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

Mfokg-Biot: A Secure IOT Framework Based on Block Chain with Enhanced Key Generation

Girija.V[1]*, Dr Victo Sudha George G[2]

Submitted: 29/01/2024 **Revised**: 07/03/2024 **Accepted**: 15/03/2024

Abstract: The increased efficiency, low cost, widespread accessibility and numerous benefits of cloud computing are currently having a significant impact on the information technology sector. Additionally, it gives various Internet users faster data transmission between locations and more storage space for data. The advancement of technology allows users to store data online and access it from anywhere. To exchange data between Internet of Things (IoT) devices, a solid security and storage mechanism for authentication is required. In order to solve this problem, a unique cluster-based secured user authentication mechanism is recommended. The anticipated paradigm consists of four main phases: (a) user authentication, (b) authorised user clustering, (c) data encryption and decryption, and (d) block chain-based secured data transfer. Initial user authentication in the Internet of Vehicles (IoV) network is performed using the Query Assisted Multi-User Authentication Protocol (QMAP). The authenticated users are then grouped using the two-fold optimal clustering model (only authorised users are allowed to participate in data transfer). For the authorised users, the two-fold objectives like angular distance and trust level are computed in the two-fold optimal clustering model. The Cluster Head (CH) is chosen as the authorised user (i.e., node) with the highest trust level and shortest angular distance. Additionally, a new Meliorated Mayfly optimization method (MMO) is presented for the selection of the best CH. The Mayfly Algorithm standard version is expanded in this MMO (MA). Once the CH is chosen, the cluster's nodes communicate with one another by using the CH that was chosen with the greatest consideration for efficiency. Additionally, block chain-based data transmission is utilised for secure data transmission between nodes in various clusters. The newly proposed Optimized Blowfish Algorithm is used to encrypt the data before it is sent via the block chain. These encrypted files are kept in the cloud and sent via blocks of the block chain. The decryption operation is carried out at the receiver end. Additionally, using the brand-new Meliorated Mayfly optimization (MMO) method, the blowfish algorithm's private key is chosen ideally to increase the security level of the data being communicated. In general, data transfer is done safely. The projected model is validated in terms of encryption time, security and decryption time as well.

Keywords: *IoV; Query Assisted Multi-User Authentication Protocol; two-fold optimal clustering; Meliorated Mayfly optimization method (MMO)*

1. Introduction

The IoT and blockchain technology (BCT) have significant demand digit growth [1]. They recognize as commonplace technologies with the potential to transform our civilization. Nevertheless, the principles behind these two technologies are distinct [2]. A unique technology called blockchain (BC) is used in the IoT to operate as a decentralized, distributed, public, and real-time ledger to hold transactions between IoT nodes [3]. Every block in a BC is connected to the blocks before it. Every block contains its data, the former block's hash, and the cryptographic hash code [4]. The fundamental unit put to use to move data between IoT nodes in BC is transactions [5]. The Internet of Things node consist various forms of physical, intelligent devices with built-in sensors, actuators, and software it can communicate with other IoT nodes.

The function of the BC in the IoT is to offer a technique for processing protected data records through IoT nodes [6]. BC is a safe technique it is accessible to everyone. This type of technology is necessary for IoT to enable secure communication among IoT nodes in heterogeneous environments. Anyone who is authorized to communicate within the IoT can track and investigate the transactions in BC. The BC in the IoT could aid in enhancing reliable communication [7].

Unprecedented advancements in our civilization have been made possible by the quick development of reduction, electronics, and networking technology. As a result, there is now more electronic gadgets exist appropriate for numerous uses, their production costs is lower, and there has been a paradigm shift from the physical world to the digital one [8]. As a result, our interactions with one another and the environment has modified as a result of our use of modern technology to better understand the world. The term IoT refers to a gathering of technologies, ranging from Wireless Sensor Networks (WSN) to Radio Frequency Identification (RFID), enables Internet-based sensing, acting, and

[1*] *Research Scholar, Dr. MGR Educational and Research Institute (Deemed to be University), Chennai-95, Tamil Nadu, India.*
[2] *Computer Science and Engineering, Dr. MGR Educational and Research Institute (Deemed to be University), Chennai-95, Tamil Nadu, India.*
[1*] *Corresponding Author Email: girijav668@gmail.com*

communication [9]. IoT allows for the digital representation of objects and other physical things. This digital "wrapper" facilitates communication with information and communication technology (ICT) components is set on a public, private, or hybrid cloud, as well as those is at the other end of a wide area network (WAN). IoT advocates sometimes refer to it as the convergence of IOT and ICT systems [10]. Documentation about the surroundings can be gathered using a variety of inexpensive sensors and linked objects, allowing us to improve our way of life [11]. Peer-to-peer networking, public key cryptography, and distributed databases is the foundation of blockchain, which enables distributed consensus among network users without the need for a central trust intermediary [12]. Transactions on a blockchain platform is organized into blocks, which producers create and use a distributed algorithm. The genesis block is the initial block in a blockchain. An immutable chain of blocks is made when each succeeding block is linked to the one before it via a cryptographic hash reference [13]. IoT is a perfect fit for RFF authentication and key generation. First off, neither of these two strategies uses a lot of energy, thus they may be spent with IoT devices have limited power [14]. Blowfish is one of the fastest, smallest, most intuitive, straightforward to use, and cost-free alternatives to currently used encryption algorithms. It also has configurable security levels, except when changing keys [15].

The major contribution of this research work is:

- To introduce a new Query Assisted Multi-User Authentication Protocol (QMAP) for secured user authentication
- To cluster the secured users via the newly projected two-fold optimized clustering model.
- To introduce a new Meliorated Mayfly optimization algorithm (MMO) for optimal CH selection.
- To introduce an Optimized Blowfish Algorithm for data encryption. In Blowfish Algorithm, the optimal key is selected via MMO model.

