International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. #, No.# (Mon-20..)

Secure Data Storage using the Internet of Things (IoT) and a New, Affordable Blockchain Model

Challapalli Sujana[1], Mylavarapu Kalyan Ram[2], Dr. RVS Lalitha[3], Divya Lalita Sri Jalligampala[4] and

[1] Computer Science and Engineering, Aditya College of Engineering and Technology (A), Surampalem, India
[2] Computer Science and Engineering, Aditya Engineering College (A), Surampalem, India
[3]Computer Science and Engineering, Aditya College of Engineering and Technology (A), Surampalem, India
[4]Computer Science and Engineering, Aditya College of Engineering and Technology (A), Surampalem, India

E-mail address: Sujana.challapalli@acet.ac.in, kalyanram.mylavarapu@aec.edu.in, rvslalitha@acet.ac.in, divya.jalligampala@acet.ac.in

Abstract: Data processing and storage in outsourced contexts has recently shifted to edge-related smart computing. Smart, interconnected, Internet of Things (IoT) software denied networks prioritize security above all else when it comes to sharing data and making it more scalable and efficient. In real-time computing systems, a variety of security-based issues may arise in operating resources and sharing data due to the fast expansion of various smart services. Boost the trustworthiness of encrypted data storage while meeting the fundamental needs of smart computing networks associated with the Internet of Things. Therefore, to offer effective and safe data storage for intelligent computer systems. related to the Internet of Things (IoT), suggest and develop a Novel Low Cost based Block chain Secure Model (NLCBSM). Using an AI calculation approach called the Leverage Bat algorithm to investigate intricate aspects, this model can adaptably record user verification for the purpose of detecting various attacks connected to users, such as distributed denial-of-service (DDOS) attacks on data reserve. Construct a a server-side blockchain end to furnish trustworthy data storage and safe transmission on the IoT terminal. As an additional data transmission mechanism, we make use of the Merkle tree, which offers low-cost communication overhead. This method employs a weighted data storage system to organize and categorize information for every individual, along with safe and unsecure storage options available in networks of intelligent computers, and each piece of data is assigned a random hash value to guarantee data integrity in the blockchain. The suggested model's experimental results show that it can investigate intricate secure characteristics, guarantee secure the authentication's operational efficiency for each user, and improve the communications overhead, accuracy, and security of smart computing data storage and sharing systems related to the Internet of Things.

Keywords: Internet of Things, Smart Computing, Block chain, Software Defined Networks, Artificial Intelligence, Bat Algorithm

1. INTRODUCTION

A developing technology that describes the association existing between the cyber and physical worlds is the Internet of Things (IoT). Barriers like efficacy, accessibility, and adaptability are brought up by the current state of IoT networks, which are maintained up by internet-connected, heterogenous smart computing devices. An important development in the domain Internet of Things (IoT) networks is the rise of software-defined networks (SDN), which offer a practical answer to the problem of data exchange while also drawing a lot of attention. Among software-defined network's many advantages is the ease with which it monitors the health of the network and the active maintenance of integrated data via a central server. Additionally, it optimises network management and employs software defined programmability to achieve IoT networks' primary benefits, as well as to maintain resource allocation and network management through software demands on IoT-related networks. In order to address the new security threats, it is important to use smart and efficient computation algorithms for SDN safe communication based on these parameter descriptions. Topics covered in the present ages include the Internet of Things (IoT), analytics as it pertains to big data, cloud computing, artificial intelligence (AI), and machine learning (ML). Smart computing, which allows for control of many users in computing systems, is also described. A number of fields, including energy, healthcare, media, social protection, and transformation, make extensive use of smart computing.

In order to address the issue of storage capacity and investigate devices that are inadequate, there are

E-mail:Sujana.challapalli@acet.ac.in

applications that are related to smart computing that store large amounts of data on various cloud servers. Also, users won't have to worry about technological concerns, such as false tolerance and expansion, in cloud computing environments, and they won't have to worry about smart computing's specialised structure, maintenance, and management. As a result of the undesirable actions of certain users in an Internet of Things (IoT) setting, malicious attack sequences involving artificial intelligence (AI) have been known to occur in certain data outsourcing apps. Methods pertaining to the cloud's architecture are necessary for smart computing environments to automatically detect user actions. Demand for AI-powered, IoT-enabled smart computing environments pertaining to real-time security. The primary motivations for choosing or implementing IoT in cloud computing include processing heterogeneous data from several sources, managing loads linked to resources and bandwidth, and making the most of limited resources. The data processing, data storage privacy, and central load maintenance are all areas where cloud computing and the Internet of Things have generated controversy. Boost the trustworthiness of encrypted data storage while meeting the fundamental needs of smart computing networks associated with the Internet of Things. In order to offer efficient and secure data storage in smart computing systems related to the Internet of Things (IoT), we present and implement the Novel Low Cost based Block chain Secure Model (NLCBSM) in this work. In order to identify various user-related assaults (such as distributed denial-of-service, or DDOS) on data storage, this model adaptably records each user's authentication and uses an AI as a metric for evaluation method, the Leverage Bat algorithm, to investigate intricate aspects. Construct a server-side blockchain, end to provide trustworthy data storage and safe transmission on the IoT terminal. This method uses a weight-based data preservation mechanism to organise and categorise data for each individual, with safe and secure storage options available in smart computing networks, and assigns every one with a random hash value piece of data to guarantee data integrity in the blockchain.

a) Safe and reliable authentication for user-provided data is the key focus of this article's special study section. The following is an ongoing list of the primary benefits of this research:

b) Avoid using distributed computing's secure services and talk about the primary uses of the edge computing architecture. Describe the configurations of cloud storage servers and the resources they use.

c) Suggest the Leverage Bat algorithm to investigate intricate aspects of data belonging to various users in this study.

The Merkle tree is also used, which offers low-cost communication over head for data transmission. d) Regarding data storage, we suggest employing technology connected to blockchain and make sure to talk about smart computing data storage security.

