International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Hybrid Cryptographic Algorithm-based User Authentication and Secured Data Transmission in Blockchain-based Internet of Vehicles (BIOV) Environment

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

Submitted: 15/12/2023 **Revised**: 20/01/2024 **Accepted**: 03/02/2024

Abstract: The emergence of Blockchain-based Internet of Vehicles (BIoV) is driven by disruptive technologies, vital for robust vehicular information systems. Disputes over data rights or security violations can disrupt transportation. Addressing BIoV's security, a new hybrid cryptographic authentication model is introduced, comprising four steps: data classification, encryption, blockchain-based transfer, and user authentication. Sensitive vehicle data is split and encrypted using Two-Level Advanced Elliptic Curve Cryptosystems (2LAECC). The private key is generated optimally via Enriched Bat Optimizer. Validated recipients receive information based on computed dual-trust scores. The model's security, encryption, and decryption are validated. This model fortifies BIoV's future through enhanced security, efficient encryption, and trusted data sharing.

Keywords: *IoV, Blockchain, Two-Level Advanced Elliptic Curve Cryptosystems (2LAECC), Elliptic Curve Cryptosystems (ECC), Advanced Encryption Standard (AES).*

1. Introduction

A blockchain consists of linked blocks storing data like scripts, records, and transactions. Participants maintain this chain using techniques that create a sequence. It's referred to as distributed ledger technology (DLT) [1]. Blockchain enables divided access to distributed details [2]. DLT and blockchain enable trusted data logging for multiple groups, creating non-repudiable databases [3]. IoV is a cooperative vehicle network [4] aiming for environmental protection, energy conservation, efficiency, and safety in smart transportation [5]. Vehicles collaborate through intelligent sensors, cameras, and devices [6].

IoV facilitates communication between vehicle nodes, enhancing safety and comfort [7]. It uses modern communication, cloud services, and Internet devices [8]. Increased safety and traffic accidents drive IoV's popularity [9]. Trust management (TM) ensures data authenticity. TM evaluates vehicles based on transmitted signals and prior behavior [12].Several notable contributions have been made in the field of Internet of Vehicles (IoV) using blockchain technology: Kang et al. [16] proposed a secure IoV utilizing blockchain. Their approach involves a two-stage soft security augmentation method that includes block verification and miner selection. They introduced a reputation-based voting system for safe miner selection, along with standby miners to prevent internal cooperation among active miners.Cui et al. [17] developed a containerized edge-computing platform named CUTE for IoV using blockchain. This platform offers low-latency computing services by distributing containers to appropriate edge servers, while orchestration and resource management are overseen by a central controller.

Electric vehicles have benefits, but face range and power grid challenges [13]. Vehicle-to-vehicle (V2V) electricity trading is explored [14]. IoV gathers traffic data for prediction and accident detection, raising security challenges [15]. To address these, we propose Two-Level Advanced Elliptic Curve Cryptosystems (2LAECC), combining ECC and AES [16].

Following are some manifestations of this research's main contribution:

- Isolated sensitive data are encrypted via the newly projected Two-Level Advanced Elliptic Curve Cryptosystems (2LAECC), which are the conceptual hybridization standard Models of the Elliptic Curve Cryptosystems (ECC) and the Advanced Encryption Standard (AES) respectively.
- The behavior of the receiver is validated (i.e., trusted or malicious) based on the computed dual-trust scores.

This essay's remaining sections are organized as follows: discuss: Part 2 demonstrates literature works experienced in the IoV-blockchain environment. Part 3 demonstrates Proposed BlockChain-based Authentication Model. Part 4, Part 5, and Part 6 manifest information about the vehicle data categorization, Data encryption, decryption, and Blockchain-based data storage respectively. The information regarding Malicious User Identification is portrayed in part 7. In addition, part 8 demonstrates outcomes received utilizing planned model, also part 9 ends this study.

2. Proposed Blockchain-Based Authentication Model

2.1. Overview of the Proposed Model

A novel secured data transmission model is created in this study by going through three main stages: (a) data classification (isolating sensitive data from non-sensitive data), (b)

[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*
** Corresponding Author Email: girijavm23@gmail.com, girijav668@gmail.com*

data encryption and decryption, (c) blockchain-based data storage, and (d) user authentication (malicious user identification). The onboard unit (OBU) and the roadside unit (RSU) make first move. At the time of registration, to find the correct TA node in the traffic order center, OBU uses the address indices; various addresses match various TA nodes. A central service called address index makes it straightforward for on-board nodes to locate the proper central nodes. The center node assesses the application supplied by the onboard node to establish its legitimacy and whether it is in command of leading address. Proposed model's general design is described in Fig.1.