The rest of this paper is arranged as: Section II discusses the literature works undergone in IoT-blockchain environment. Section III tells about the Proposed Secured Multi-User Authentication in Blockchain-IoT. Section IV, Section V, Section VI manifest the information about the User authentication Phase, Authorized user clustering and Data encryption and decryption, respectively. The information regarding Merkle Root Tree-blockchain data transmission is portrayed in Section VII. In addition, the results acquired with the projected model is discussed in Section VIII, and this paper is concluded in Section IX.

2. Literature Review

“Some of the recent research works related to IoT - blockchain models are portrayed in this section”

Pavithran et. al.[16] They had suggested examining blockchain in IoT. Highlight the five major elements, design considerations, and obstacles that should be considered while creating blockchain architecture for IoT. We list the problems that make it difficult to create a secure blockchain architecture for IoT. According to our simulation of two different blockchain implementation models, device-to-device design offers a significantly higher throughput than gateway-based implementations.

Singh et. al.[17] had proposed a blockchain concept with pertinent elements that offer a thorough examination of potential security threats and also describe existing solutions that can be used as defenses against such assaults. By distilling important ideas that can be utilized to create multiple blockchain systems and security tools that address security flaws, then blockchain security enhancement options are presented it covers unresolved problems and potential research avenues for blockchain-IoT systems.

Kuzminykh et. al.[18] had examined how the encryption technique and packet length affect an IoT device's longevity when transferring encrypted data. Then concentrate the investigation in particular on lightweight algorithms used in IoT ecosystems, such as Serpent, Piccolo, Blowfish, and Twofish, as well as AES, XTEA, HIGHT, KLEIN, ECC, and PRESENT. The study's findings show that, along with information length and other input factors, the kind of data encryption used for transmission has a substantial influence on the lifespan of Internet of Things devices. AES, XTEA, and KLEIN are the next most energy-efficient algorithms, resulting in a maximum lifetime and low power usage. On the opposite end of the spectrum, because of their high-power consumption, ECC, Blowfish, Twofish, PRESENT, and Serpent should be less desirable for device-to-device or device-to-gateway IoT communication.

Kiruthiga et. al.[19] had developed a smart home automation system that gathers information about the gadgets inside a home and secures that information through privacy-preservation technologies like the Customer data engine and the blowfish algorithm, the strategy was to address security challenges in home automation. As a result, the system can enable automatically on/off switching of the devices.

Singh et. al.[20] had proposed potential broad drivers for the overlapping of AI and Blockchain to deliver scalable and protected IoT applications like smart cities and healthcare. Blockchain and AI for the IoT offer two solutions to the problem of AI utilizing blockchain:

"Blockchain driven AI" and "AI driven Blockchain." Along with a high-level taxonomy of AI for blockchain in IoT and blockchain for AI in IoT with topics, subcategories, computing platforms, and blockchain techniques and applications, we also discussed a thorough classification of "AI driven Blockchain" and "Blockchain driven AI" for IoT with contemporary state-of-the-art technologies and applications.

Hammi et. al. [21] had proposed sphere of authority was a novel democratic method that guarantees reliable device identification and authentication. It also safeguards the availability and integrity of the data. Our method relies on the security benefits offered by blockchains to accomplish specific aim and works to establish safe virtual areas (bubbles) where objects may recognize and trust one another. Additionally, we offered a working version of our mechanism that made use of the Ethereum blockchain and C++ programming. The acquired outcomes show its potential to satisfy IoT security requirements as well as its efficiency and affordability.

Cui et. al. [22] had proposed IoT multi-WSN access control based on blockchain is suggested. According to the variations in their capabilities, IoT nodes are separated into base stations, cluster head nodes, and regular nodes, which are organized into a hierarchical network. A hybrid blockchain model is created by building a blockchain network across several node types, with local chain and public chains. This hybrid paradigm allows for the reciprocal validation of nodes' identities in a variety of communication circumstances, the use of local blockchain for routine node verification, and the use of public blockchain for cluster head node identity authentication. The system features complete security and higher performance, according to the examination of security.

Panda et. al. [23] had presented that for guarantee data privacy in IoT situations and hence create a safe environment for communication, the architecture takes advantage of fundamental aspects of Blockchain technology, such as openness, immutability, traceability, and fault tolerance. It offers a plan for safe and effective key management and generation for communication entities' mutual authentication. The suggested method utilizes a one-way hash chain methodology to give the IoT devices a set of public and private key pairs that enable the key pairs to independently validate themselves at any moment. It performs better than traditional mechanisms, according to an experimental study.

Hang et. al.[24] had presented a unique design and implementation strategy for a public blockchain network-based decentralized IoT platform to handle scalability, identity, and data security issues. To use the Raspberry Pi and numerous physical components, the proposed is put into practice as a proof of concept and assess the performance through a variety of performance measures, and the results show a consistent level that enables efficient transaction processing.

Alrubei et. al.[25] had suggested an architecture it offers a platform that was reliable, powerful, and cost-effective relating to resources and traffic to handle edge-based IoT applications with AI capabilities. In the ability to provide governmental institutions and organizations with processed data and results for improved decision-making, the system will be able to provide continuous AI prediction, hence eradicating a single point of failure. By leveraging a safe, decentralized, and open blockchain platform to validate and safeguard all AI data (inputs and outputs), it maintains data integrity. This method integrates the security benefits of blockchain with the knowledge benefits of AI to deliver a publicly accessible platform that enables a protected framework for detecting, analyzing, reasoning, and providing actionable results.

3. Proposed Secured Multi-User Authentication In Blockchain-IoT

The major objective of this research work is, data security enhancement. To achieve this objective, a novel cluster-based secured user authentication approach is developed for IoT-blockchain environment.