2. Review of Related Work

In this part, we will go over the fundamentals of data processing in SDN as it relates to the Internet of Things (IoT), and we will go over the various factors and the process that make up the IoT concerned intelligent computing. To fulfil the obligations the reliability and scalability requirements of IoT networks, many network operators will work together and utilise the advanced technology of Software Defined Networks (SDN) and the Internet of Things (IoT). Every client in a centralised server takes care of the dynamic network configurations and the provisioning of flexible services. Integrating the Internet of Things (IoT) with software-defined networking (SDN) has sparked a flurry of activity in the field of network configuration management. A number of writers detail the installation of an Internet of Things gateway with various capabilities, while others talk about these parameters in terms of network function virtualization (NFV). This allows for elastic, scalable, and dynamic activities within Internet of Things networks, as described in [1,2] via the overall methodology execution mechanism of virtual zing the IoT accession. As said in [3], the process for implementing an SDN-based IoT architecture helps alleviate the issue of massive data evaluation transmitted by various users or nodes in relation to values sensed at lower layers of the network infrastructure, rather than higher ones.

Improved network status monitoring and statistical analysis of network metrics are two outcomes of SDN's recent advancements in IoT security. These statistics outline various vulnerabilities in wireless Internet of Things (IoT) environments, including attack sequence detection and prevention, including user authentication, automated network management, identity-based security, and packet data transmission routing [4]. The procedure of Secure communication and prevention are illustrated in figure 1.

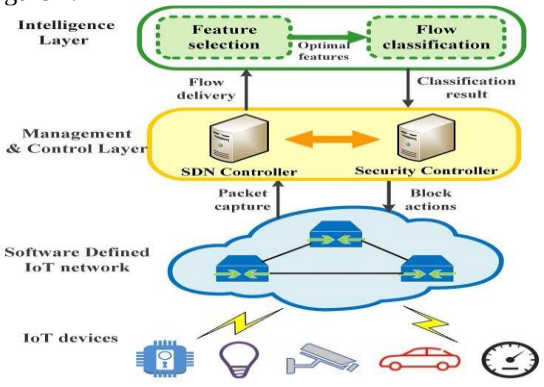

Figure 1 IoT-based software-defined networks with secure communication and intrusion detection

Figure 1 shows the process that is involved in identity-based approval for SDN-based Internet of Things (IoT) networks. A trusted authority is established on SDN controllers, and many protocols pertaining to communication employ specific identification formats. It protects against various assaults, such as denial of service, by utilizing security via services provided by third parties. Particle swarm optimization (PSO) [6] and Ant colony optimization (ACO) [5] are only two examples of the many Swarm Intelligence (SI) algorithms that have recently found use in optimum highlight selection. Last but not least, we identify organized streams by seeing if they contain any malicious or benign traffic. As a neural classifier to identify instances of abuse, the authors of [7] recommended to use a Recurrent Neural Network (RNN) with three layers that can subsequently discover the connections between stream records. But existing computations still aren't good enough to pick appropriate highlights and identify various novel attacks with minimal costs under diverse scenarios based on their fundamental restrictions.

Blockchain Models that do not break the bank

Various forms of blockchain technology that are both efficient and inexpensive are detailed here.

Blockchain technology Most people use and trust Ethereum [10]. With an emphasis on smart contracts, it is the biggest public blockchain network on a permissioned public blockchain, where users can examine Ethereum data and initiate transactions directly with no third party involved. Making it easier to build decentralized applications was its main goal.

Instead of monetary transactions, one can store smart contracts, which are bits of code, in the blocks indicated in Figure 2. Using the solidity programming language, the Ethereum virtual computer compiles the smart contracts utilized by Ethereum. The total workload and memory available to each contract dictate its gas cost. As the sizes of data sets grow, more costly alternatives become accessible. Ethereum, similar to Bitcoin, has a PoW consensus mechanism; however, its hash puzzles are far easier to solve, leading to a block time of 10–20 seconds. To that end, Ethereum boasts higher throughput and quicker block production.

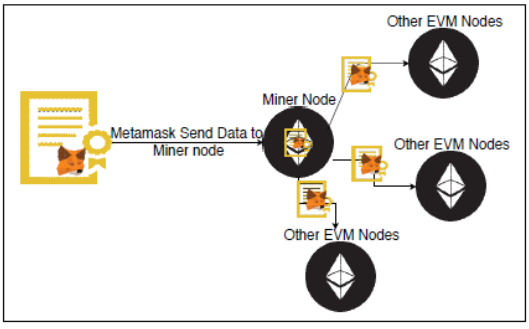

Figure 2. Distribution of Ethereum contract

Stellar aspires to be a scalable payment gateway and was the first blockchain network to concentrate on smart contracts [11] [12]. Stellari is very scalable because the time it takes to mine a block or contract is only three to five seconds. It has a transaction verification rate in the thousands per second. Stellar is a consensus technique for blockchains that relies on a gossip network for voting. Stellar blockchain developers can take advantage of the development team's many APIs and software development kits (SDKs). Lastly, applications with several users can benefit from smart contracts that support multiple signatures. Lumenis is a Stellar platform cryptocurrency. Stellar has lower transaction costs and faster contract development and deployment timeframes than Lumen and other rival cryptocurrencies, making it a more wallet-friendly blockchain option than Bitcoin or Ethereum.

EOS

EOS is an efficient and well-known blockchain network. Its name is derived from the Ethereum operating system. Using a consensus method known as delegated proof of stake, EOS is able to accomplish its objectives of low energy consumption and great efficiency. Deploying smart contracts on the EOS network is straightforward and doesn't cost anything. However, in order to maximize the network's bandwidth, contract creators will want access to EOS, CPU, and Memory. A single central EOS full node can handle several wallets.

