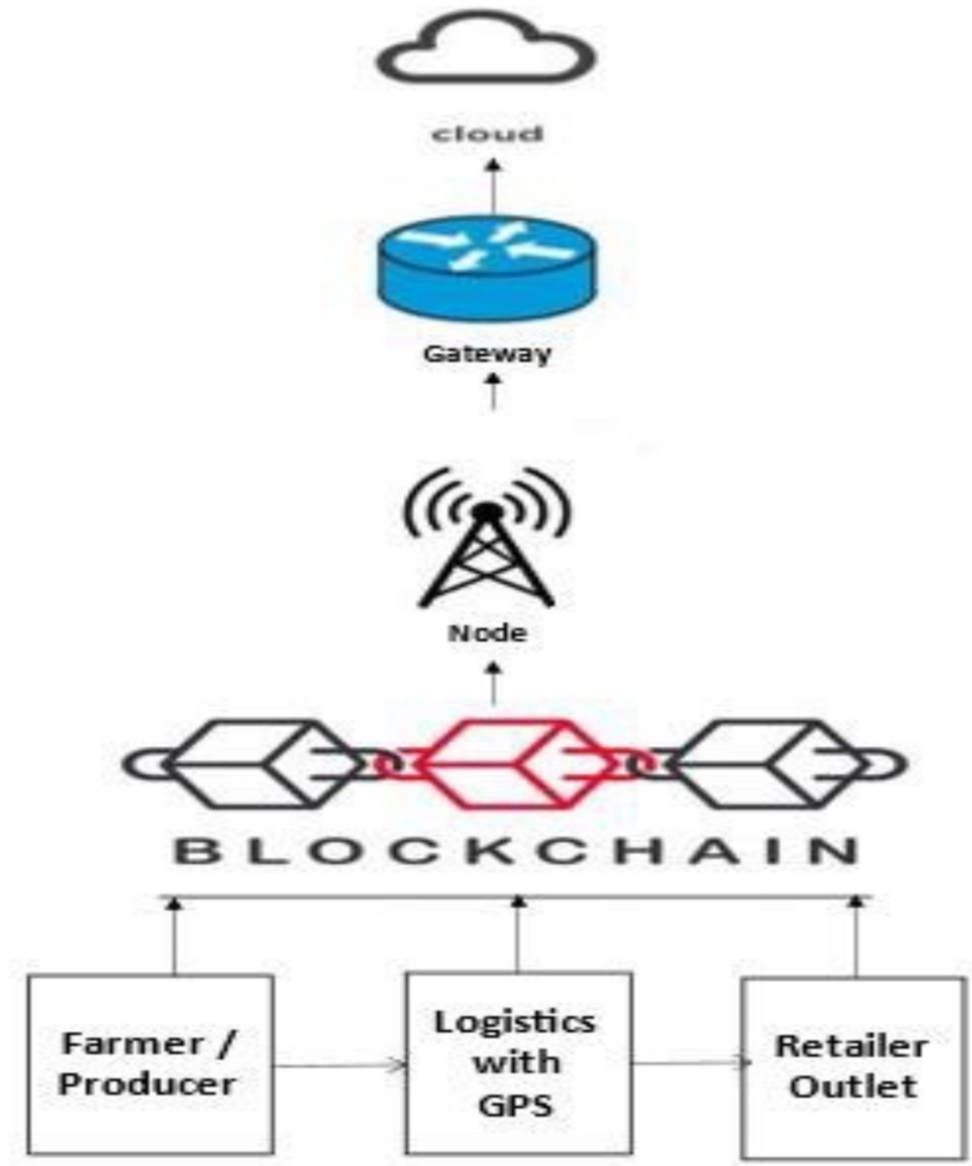

Figure 4

The Implementation model for supply chain management with blockchain technology and NB-IoT.