3.1 Proposed System Architecture

In this research work, a novel cluster-based secured user authentication technique is suggested. The projected model includes four major phases: (a) user authentication, (b) Authorized user clustering, (c) data encryption and decryption and (d) block chain based secured data transmission. The architecture of the projected model is manifested in Fig.1. The steps followed in the projected model is manifested below:

Step 1: Initially, the vehicles users is authenticated using the new Query Assisted Multi-User Authentication Protocol (QMAP).

Step 2: Then, the authenticated users are clustered based on the two-fold optimized clustering model. In the two-fold optimized clustering model, the two-fold objectives like angular distance and trust level is computed for the authorized users. The authorized user (i.e. node) with the highest trust level and lowest angular distance is selected as the Cluster Head (CH). Moreover, for optimal CH selection, a new Meliorated Mayfly optimization algorithm (MMO) is introduced. This MMO is an extended version of the standard Mayfly Algorithm (MA).

Step 3: Once, the CH is selected, the data transmission between the nodes within the cluster takes place via the optimally selected CH. In addition, for secured data transmission between the nodes in diverse clusters, the block chain-based data transmission is used.

Step 4: Before transmitting the data via the block chain, they are encrypted via the newly projected Optimized Blowfish Algorithm. These encrypted data is stored in cloud, and they are transmitted via the block of the block chain. At the receiver end, the decryption process is carried out. Moreover, to enhance the security level of data being transmitted, the private key of blowfish algorithm is selected optimally via the new Meliorated Mayfly optimization algorithm (MMO). As a whole, the data transmission takes place securely.

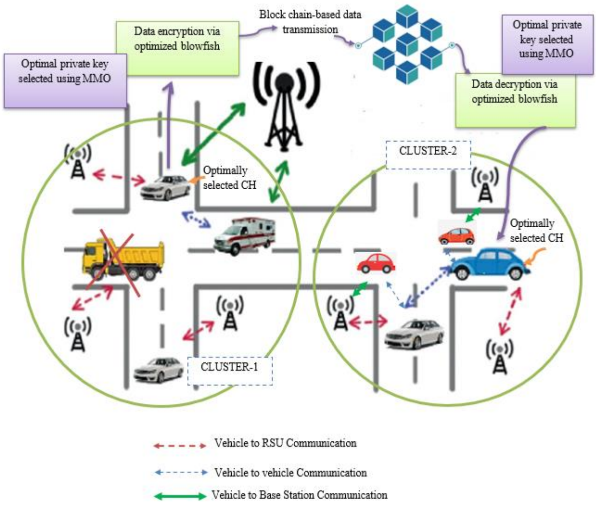

Optimal private key selected using MMO
Data encryption via optimized blowfish
Block chain-based data transmission
Optimal private key selected using MMO
Data decryption via optimized blowfish
Optimally selected CH
CLUSTER-2
Optimally selected CH
CLUSTER-1
Vehicle to RSU Communication
Vehicle to vehicle Communication
Vehicle to Base Station Communication

Fig 1: Architecture of the projected model

4. User Authentication Phase

The user authentication phase is the initial phase. In this phase, every user in the network is authenticated via new QMAP process. The QMAP process is diagrammatically shown in Fig.2.

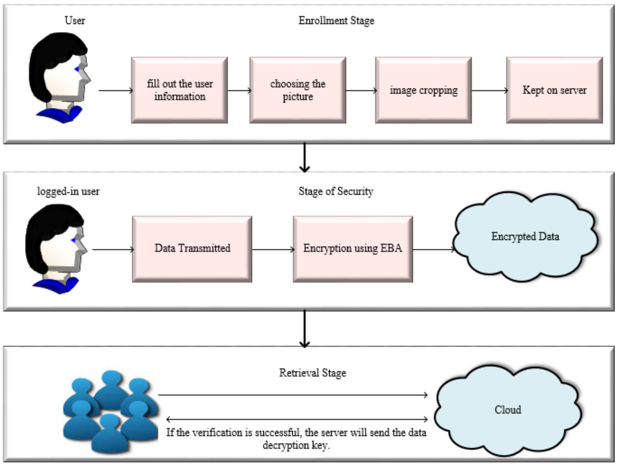


Fig 2: User Authentication Phase

4.1 Procedure for Registration

Customers entered their data on the data center during the registration phase. Initially, the client creates the user id US^{id}, password PW^{id} and enters all of the user's information. The

4.2 Procedure for Login

After successfully registering, consumer could upload or download information into the cloud. Any client can neither access the cloud nor collect any data without first registering. This method allows us to protect loss of data. Clients must first insert one 's login details, including their user ID (US^{id}) and password (PW^{id}). The server verifies whether the user is authorized or not after receiving it. The authentication is accomplished via the new QMAP Model.

4.3 QMAP

An adversary $\mathcal{B}$ and a challenger $\mathcal{D}$ engage in a game that determines the security of a QMAP protocol. Let II_{Λ}^{i} stand for the participant of $\Lambda \in \{S_a, U_b\}$ in its ith instance. In the game, $\mathcal{B}$ can ask $\mathcal{D}$ questions, and $\mathcal{D}$ will respond as follows.