Merkle Tree

Data structures like the Merkletree [13] are crucial for ensuring the accuracy and efficiency of content verification in large datasets. Making sure the data is correct and comprehensive is the main goal of this approach. Any actor can check if a particular node is part of a Merkletree since the data structure collects all the information in a tree and then generates a digital fingerprint of the whole set. The Merkle Root, seen in Figure 3, is the last hash that remains after repeatedly hashing the nodes of a Merkle tree.

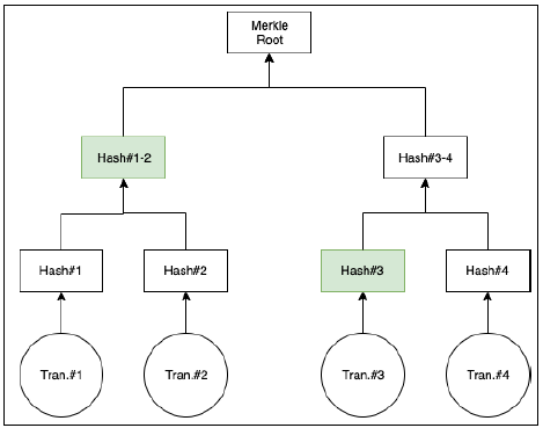

Figure 3. Merkle root block chain calculation

The hashing process starts with hashes of individual data points and proceeds in reverse order.

To be more specific, the data hashes of the tree's leaf nodes are distinct from those of the non-leaf nodes, which correspond to the roots of two separate sub-trees. When the leaf nodes count is exactly equivalent to two, we have a Merkle tree. You can make the number of leaf nodes equal to even if the number of data points is odd by duplicating the final data point. A Merkletree differs significantly from a regular hash list in that its branches can be generated independently.

In this way, it is possible to independently verify the integrity of every branch. To confirm the integrity of each leaf node, only a part of its data needs to be retrieved, which is made possible by breaking records down into smaller data chunks. You can check if some transactions are in a Merkle tree using simplified verification (SV) instead of downloading the whole tree.

3. MATERIALS AND METHODS

A. *Cost-Effective Blockchain Model*

Electronic crime scene investigation chain of custody system based on block chain technology. It allows the system to create a decentralized database for logging and storing transactions.

Examination of Occurrences, Results, and Other Data.

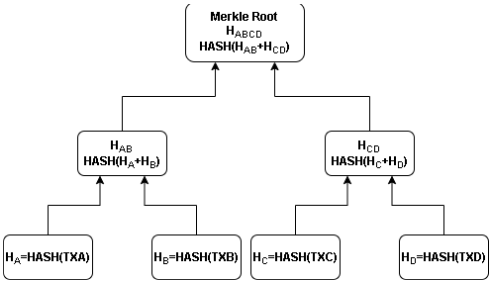

Figure 4. Structure of Low-Cost Model

Using the blockchain protocol, these TEs will be accessible to all legitimate users. You can see the framework's constituent parts listed below.

The word "users" regarding the Internet of Things (IoT)might include anyone who uses, owns, or investigates the system [35]. The case-specific IoT infrastructures, sensors, and devices are all part of this architecture.

The usage of a Merkle tree allows for the safe and rapid verification of TEs throughout an investigation [12]. By collecting all TEs, analysing all other data in the block, and then generating a digital signature for every item in the collection, a user can confirm whether a transaction is part of a block.

Figure 4 shows a Merkle tree of nodes, which could represent a folder or memory, and in this instance, the TE is a le.

Information Hash#2 (HT2) (Transactional Evidence#) and Hash#1 (HT1) for Transactional Evidence

12. HT1jHT2 HT12 D Hash

Hash function D with root key H12j: : :

In this context, HT stands for the hash value of the evidence, which can be found by repeatedly hashing the transaction evidence. To get a single root hash, you can keep doing this

Algorithm 1 Merkle_Tree

Input Mined Block Header H : Block payload P
Output Similarity, Boolean valid
H = Extract_nonce_value ( )
B = Calculate_Merkle_Tree ( )
V = Create header_verify(H, P, B)
R = verify(H, B, V)
Similarity = calculate_ssdeep_hashed_value(R)
if (similarity >= 90) **then**
Valid ← TRUE;
else
Valid ← FALSE;
end if
return Valid;
End

Here, we use the Merkle tree method and the fuzzy hash for cross-block transaction validation by reading data from each block. At this node, the Merkle tree approach is used to create the new block as a header. In Algorithm 1, the process of creating a Merkle tree is outlined in great depth.

Blockchain: The proposed method makes use of a distributed ledger system, which allows for the verification of the evidence item's signature. Figure 4 shows that the block header contains the pre-block hash, nonce, timestamp, and block state, while the block state field contains the Merkle root, version, and block state. To keep track of regarding the piece of evidence, the TE is hashed into a Merkle tree.

Dealing with Contracts Online: You can find digital contracts called "smart contracts" on the blockchain that can be executed by computers. The smart contract is often kept on the blockchain and kept tabs on by the nodes in the network. Data, information, and business processes can be easily and quickly shared and transferred across users. The immutable distributed ledger can support smart contracts, which allow for automated execution, verification, and decision-making [12]. The following smart contract features may be relevant to the DF investigation. To illustrate: The criteria for autonomously locating related pieces of evidence may be defined by autonomy. Cryptographically storing trust evidence on a distributed ledger is a viable option.

The use of a cryptographic technology allows for the encryption of security aspects.

Rapidity Smart contracts have the potential to significantly reduce review times when contrasted to manual processing. Furthermore, smart contracts eliminate the need for costly third parties like witnesses and notaries, which brings us to our fifth point.

Truthfulness, the Sixth

Efficiency, accuracy, and cost-effectiveness are all enhanced by automating the smart contract.