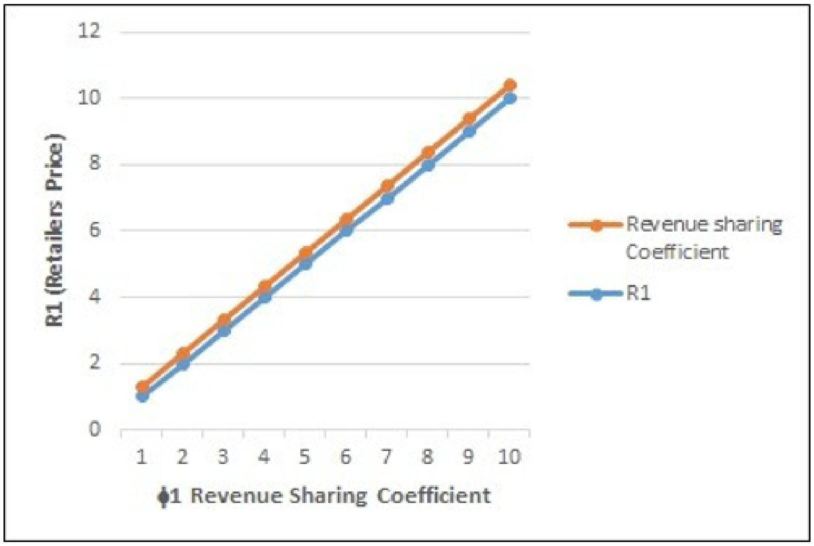

Figure 5

The Correlation Between retailers' price and revenue sharing coefficient

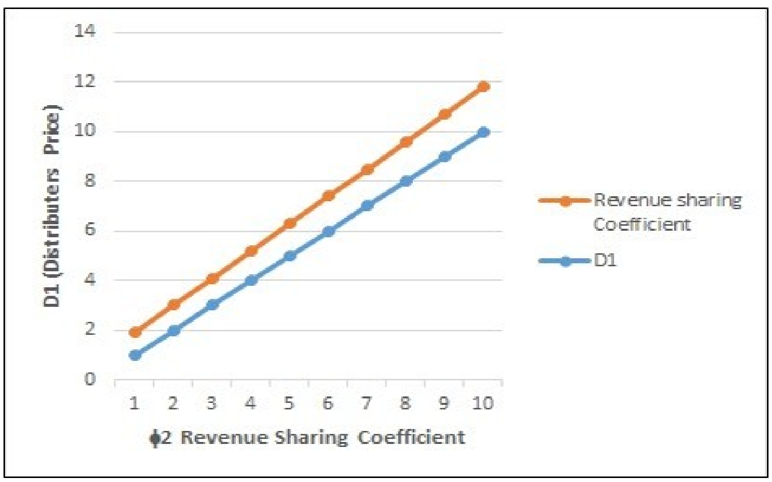

Figure 6

The correlation between the distributor's price and revenue sharing coefficient.