1. $h_a(m_a)$: When $\mathcal{B}$ runs the query with message m_a, $\mathcal{D}$ creates a random number $r_a \in z_*^w$, stores (m_a, r_a) in the list Li_{h_a}, and then returns r_a to $\mathcal{B}$, where $a = 0,1, \dots ,6$.
2. $ExtractUser(EU_{S_a})$: When $\mathcal{B}$ runs the query using the identity of the user $S_a's$ is EU_{S_a}, $\mathcal{D}$ generates the private key for S_a and stores it in the list Li_{SK}.
3. $ExtractServer(ES_{U_b})$: When $\mathcal{B}$ runs the query using the identity of the user $U_b's$ is ES_{U_b}, $\mathcal{D}$ generates the private key for U_b and stores it in the list Li_{UK}.
4. $Send(II_{\Lambda}^{i})$: When $\mathcal{B}$ runs the query with message m, $\mathcal{D}$ runs the QMAP protocol in accordance with its requirements and sends $\mathcal{B}$ the outcome.
5. $Reveal(II_{\Lambda}^{i})$: When $\mathcal{B}$ runs the query, $\mathcal{D}$ gives $\mathcal{B}$ the session key used in II_{Λ}^{i}
6. $CorruptUser(EU_{S_a})$: $S_a's$ private key is returned to $\mathcal{B}$ by $\mathcal{D}$ when $\mathcal{B}$ runs the query using $S_a's$ identity EU_{S_a}.
7. $CorruptServer(ES_{U_b})$: $U_b's$ private key is returned to $\mathcal{B}$ by $\mathcal{D}$ when $\mathcal{B}$ runs the query using $U_b's$ identity ES_{U_b}.
8. $Test(II_{\Lambda}^{i})$: When $\mathcal{B}$ runs the query, $\mathcal{D}$ chooses a coin at random $a \in \{0,1\}$. If a is greater than zero, $\mathcal{D}$ returns to $\mathcal{B}$ a random number with the similar length as the session key. If b is greater than one, $\mathcal{D}$ sends the session key involved in II_{Λ}^{i} to $\mathcal{B}$.

As a result, the authorized users are identified, and only those authorized users will be allowed to take part in the data transmission process.

5. Authorized User Clustering

The new two-fold optimal clustering approach is used to cluster the allowed users in the region once they have been recognized. The angular distance and trust level (direct trust) are calculated for each authorized user as per the anticipated model. These approved users are grouped together (i.e., grouped together). Based on the new MMO, an optimal CH for transporting the data between the nodes is found inside each of the formed clusters shown in Fig 3.

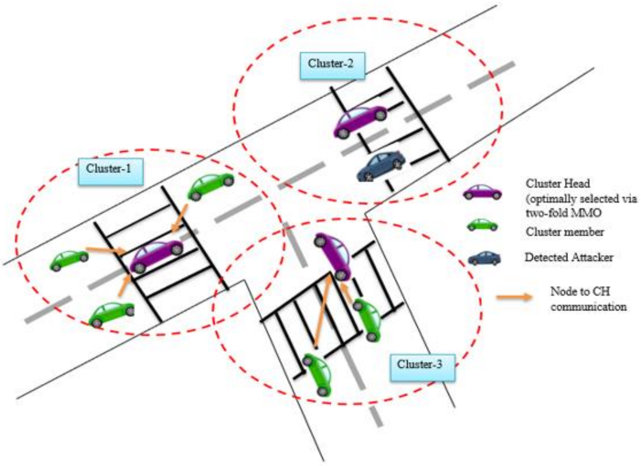


Fig 3: Clustering and optimal CH selection based on two-fold MMO model

5.1 Two-Fold Objectives

Angle Distance (AD): AD to figure out how far the IoT device is from the cluster that it wants to join. Using the angular matrix $\begin{bmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$, one can determine the angular distance. Eq.1 can be used to determine the new coordinates of a CM if it moves with an angle of with respect to the original coordinate. However, if the device is first added to the cluster, there is no previous coordinate, so the angle would be zero degrees. Equation 2 is used to determine the distance after determining the new coordinate. Assuming the IoT device is at coordinate $Q_i(Y_i, X_i)$, the CH's coordinate is $Q_{ch}(Y_{ch}, X_{ch})$ and the new coordinate after movement is $Q_i'(Y_i', X_i')$, the AD is calculated as per Eq. (1) and Eq. (2), respectively.

$$\begin{bmatrix} Y_i' \\ X_i' \\ 1 \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} Y_i \\ X_i \\ 1 \end{bmatrix} \qquad (1)$$

$$E_{i,j} = \|Y_{ch} - Y_i\| + \|X_{ch} - X_i\| \qquad (2)$$

Where, $\|\cdot\|$ the exact difference.

Each IoT device is created during the controller phase, and the Cluster Head (CH) oversees each one. Device authentication, block and cluster creation, and secret-key Sk generation are all handled by this layer. All of these transactions are gathered by the controller, which then creates a Merkle-root to produce the subsequent block to be added to the blockchain. The Angular Distance (AD) is used in this stage to gauge how far the Cluster Member (CM) is from the CH. If the CM is located closest to the CH, the CM may ask the CH to join the Cluster.

Trust: In direct trust, a trustor directly observes a target vehicle while depending on their interactions. Some academics define knowledge as the explicit data acquired by the trustor to assess the trustee based on certain factors that depend on the participating nodes and services. Although the importance of direct trust is seen to outweigh that of indirect trust, the combination of both is taken into account when evaluating a vehicle.

5.2 Meliorated Mayfly optimization algorithm (MMO)

The newly developed MMO model is the conceptual improvement of the standard MA. In fact, MA model has been developed with the inspiration acquired from the behavior of the mayflies. Insects called mayflies are members of the order Ephemeroptera, which is a suborder of the palaenoptera family of insects. These insects primarily occur in the UK during the month of May, hence the name "mayfly". Aquatic nymphs of immature mayflies spend several years developing before they are preparing to develop as adult mayflies. The females are attracted by the male by swarming beyond the water within few meters. They dance as nuptials, moving in a distinctive sequence of up and down motion. To reproduce, these Female mayflies move to these swarms. That process stays only for some seconds then the eggs are dropped in the water and they continue the cycle. Here, MA do all the essential modifications, thereby the algorithm's performance is enhanced across feature sets of varying sizes.