Every time one of our nodes receives proof of a transaction, it starts a smart contract by computing the nonce with consensus protocol - Proof of Work (PoW) and sending it out into the blockchain. The node uses the validity of the blocks preceding it to construct a Merkle tree. To ascertain whether the freshly produced block need to be integrated into the operational blockchain, the node employs a fuzzy hash of the whole blockchain's preceding blocks inside the Merkle trees.

B. A Trusty Secure Block Chain Model Based on Privacy Preservation

Here we will describe the various components that comprise the suggested TP2SF framework, including the modules for trust management, privacy protection, and anomaly detection. This design incorporates a reputation system for verifying addresses on the blockchain and a privacy protection module with two layers that utilise enhanced proof of work (ePOW) on the blockchain and a data transformation methodology was found based on Principal Component Analysis (PCA). Finally, an intrusion detection module based on XGBoost is integrated. The aforementioned sections will be described separately below:

```
procedure BLOCK_PROPOGATION(proof)
    if (Block_Index==0) then
        Previous_Hash=0
        Block_Hash= Digest(Block_Index, Previous_Hash,
timestamp, Data (T_value), T_xscore, Rp_s, Current_Proof, Cur-
rent_Block_Hash, SHA512)
        return(Block_Hash)
    end if
end procedure
procedure ENHANCED_PoW(last_proof)
    proof ← last_proof + 1
    while ((proof + last_proof)% 7 == 0) do
        proof ← last_proof + 1
        return (proof)
    end while
end procedure
procedure ADD_NEW_BLOCK
    for i=1 to N do
        if (i==1) then
            proof=1 /*Genesis Block Creation*/
            add_block = BLOCK_PROPOGATION(proof)
        else
            last_proof = i
            ePoW= ENHANCED_PoW (proof)
            add_block = BLOCK_PROPOGATION(ePoW)
        end if
    end for
end procedure
```

Algorithm -2 Trusty oriented block chain security process in IoT based framework.

Figure 5 depicts a two-tiered privacy-preserving module that is introduced in this part to avoid data leakage in an IoT-driven smart city's public service systems, such as anomaly detection. The first step is to develop a data integrity checker that uses blockchain technology to ensure that all processed data is legitimate. The second step is to use principal component analysis to reformat the original data so that inference attacks based on prior knowledge cannot be executed.

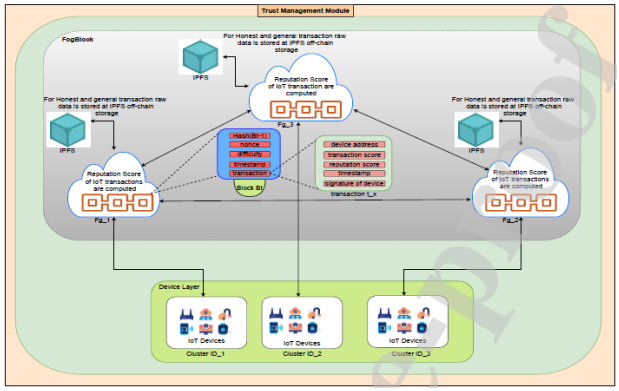

Figure 5. A trustworthy approach to an Internet of Things (IoT) forensic architecture built on the blockchain.

The notion of privacy on the blockchain is an extension of the blockchain protocol, which employs a peer-to-peer design to reliably and securely deliver encrypted data transfers or network nodes. These validated messages establish a chain of records, or blocks, on all nodes in the

fog or cloud, guaranteeing the ledger's immutability and decentralization.

C. A New Security Model for Low-Cost Block Chains (NLCBSM)

Redundancy is a method to guarantee a code-based secure technique gets more attention, and it is used in outsourced storage systems to improve network stability. Redundant coding allows users to recover data in the event of storage loss. However, this typically happens anytime users restore data, which causes the transferred quantity of data to exceed their storage capacity. This discrepancy could be caused by changes in bandwidth. When it comes to the idea of network coding, the most fundamental way to deal with bandwidth changes is to generate secure erasure codes. Each user's data will be securely stored and transmitted using MD5 and blockchain technology.

i. NLCBSM Design By utilizing Smart Edge Computing

Figure 6 depicts the fundamental steps of the suggested method for network storage; Figure 6 shows the various parts of the suggested secure storage models. 1. Establish a server infrastructure. 2. Build a blockchain computing network. 3. Establish a smart computing center at the edge. 4. Install equipment for exchanging data from the Internet of Things. 5. Build a blockchain for users.

ii. Establish a Blockchain-Based Computer System

We use a cutting-edge idea, a blockchain-based global storage system to guarantee the security of the data stored on the server. Each server uses an updated bat calculating algorithm for dispersed environments, keeps a copy of the data blocks for verification and storage, and shares and updates user data via a block structure.

Using a representative code technique to investigate the redundant data and enhance storage system reliability can increase data security and efficiency.

iii. A Smart Computing Centre with an Edge

Due to hardware constraints, this smart computing edge maintains scattered edge network devices associated with the Internet of Things (IoT). Additionally, to securely transferring data from higher layers to lower ones, the edge computing system is also responsible for managing the network's limited capabilities and resources.

iv. Building a blockchain for users

User block chains are lightweight due to limited resources of IoT distributed network devices, and they are managed by edge network centers that also construct and oversee IoT networks. When user data reaches a certain level in the blockchain, it ought to be hashed and kept retained the deletion of IoT devices.

v. Web of Things Data Exchange Devices

Data transmission basics, it delves into human interaction, and then human communication expands to include global information and the ability to communicate in real time in relation to newly emerged technologies, regardless of location or time of day, all through the interconnection of devices in the Internet of Things (IoT) network.

4. Secure Storage Model Based on Blockchain Technology

For edge-based smart computing, the key concern is the potential invasion of user privacy due to the endless storage space offered by cloud servers, which are utilized to store all user data in the computing environment. It discusses the current difficulties with ensuring the accuracy and integrity of user data throughout storage. The network uses blockchain technology to store data, investigate data into various edge center communication across the Internet of Things (IoT) environment, and increase the reliability of edge based smart computing systems; however, privacy remains a big issue. Data blocks, decentralization, and increased accessibility and security are some of the unique features of blockchain technology. To further enhance the dependability, accessibility, serviceability, and availability of the environment for outsourced edge-based smart computing was depicted in figure 3, data storage needs to be improved.