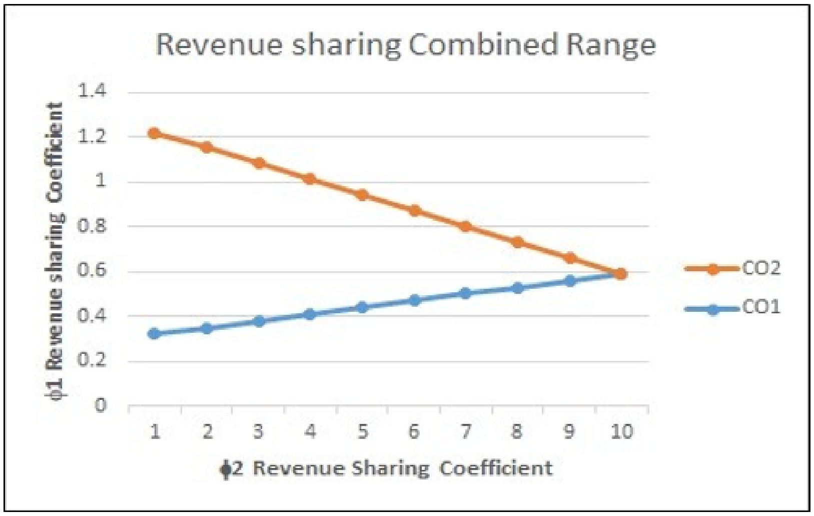

Figure 7

Revenue Sharing Co-Efficient Combined range of $\phi 1$ and $\phi 2$

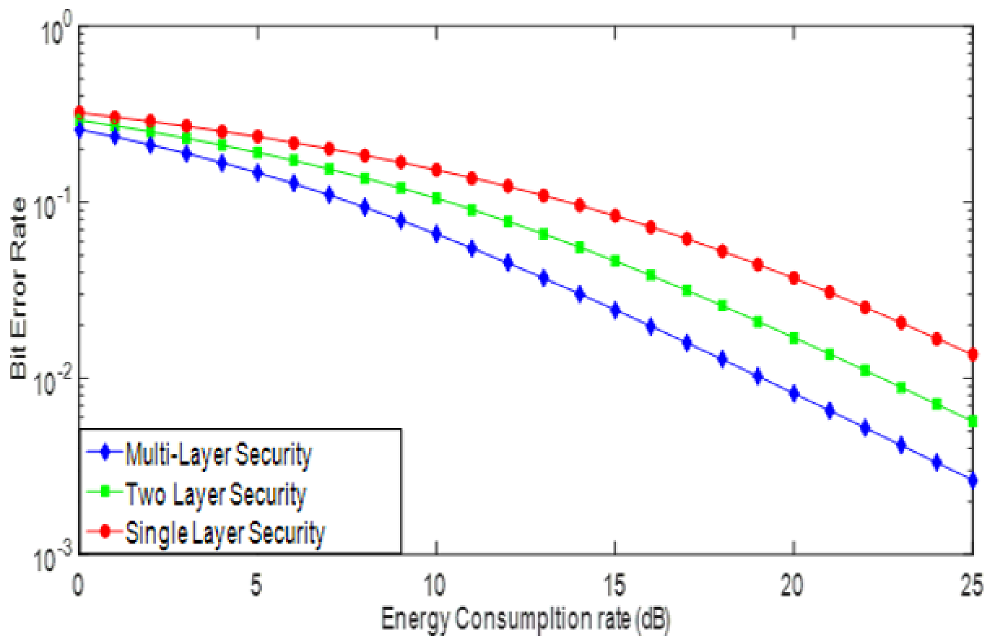

Figure 8

Bit Error Rate vs. Energy Consumption Rate (dB)

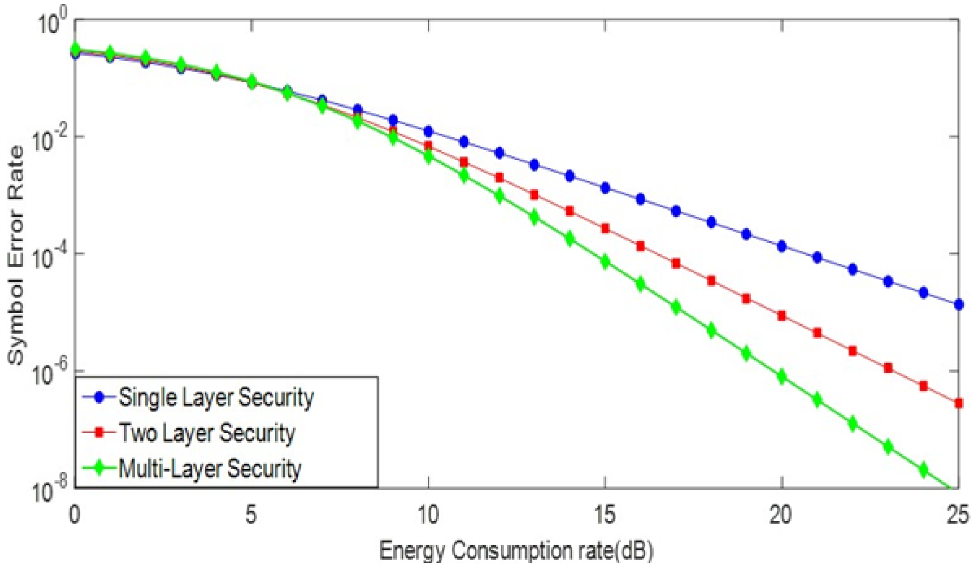

Figure 9

Symbol Error Rate v/s Energy Consumption Rate (dB)

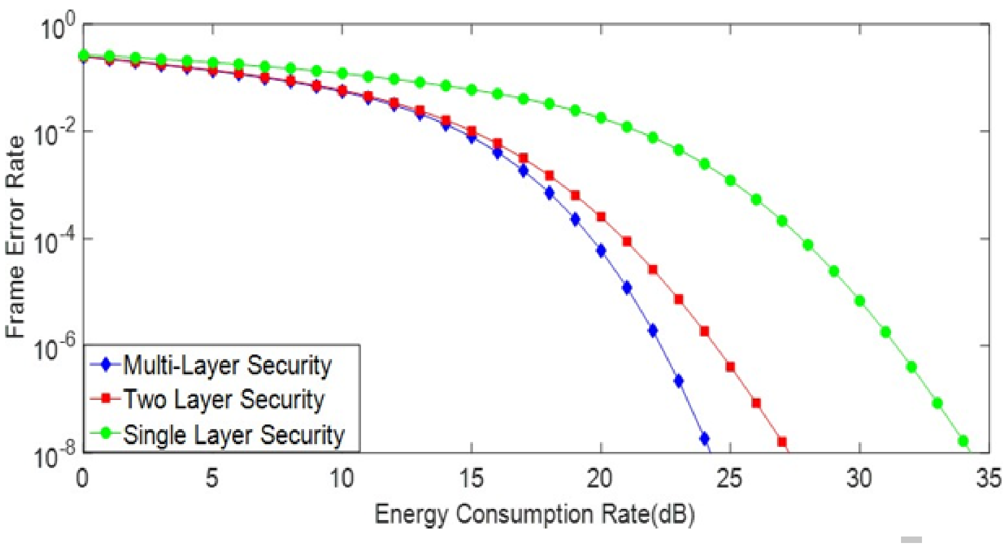

Figure 10

Frame Error Rate v/s Energy Consumption Rate (dB)

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- APPENDIX.docx