- The behaviour of Male mayflies:

Eq. (3) is used to update the position of the male mayfly:

$$\boldsymbol{y_i^T} = \boldsymbol{y_i^{T+1}} + \boldsymbol{u_i^{T+1}} \qquad (3)$$

Here, y_i^T is the male mayfly's current position and by calculating the velocity u_i^{T+1} with the current position, the next position y_i^{T+1} is achieved. To increase their speed, Male mayflies float a few metres just above water's level. The velocity is measured for male mayfly in Eq.(4).

$$u_{kj}^{T+1} = G * u_{kj}^T + b_1 * E^{-\beta r_p^2} * (\mathrm{pbest}_{kj} - y_{kj}^T) + b_2 * E^{-\beta r_g^2} * (\mathrm{gbest}_j - y_{kj}^T) \qquad (4)$$

Here, u_{kj}^T reflects the velocity of the mayfly at time T, y_{kj}^T in dimension j, is the similar mayfly's position at time T, the positive attraction constants are b_1 and b_2 in which the cognitive and social components contribution is quantified, g is a coefficient of gravitation and β is a coefficient of fixed visibility, which limits the visibility of mayfly to others. pbest_{kj} is the position mayfly k visited and it is optimal and gbest_j is the component jth position of the best male mayfly. The minimization problem pbest_{kj} is shown in Eq. (5)

$$\text{pbest}_k = \begin{cases} y_k^{T+1} \\ if\ fitness(y_k^{T+1}) < fitness(\text{ pbest}_k) \end{cases} \quad (5)$$

Here, fitness (y_k^T) gives the position for fitness value, i.e., the solutions quality. Finally, the Cartesian distance between y_k and pbest_k are represented as r_p and the Cartesian distance between r_k and $gbest$ is represented as r_g.

$$|y_k - z_k| = \sqrt{\textstyle\sum_{j=1}^{n}(}\, y_{kj} - y_{kj})2 \quad (6)$$

Here, y_{kj} depicts the position of the element as jth and the position of mayfly as kth and z_k denotes either pbest_k or $gbest.$ nuptial dance performance of the best mayfly is important because it gives an element randomly to the algorithm. This dance's mathematical formulation is in Eq.(7)

$$u_{kj}^{T+1} = \text{g} * u_{kj}^{T} + \text{d} * \text{s} \quad (7)$$

Here, d represents the coefficient of nuptial dance, random value is represented as s ∈ $[-1, 1]$. The coefficient of the nuptial dance decreases progressively as $ditr = d0 \times \delta\ itr$. The nuptial dance coefficient's initial value is d0, iterations current number is represented as itr and a random number δ is ∈ [0, 1]. The newly proposed equation is given in the Eq. (8) and Eq. (9), respectively.

$$y_i^{T+1} = \frac{(y_i^T + u_i^{T+1}) * g}{d} \quad (8)$$

$$g = g_{max} - \left(\frac{g_{max} - g_{min}}{iter^{max}}\right) \quad (9)$$

In the male mayfly update stage, the gravitational coefficient has been considered to enhance the convergence of solution.

- Female mayflies Movement:

Female mayflies gather near males to reproduce. The updated new mathematical model (proposed) is shown in Eq. (10).

$$Z_i^{T+1} = Z_i^T + u_i^{T+1} * g + fl \quad (10)$$

Here, the gravity coefficient as well as random walk is considered to prevent the solution from getting trapped into local optima. Z_i^T is the female mayfly's present position at time T is enhanced by computing its velocity u_i^{T+1} . The current solution's attraction quality is an attraction process among males and females, i.e., the optimal male performance attracts the optimal female performer, and so forth.

$$u_{kj}^{T+1} = \begin{cases} if\ fitness\ (z_k) > fitness(y_k) \\ g * u_{kj}^T + b_2 * e^{-\beta r_{mf}^2 * (y_{kj}^T - z_{kj}^T)} \\ else\ if\ fitness(z_k) \le fitness(y) \\ g * u_{kj}^T + fl * s \end{cases} \quad (11)$$

In Eq. (11), u_{kj}^T at time t, represents the jth element of the kth female mayfly's speed, z_{kj}^T at time T represents the position k in dimension j for female mayfly, y_{kj}^Tat time T represents the jth component position in k of male mayfly, b_2 and β are pre-defined constants for the transparency coefficient and the attraction coefficient, correspondingly, g is the formerly defined gravity coefficient, the random value s has ∈ $[-1, 1]$, and r_{mf} is the male mayfly and female mayfly's Manhatan distance (instead of cartesian distance). fl is a random walk coefficient when a female does not find a man attractive and $fl_{itr} = fl_0 \times \delta_{\ itr}$. Here itr and δ are two variables already described. The Manhattan distance (in Eq. (12)) in n-dimensional space from two locations $(y = y_1, y_2, \dots, y_n)$ and $(x = x_1, x_2, \dots, x)$ is the total of the distances in each dimension.

$$d(y, x) = \textstyle\sum_{i=1}^{n} |y_i - x_i| \quad (12)$$

- crossover:

The proposed crossover procedure starts by recognizing a male mayfly and then a female mayfly. Selections are made according to fitness value, with the best male paired with the best female. This is mathematically shown in Eq. (13) and Eq. (14), respectively.

$$Offspringa = s_{of} * male + (1 - s_{of}) * female \quad (13)$$

$$Offspringb = s_{of} * male + (1 - s_{of}) * female \quad (14)$$

Male indicates the male parent mayfly, while female indicates the female parent mayfly and r_{of} is a given value among 0 and 1. The initial offspring's velocities that are initially set as 0.