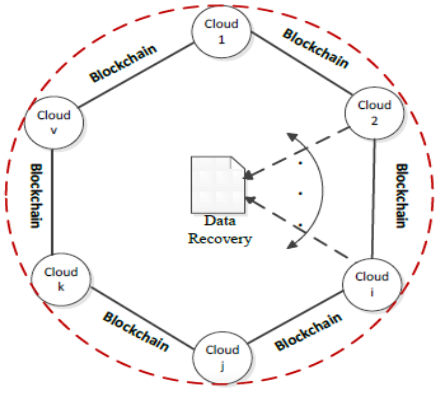

Figure 7. Block chain based secure data storage.

Figure 7 shows that Data encryption is done in edge smart computing and stored on edge cloud servers. Numerous applications generate encrypted data on each server, and if data is not retrieved by the server, the services can drive to download data automatically from a backup server that can fix various bandwidth issues. The

Minimum Bandwidth Restate-owned (MBR) & Repair by Transfer (RBT) protocols ensure that no data loss occurs and that the amount of data to be transferred is proportional to the amount of data that could be lost. A matrix is used to store RBT at each server:

$$N = \begin{bmatrix} R & P \\ -P^t & 0 \end{bmatrix} \quad (1)$$

Where P is the vector filling $n \times (k-n)$, R is the matrix which consists anti-symmetric features and 0 is the vector present in between $(k-n) \times (k-n)$, Examine each user's behavior that is saved in the matrix that is described as

$$l_j^{'} \begin{cases} l_j[i] i \geq j \\ -l_j[i] i \geq j \end{cases} \quad (2)$$

The block chain technology literature states that block chain stores can be replicated

$$L(\alpha) = \begin{cases} A + (n-1)\alpha & \alpha \in [0, a_0] \\ A + a_0 + (n-2)\alpha & \alpha \in [a_0, a_1] \\ A + a_0 + C + a_{n-3}\alpha \, \alpha \in [a_{n-3}, a_{n-2}] \end{cases} \quad (3)$$

Satisfying minimum value $L(\alpha) \geq A$

$$\alpha' = \begin{cases} \dfrac{A}{n-1} A \in [A, A + (n-1)\alpha_0] \\ \dfrac{A - \sum_{j=0}^{i-1} aj}{n-1-i} A \in [A + \sum_{j=0}^{i-1} (n-i-1), A + \sum_{j=0}^{i-1} a_j + (n-i-2)\alpha_i] \end{cases} \quad (4)$$

$$\sum_{j=0}^{i-1} a_j = \sum_{j=0}^{i-1} \left(1 - \frac{n-j-2}{d}\right)\beta = \beta_i \left[\frac{d-n+2}{d} + \frac{n-1}{2d}\right] = \beta g(i) \quad (5)$$

$$= \sum_{j=0}^{i-1} \left(1 - \frac{n-j-2}{d}\right)\beta + (n-i-2)\left(1 - \frac{n-2-i}{d}\right)\beta \quad (6)$$

$$\beta \left(\frac{(n-1)(d-k+2)}{d} + \frac{(2n-i-3)}{2d} \right) \quad (7)$$

According to equations 3–7 above, the ultimate bandwidth for every user in relation to the scanned copy is as follows

$$\left(\alpha^{'}, \beta^{'}\right) = \left(\frac{2Ad}{(2d-n+2)(n-1)}, \frac{2Ad}{(2d-n+2)(n-1)} \right) \quad (8)$$

A. Block chain based IoT data storage

In a cloud service for smart computing, several Internet of Things (IoT) terminals share the same storage and communication resources, allowing users to construct their own blockchain. The encryption used to store data in IoT terminals and the fact that each terminal has a limited amount of power are the two main factors that dictate the terminals' efficiency. The suggested method use energy-aware communication to encrypt data using blockchain technology, and when data is being transmitted, every node keeps up energy-conscious data transmission to lessen the likelihood of energy reduction at every individual. What follows is a summary of the literature on blockchain technology that focuses on energy savings for individual users:

According to the data representation in $Are(j) = K(i)RE(j) / \sum_{n \in K(i)} RE(n).K(I)$ in Are format above, data shared by numerous users with adequate capacity may be utilized for encryption to recover lost data; the process ought to be documented in a figure 8.

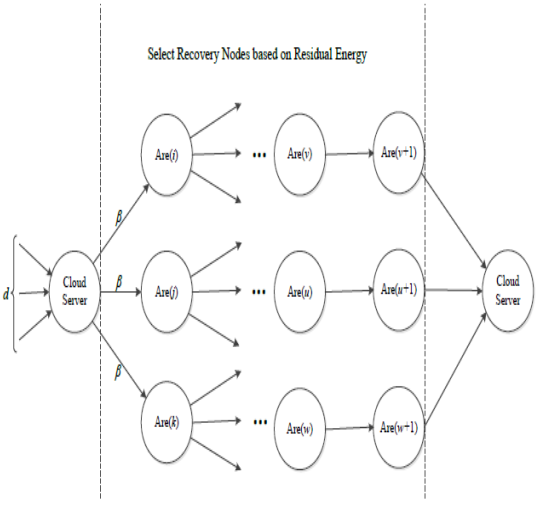

Figure 8. User's block chain based data storage

Figure 4 illustrates the entire IoT terminal equipment in terms of energy maintenance at each user to store lost data and collaborate in an encrypted manner. Data file kept in multiple blocks i.e; N and split into n local blocks, which are further subdivided into n components denoted by the matrix as

$$N_1 = \begin{bmatrix} x_1^1 & x_2^1 & x_{n-1}^1 & x_k^1 \\ x_1^2 & x_2^2 & x_{n-1}^2 & x_n^2 \\ L & L & L & L \\ x_1^n & x_2^n & x_{n-1}^n & x_n^n \end{bmatrix} \quad (9)$$

Boost the dependability of the smart computing system's data storage by using a source data file that is encrypted using the same code block and redundant features, and is shown in the matrix below

$$N_2 = \begin{bmatrix} x_{n+1}^1 & x_{n+2}^1 & L & x_k^1 \\ x_{n+1}^2 & x_{n+2}^2 & L & x_n^2 \\ L & L & L & L \\ x_{n+1}^n & x_{n+2}^n & L & x_k^n \end{bmatrix} \quad (10)$$

Equations 9,10 describes in smart computing-based IoT networks, N1, N2 stand for complete data storage with completer blocks. When any user is damaged, IoT terminals download the entire data set and distribute it to every user.

B Block chain based Data Transfer

The user's block chain is an integral part of the main chain method; it generates computations based on the center's edges and stores the data of user in the IoT using hash values. The user's block chain contains all data collected by the server's block chain. The suggested schema offers compete hash values for investigating secure data integrity, which is comprised of two separate chains: one for user data and the other for server communication.

When the data collected from all the Internet of Things devices attain the top layer, the hash values are broadcast into a networking system that allows data exchange at the edge. If the storage server empties, the data is retrieved from the edge-based cloud data storage system. Figure 5 shows the method.

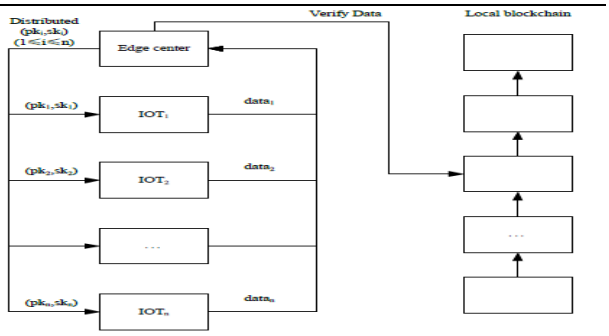

Figure 9. User's block based data transmission

As shown in figure 9, data updated into the user's blockchain should occur at regular intervals through the server. However, the hash values of the user's blockchain do not change when data updated into the server.

A broad summary of the is provided in the below steps to investigate server-side blockchain communication in IoT smart computing system:

i) Data uploaded and updated in global blockchain communication

ii) In Intelligent edge-based IoT network computing systems, every client in the overall blockchain receives a hash value from an edge-based cloud server. If the hash values are okay, the two blocks are identical, and the data encrypted and decrypted from the server to all users is sent accordingly.

iii) Create a tree structure for all the blockchain concepts after verifying their hash values on the server and with users.

iv) After validation, check the integrity relation between the user's and server block chains at regular intervals using each hash value.

C Assessment by Experiment

Compared to more conventional methods, such as the Common Database Forensic Investigation Process (CDFIP), we provide here the results of our assessment of the proposed performance technique, a new approach Artificial Intelligence based Block chain Secure Model (NLCBSM). [8] The ETL process for real-time operational databases (RODBs) [9], the LSTM to RNN (Recurrent Neural Network) [10] transformation from LSTM to RNN. Each of these mechanisms uses an Amazon S3 server setup to distribute storage and makes use of the newest software to create a custom server setup that allows it to explore various heterogeneous services. Deploy distributed service processing and investigate various characteristics such as response time, encryption time, decryption time, and energy consumption. Based on block chain technology the data will be stored in numerous blocks, both the cryptographic mechanisms-Encoding and Decoding with hash values assists in storage of safe data. The following results demonstrate

the production and calculation of hash values using various notations.

TABLE 1 VARIATIONS IN USER INSTANCES CONCERNING TIME

No. of User Instances	CDFIP	RODB & ETL	LSTM to RNN	NLCBSM
10	4.4	3.8	3.7	1.9
30	5.5	4.9	5.3	3.5
50	6.5	5.5	4.7	3.8
70	7.4	6.3	7.2	4.7
100	8.7	7.5	6.4	7.4

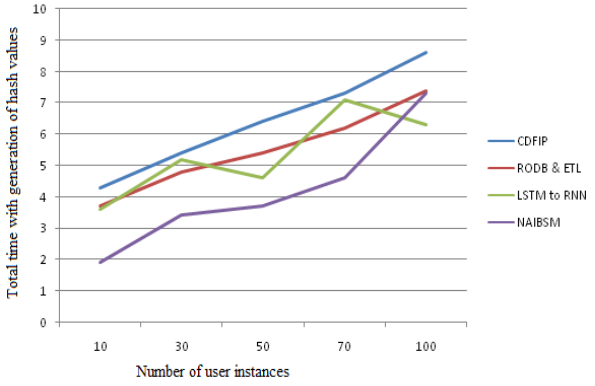

Figure 10. Performance evaluation of time with different users.

Table 2 displays the encryption time for service requests made by users to upload data in an encrypted format with various notations into multi-cloud storage.

TABLE 2. DIVERSE VALUES FOR USER REQUEST INSTANCES IN ENCRYPTION

No. of User Instances	CDFIP	RODB & ETL	LSTM to RNN	NLCBSM
100	4.4	3.8	3.7	3.6
200		4.8	5.2	4.1
300	6.4	6.7	5.2	4.3
400	7.3	6.2	7.1	4.6
500	8.6	7.4	6.3	7.3

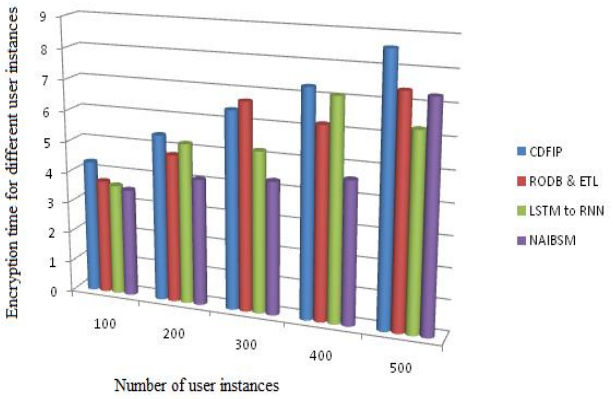

Figure 11. Performance evaluation with respect to users in encryption.