- **Mutation:**

The exploration ability in this algorithm is enhanced by mutating the newly created offspring. A random number that is normally distributed is included with the variable offspring is denoted as per Eq. (15).

$$Offsprings_n' = Offsprings_n + k \quad (15)$$

Here, a random value k is normally distributed.

6. Data Encryption and Decryption

The newly proposed Optimized Blowfish Algorithm is used to encrypt the data before it is sent via the block chain. These encrypted files are kept in the cloud and sent via blocks of the block chain. The decryption operation is carried out at the receiver end. Additionally, using the brand-new Meliorated Mayfly optimization method, the blowfish algorithm's private key is chosen ideally to increase the security level of the data being communicated (MMO).

The first symmetric encryption algorithm is called blowfish. Data is encrypted and decrypted employing the similar encryption key in symmetric encryption. The encryption algorithm employs the sensitive information and the symmetric encryption key to transform the sensitive material into cipher - text. In order to make intruders' encryption techniques more secure and their key space larger, a new method of manipulating bits that works with 4-states has been demonstrated (0,1,2,3). 0 and 1 are the only bits utilised in (XOR). Device authentication, block and cluster creation, and secret-key S_k generation are all handled by the controller layer.

Every round of the proposed update uses the current procedure hash function (#) that was first used in the original Blowfish algorithm. To apply this operation on both sides, an additional key, a binary key that converts to a 4-state key, is required. The first K1 key will generate the following when combined with XL and Pi. In the initial blowfish, it left a portion in each round. The second key will create the right position using F(XL) and XR. Each of the three inputs can be converted to one of four states (0, 1, 2, or 3), or to the corresponding decimal digits, turning them from 64 bits to 32 digits. Boost F2 function The Blowfish function F was changed without going against the security guidelines. This is mathematically shown in Eq. (16) to Eq. (18), respectively.

$$FU_1(yL) = \left(\left((A_1 xor A_2) + A_3, mod\ 2^{64}\right) xor A_4\right) \tag{16}$$

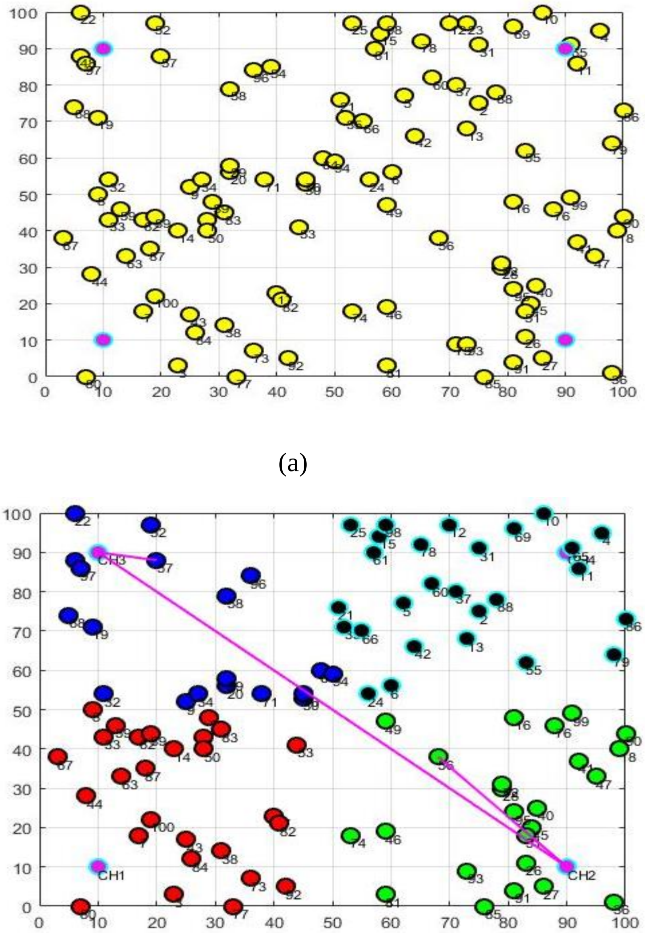
$$FU_2(yL) = \left(\left((A_5 xor A_6) xor A_7\right) xor A_8\right) \tag{17}$$

$$FU(yL) = [FU_1(yL), FU_2(yL)] \tag{18}$$

Concatenating FU_1 and FU_2 results in the final FU function, each of which has four S-boxes (yL). This change shortens the time by converting the original 64 bits Function FU to a 128 bits Function FU.

7. Merkle Root Tree-Blockchain Data Transmission

Merkle tree, or the overview of every transaction in a block, is the tree of hash values of types of transactions in the frames. Then it is called as "Hash Tree". It aids in the efficient and protected verification of a block's contents.



(a)

(b)

Fig 4: (a) Initialization and (b) Routing

Above figure 4 explains as first, the nodes are initialized and after authentication, the nodes are routed to transfer the data. Additionally, it ensures that the blocks' content is consistent. The Merkle tree structure is employed by both Ethereum and Bitcoin for transaction processing. The interacting notifications are addressed as transactions in blockchain. The controller assembles all of these transactions, and Merkle-root is used to generate the resulting block that will be added to the blockchain.

8. Result And Discussion

8.1 Experimental Setup

The projected model has been implemented in MATLAB. The evaluation has been made in terms of encryption time, security and decryption time as well.

8.2 Overall Performance Analysis of the projected model

In this part, the test outcomes from the suggested method are examined. Multiple threaded requests are used to simulate the transaction load and user count. The proposed method's effectiveness is evaluated by different methods using a variety of metrics, including encryption time, decryption time, and security is shown in the below Table 1. On analyzing the outcome, the projected model has recorded the highest security level as 97.3%, and this is owing towards the optimal selection of the private keys with MMO model in blowfish cryptography model.