Table 3 displays the decryption time for various instance requests from user in order to access data from multiple cloud storage providers.

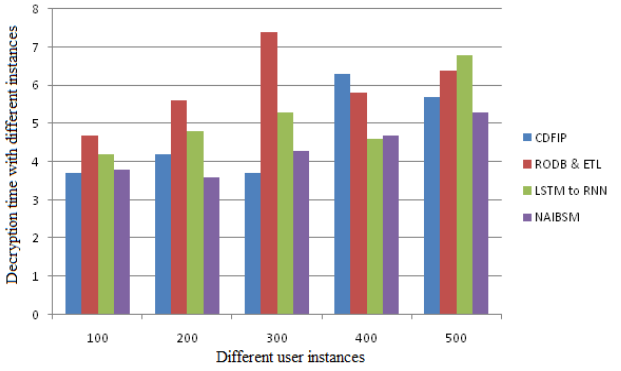

Figure 12. An assessment of decryption performance using various user instances

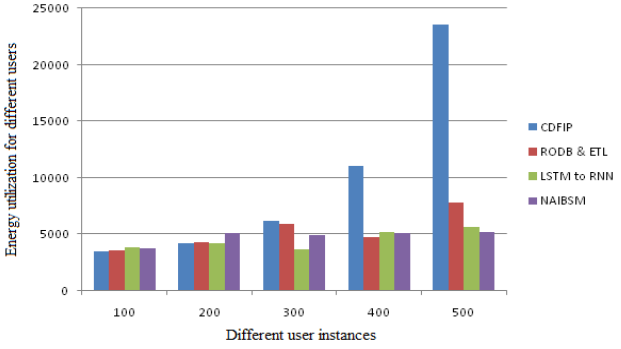

Figure 13. Evaluation of energy consumption performance for various user scenarios

TABLE 3. DESCRIPTION TIME VALUES

No. of User Instances	CDFIP	RODB & ETL	LSTM to RNN	NLCBSM
100	3.8	4.8	4.3	3.9
200	4.3	5.7	4.9	3.7
300	3.8	7.5	5.4	4.4
400	6.4	5.83	4.7	4.8
500	5.8	6.5	6.9	5.4

TABLE 4. ENERGY FOR VARIOUS USERS STORE DATA

No. of User Instances	CDFIP	RODB & ETL	LSTM to RNN	NLCBSM
100	3540	3643	3877	3760
200	4217	4327	4215	5125
300	6248	5975	3655	4927
400	11022	4786	5244	5148
500	23543	7855	5675	5215

Table 4 displays the memory utilization values for various users who store and retrieve data from cloud environments in a practical manner.

TABLE 5 DESCRIBE THE COST EFFICIENCY OF PROPOSED APPROACH WITH TRADITIONAL APPROACH

Computation processing cost				
User Instances	Novel Low Cost based Block chain Secure Model (NLCBSM)	CDFIP	RODB & ETL	LSTM to RNN
10	267	463	568	653
20	356	526	656	763
30	464	668	796	799
40	525	763	856	897
50	665	875	968	956

With regard to the cost of communication between nodes in IoT networks, the suggested blockchain model uses less resources, as demonstrated in table 5.

Results for total time, encryption, decryption time, and memory are displayed in Figures 11–15 for various user instances. The suggested hybrid solution outperforms the alternatives in terms of cost efficiency and reliable secure data transmission in the forensic-based IoT framework.

CONCLUSION

Data storage under Internet of Things (IoT) related edge based computing is heavily reliant on security measures, which in turn impact the development of smart computing networks. In order to ensure the efficient and secure data storage in smart computing systems related to the Internet of Things (IoT), it is necessary to build a Novel Low Cost based Block chain Secure Model (NLCBSM). This solution encrypts data stored in edge cloud servers using blockchain technology and uses the bat calculation mechanism for user authentication in storage. In NLCBSM, data is securely stored by each client using a unique blockchain that is produced by hash values. The server there by maintains the obtained hash values and uses them to verify that each user's block is compatible with the server's block. An experimental review has shown that a low-cost blockchain architecture for storing and exploring data in an Internet of Things (IoT) based data sharing environment at the edge produces the greatest outcomes in terms of energy, encryption, and decryption.

REFERENCES

[1] Y. Zhang, M. Chen, and Lai, "Codified and Software Defined 5G Networks: Architecture, Solutions, and Emerging Applications" Mobile Networks and Applications, vol. 21, no. 5, pp. 727–728, 2016.

[2] M. Ojo, D. Adami, and S. Giordano, "A SDN-IoT architecture with NFV implementation," in GLOBECOM Workshops, 2017, pp. 1–6.

[3] M. T. Kakiz, E. Ozturk, and T. Cavdar, "A novel SDN-based IoT architecture for big data," in International Artificial Intelligence and Data Processing Symposium, 2006, pp. 1–5.

[4] D. B. Rawat and S. R. Reddy, "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey," IEEE Communications Surveys and Tutorials, vol. 19, no. 1, pp. 325–346, 2017.

[5] T. Mehmood and H. B. M. Rais, "SVM for network anomaly detection using ACO feature subset," in International Symposium on Mathematical Sciences and Computing Research, 2016, pp. 121–126.

[6] N. Cleetus and K. A. Dhanya, "Multi-Objective Functions in Particle Swarm Optimization For Intrusion Detection," in International Conference on Advances in Computing, Communications and Informatics, 2014, pp. 387–392.

[7] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in International Conference on Platform Technology and Service, 2016, pp. 1–5.

[8] ARAFAT AL-DHAQM1,SHUKOR RAZAK,SITI HAJAR OTHMAN1,KIM-KWANG RAYMOND CHOO,"CDBFIP: Common Database Forensic Investigation Processes for Internet of Things", 2169-3536 2017 IEEE. Translations and content mining are permitted for academic research only.

[9] WEI CAI 1,2, (Member, IEEE), ZEHUA WANG2,3, (Member, IEEE), JASON B. ERNST, "Decentralized Applications: The Blockchain-Empowered Software System", 2169-3536 2018 IEEE. Translations and content mining are permitted for academic research only.

[10] Jihyun Kim, Jaehyun Kim, Huong Le Thi Thu, and Howon Kim,"Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection", INTERNATIONAL CONFERENCE ON PLATFORM TECHNOLOGY AND SERVICE, 2015.

[11] D. B. Rawat and S. R. Reddy, "Software defined networking architecture, security and energy efficiency: A survey," IEEE Communications Surveys and Tutorials, vol. 19, no. 1, pp. 325–346, 2017.

[12] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the internet of things," Computers and Communication, pp. 1109–1111, 2016.

[13] M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home IoT using openflow," in International Conference on Availability, Reliability and Security,2016, pp. 147–156.

[14] P. Bull, R. Austin, M. Sharma, and R. Watson, "Flow based security for iot devices using an SDN gateway," in IEEE International Conference on Future Internet of Things and Cloud, 2016, pp. 157–163.
[15] N. Farah, M. Avishek, F. Muhammad, A. Rahman, M. Rafni, and D. Md,"Application of machine learning approaches in intrusion detection system: A survey," International Journal of Advanced Research in Artificial Intelligence, vol. 4, no. 3, 2015.
[16] A. S. D. Silva, J. A. Wickboldt, L. Z. Granville, and A. Schaeffer-Filho,"Atlantic: A framework for anomaly traffic detection, classification, and mitigation in SDN," 2016, pp. 27–35.
[17] T. Mehmood and H. B. M. Rais, "SVM for network anomaly detection using ACO feature subset," in International Symposium on Mathematical Sciences and Computing Research, 2016, pp. 121–126.
[18] W. D. Wang and J. Y. Lang, Reflection and prospect: precise radiation therapy based on bionomics/radionics and artificial intelligence technology, Chinese J. Clin. Oncol., 45 (2018), 30648–30656.
[19] R. Khanna, H. Liu and T. Rangarajan, Wireless data center management: sensor network applications and challenges, IEEE Microw. Mag., 15 (2014), S45–S60.
[20] C. Yang, D. Puthal, S. Mohanty, et al., Big-sensing-data curation for the cloud is coming: a promise of scalable cloud-data-center mitigation for next-generation IoT and wireless sensor networks, IEEE Consum. Electr. M., 6 (2017), 48–56.
[21] J. Wang, C. Ju, H. Kimet, et al., A mobile assisted coverage hole patching scheme based on particle swarm optimization for WSNs, Cluster Comput., 3 (2017), 1–9.
[22] R. Meng, S. Rice, J. Wang, et al., A fusion steganographic algorithm based on faster R-CNN, Comput. Mater. Con., 55 (2018), 1–16.
[23] B. Gong, P. Cheng, Z. Chen, et al., Spatiotemporal compressive network coding for energy-efficient distributed data storage in wireless sensor networks, IEEE Commun. Lett., 19 (2015), 803–806.
[24] Y. Yang, J. Miao, Y. Zhao, et al., Distributed information storage and retrieval in 3D sensor networks with general topologies, IEEE ACM T. Network., 23 (2015), 1149–1162.
[25] J. Wang, J. Cao, S. Ji, et al., Energy-efficient cluster based dynamic routes adjustment approach for wireless sensor networks with mobile sinks, J. Supercomput., 73 (2017), 3277–3290.
[26] L. Xiang, Y. Li, W. Hao, et al., Reversible natural language watermarking using synonym substitution and arithmetic coding, Comput. Mater. Con., 55 (2018), 541–559.
[27] O. Diallo, R. Joel, M. Sene, et al., Distributed database management techniques for wireless sensor networks, IEEE T. Parall. Distr., 26 (2015), 604–620.
[28] A. Al-Dhaqm, S. Razak, S. H. Othman, et al., CDBFIP: common database forensic investigation processes for Internet of Things, IEEE Access, 5 (2017), 24401–24416.

Challapalli Sujana, currently pursuing Ph.D in JNTUK, Kakinada and working as an Assistant Professor in the Department of CSE, at Aditya College of Engineering & Technology (A), Surampalem. Her research includes WSNs, IoT, Blockchain technology, Machine learning, Data Mining.

Mr. M. Kalyan Ram, received MCA and M. Tech (CSE) from JNTUK and currently pursuing Ph.D. from K.L. University. He is working as Associate Professor, Department of CSE, Aditya Engineering College(A), Surampalem. His area of Interest includes Artificial Intelligence, Machine Learning, Data Mining, Block chain Technology and Internet of Things.

Dr.R.V.S.Lalitha is working as a Professor in the Department of Computer Science and Engineering, Aditya College of Engineering & Technology(A), Surampalem. She received Ph.D. in Computer Science & Engineering, JNTUK, Kakinada in the year 2017. She published papers in SCIE, Scopus indexed conferences and Journals. She received awards for her contributions in research. Her specializations include Machine Learning, Deep Learning and Wireless Sensor Networks.

Divya Lalita Sri Jalligampala, M.Tech(Ph.D) currently pursuing Ph.D at Acharya Nagarjuna University and working as Assistant Professor in CSE department, Aditya College of Engineering & Technology (A), Surampalem. Her research areas include Machine Learning, Deep Learning and IoT.