Table 1: Overall Performance Analysis of proposed and Existing Methods

Methods	***Encryption Time (Sec)***	***Decryption Time (Sec)***	***Securit y (%)***
Proposed Model	***0.7913***	***0.7604***	***97.3***
Blowfish	***1.2968***	***0.7774***	***93.4***
AES	***2.7092***	***3.0029***	***79***
ECC	***4.771***	***1.2354***	***85***

8.3 Performance Analysis of the projected model in terms of Encryption Time

The effectiveness of the suggested methodology is estimated relating to security, decryption time, and encryption time. The main goal of the suggested method is to transmit data safely and without information loss. The outcomes acquired in terms of encryption time is shown in Fig.5. The encryption time recorded with proposed model is 0.5s, which is the lowest value compared to blowfish=1.5s, AES=2.5s and ECC=5s. The major reason behind the reduction in the encryption time is due to the

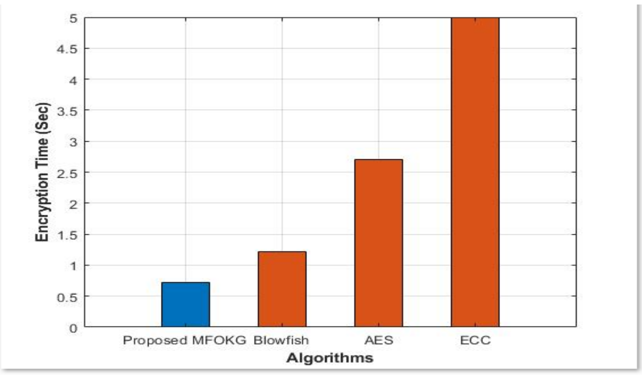


Fig 5: Performance of the suggested method based on encryption time

8.4 Performance Analysis of the projected model in terms of Decryption Time

The effectiveness of the suggested methodology is evaluated in terms of decryption time, and the corresponding results acquired are shown in Fig. 6. On analyzing the acquired outcomes, it’s clear that the projected model has recorded the lowest decryption time as 1.2s, which is the least value.

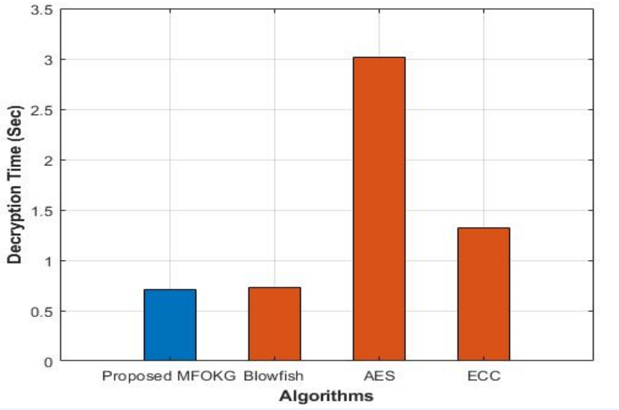


Fig 6: Performance of the suggested method based on decryption time

8.5 Performance Analysis of the projected model in terms of Security

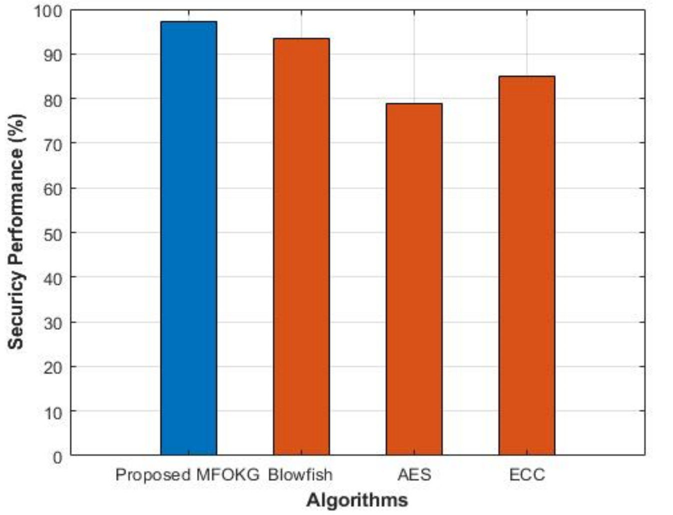


Fig 7: performance analysis of the projected model in terms of security

The results of measuring the proposed algorithm's security level are shown in Fig. 7. The total no. of packets effectively received by the target side and the total no. of packets sent by the source side during the simulation are used to determine the security level. The proposed method has a high level of security, as QMAP based user authentication and optimal CH based data transmission is used. All of the aforementioned findings make it clear that the suggested technique is superior to the suggested strategy. The suggested method reduces storage and computational overhead while securing user data from numerous threats.

9. Conclusion

This paper has developed a unique cluster-based secured user authentication mechanism is recommended. The four primary phases of the anticipated paradigm were (a) user authentication, (b) clustering of authorised personnel, (c) data encryption and decryption, and (d) block chain-based protected data transit. Using the Query

Assisted Multi-User Authentication Protocol, the Internet of Vehicles (IoV) network performs initial user authentication (QMAP). The two-fold optimum clustering model has been employed to group the authorised users after that (only authorised users are allowed to participate in data transfer). The two-fold optimum clustering model was used to determine the two-fold objectives for authorised users, such as angular distance and trust level. The authorised user with the highest degree of trust and smallest angular distance has been determined to be the Cluster Head (CH). The best CH was therefore chosen using the Meliorated Mayfly optimization technique (MMO). In this MMO, the Mayfly Algorithm standard version was extended. The cluster's nodes communicate with one another using the CH that was selected with the highest regard for efficiency after it has been determined. Additionally, secure data transfer across nodes in different clusters is accomplished using block chain-based data transmission. Prior to transmission across the block chain, the data is encrypted using the recently developed Optimized Blowfish Algorithm. These encrypted data are transferred across blocks of the block chain and stored in the cloud. The receiver end performs the decryption operation. Additionally, the blowfish algorithm's private key has been optimally selected utilising the brand-new Meliorated Mayfly optimization (MMO) technique to raise the security level of the data being conveyed. Data transport has been done securely. In terms of encryption time, security, and decryption time, the proposed approach has also been validated. On analyzing the outcome, the projected model has recorded the highest security level as 97.3%, and this is owing towards the optimal selection of the private keys with MMO model in blowfish cryptography model.

Declarations:

Funding

On Behalf of all authors the corresponding author states that they did not receive any funds for this project.

Conflicts Of Interest

The authors declare that we have no conflict of interest.

Competing Interests

The authors declare that we have no competing interest.

Data Availability Statement

All the data is collected from the simulation reports of the software and tools used by the authors. Authors are working on implementing the same using real world data with appropriate permissions.

References

[1] Viriyasitavat, W., Da Xu, L., Bi, Z. and Hoonsopon, D., 2019. Blockchain technology for applications in internet of things—mapping from system design perspective. IEEE Internet of Things Journal, 6(5), pp.8155-8168.

[2] Viriyasitavat, W., Anuphaptrirong, T. and Hoonsopon, D., 2019. When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities. Journal of industrial information integration, 15, pp.21-28.

[3] Alam, T., 2019. Blockchain and its Role in the Internet of Things (IoT). arXiv preprint arXiv:1902.09779.

[4] Sheth, H. and Dattani, J., 2019. Overview of blockchain technology. Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146.

[5] Ali, J., Ali, T., Musa, S. and Zahrani, A., 2020. Towards secure IoT communication with smart contracts in a blockchain infrastructure. arXiv preprint arXiv:2001.01837.

[6] Bodkhe, U. and Tanwar, S., 2021. Secure data dissemination techniques for IoT applications: Research challenges and opportunities. Software: Practice and Experience, 51(12), pp.2469-2491.

[7] Mylrea, M. and Gourisetti, S.N.G., 2017, September. Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In 2017 Resilience Week (RWS) (pp. 18-23). IEEE.

[8] Zhu, X., 2021. Complex event detection for commodity distribution Internet of Things model incorporating radio frequency identification and Wireless Sensor Network. Future Generation Computer Systems, 125, pp.100-111.

[9] Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M., 2018. On blockchain and its integration with IoT. Challenges and opportunities. Future generation computer systems, 88, pp.173-190.

[10] Atlam, H.F., Alenezi, A., Alassafi, M.O. and Wills, G., 2018. Blockchain with internet of things: Benefits, challenges, and future directions. International Journal of Intelligent Systems and Applications, 10(6), pp.40-48.

[11] Minoli, D. and Occhiogrosso, B., 2018. Blockchain mechanisms for IoT security. Internet of Things, 1, pp.1-13.

[12] Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R.C., Michelin, R.A., Zorzo, A.F. and Kanhere, S.S., 2020. Blockchain technologies for iot. In Advanced applications of blockchain technology (pp. 55-89). Springer, Singapore.

[13] Nair, G. and Sebastian, S., 2017. Blockchain

technology; centralised ledger to distributed ledger. International Research Journal of Engineering and Technology, 4(3), pp.2823-2827.

[14] Zhang, J., Rajendran, S., Sun, Z., Woods, R. and Hanzo, L., 2019. Physical layer security for the Internet of Things: Authentication and key generation. IEEE Wireless Communications, 26(5), pp.92-98.

[15] Quilala, T.F.G., Sison, A.M. and Medina, R.P., 2018. Modified blowfish algorithm. Indones. J. Electr. Eng. Comput. Sci, 11(3), pp.1027-1034.

[16] Pavithran, D., Shaalan, K., Al-Karaki, J.N. and Gawanmeh, A., 2020. Towards building a blockchain framework for IoT. Cluster Computing, 23(3), pp.2089-2103.

[17] Singh, S., Hosen, A.S. and Yoon, B., 2021. Blockchain security attacks, challenges, and solutions for the future distributed iot network. IEEE Access, 9, pp.13938-13959.

[18] Kuzminykh, I., Yevdokymenko, M. and Sokolov, V., Encryption Algorithms in IoT: Security vs Lifetime.

[19] Kiruthiga, N., Lokitha Karthi, R. and Ramya, B., 2018. SECURED SMART HOME AUTOMATION SYSTEM BASED ON USER BEHAVIOUR USING INTERNET OF THINGS. Pakistan Journal of Biotechnology, 15(2), pp.383-389.

[20] Singh, S.K., Rathore, S. and Park, J.H., 2020. Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. Future Generation Computer Systems, 110, pp.721-743.

[21] Hammi, M.T., Hammi, B., Bellot, P. and Serhrouchni, A., 2018. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Computers & Security, 78, pp.126-142.

[22] Cui, Z., Fei, X.U.E., Zhang, S., Cai, X., Cao, Y., Zhang, W. and Chen, J., 2020. A hybrid blockchain-based identity authentication scheme for multi-WSN. IEEE Transactions on Services Computing, 13(2), pp.241-251.

[23] Panda, S.S., Jena, D., Mohanta, B.K., Ramasubbareddy, S., Daneshmand, M. and Gandomi, A.H., 2021. Authentication and key management in distributed iot using blockchain technology. IEEE Internet of Things Journal, 8(16), pp.12947-12954.

[24] Hang, L. and Kim, D.H., 2019. Design and implementation of an integrated iot blockchain platform for sensing data integrity. Sensors, 19(10), p.2228.

[25] Alrubei, S.M., Ball, E. and Rigelsford, J.M., 2022. A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer. IEEE Access, 10, pp.18583-18595.