Step 1 : **Data Categorization**- user data (inclusive of VIN, car owner information, the brand of car, license plate, and color) $U^i; i = 1,2, \ldots N$ is first divided into sensitive and non-sensitive categories. Here, N denotes the overall count of users in the considered network. Among U^i, the VIN and information of the car's owner are considered sensitive data, while the license plate, brands, and color are considered non-sensitive data. The sensitive data is represented as S^i, while the non-sensitive data is pointed as G^i.

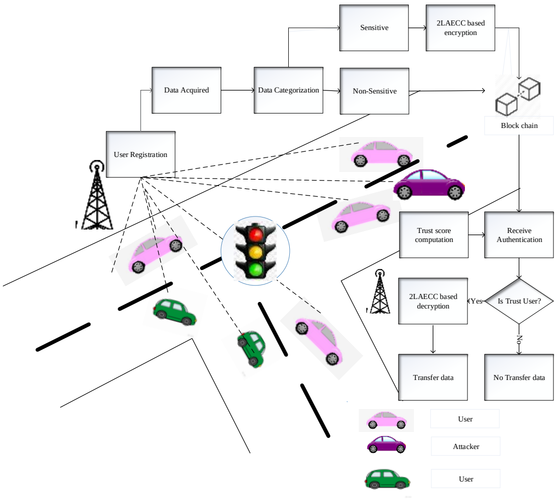


Figure 1: Architecture of the projected model

Step 2 : **Proposed Data Encryption and Decryption Phase-** The identified sensitive data S^i is encrypted using a newly introduced Two-Level Advanced Elliptic Curve Cryptosystems (2LAECC) Model. This 2LAECC is the conceptual blend of Elliptic Curve Cryptosystems (ECC) and standard Advanced Encryption Standard (AES), respectively. In 2LAECC model the optimal private key PK_{TC} is selected via Enriched Bat Optimizer (EBO). The encrypted data acquired from the 2LAECC model is denoted as E^i.

Step 3 : **Blockchain-based data storage-** Then, the encrypted sensitive data E^ias well as the non-sensitive data $G^i$is sent in via the blocks of the blockchain (for data transmission).

User authentication- Using a computer trust score T (direct and indirect), the receiver (user) is identified to be a trusted or malicious one. If the receiver is identified to be the trusted one, then the data E^i is decrypted via the 2LAECC approach, and the receiver gets the original information U^i. As a whole, secured data transmission takes place in BIoV.

2.2. System Model

The components of the system are as follows:

- Traffic Management Center (TC): The TC is the supreme control hub of the IoV system. It is connected to Road Side Units (RSUs) and is responsible for managing critical data and recording traffic participants. TC maintains direct or indirect links to both temporary and permanent vehicle identities. It is highly trustworthy and resilient to external threats. The TC functions as a full node, creating Genesis blocks, mining, generating, and uploading certifications to the blockchain ledger.

- Road Side Units (RSUs): Positioned at road edges and intersections, RSUs handle tasks like vehicle access and identity validation. They serve as the edge processor core for the blockchain.

- Vehicles: The term "vehicle" encompasses all intelligent vehicles, each maintaining its blockchain accounts, private-public key pairs, and relevant data. The processing capabilities vary among different vehicle types.

Blockchain Operation: The blockchain's functionality relies on distributed ledger technology, transaction processing, consensus methods, and encryption algorithms. IoV members generate their public-private key pairs and wallet addresses using blockchain's encryption algorithms.

2.2.1. Establishment of Transport Equipment

The device generates distinct public and private key pairs as well as wallet addresses following TC and RSU that have joined the blockchain-powered Internet of Vehicles system. Roadside unit RSU_a applies for a device certificate by encrypting its attribute data (device serial number, geographic coordinates, etc.) using PK_{TC} (optimally generated private keys), and then sends it to TC. TC encrypts (PK_{TC},$address_a$) along public key of RSU_a also publishing it to blockchain while credential of the RSU_a. A timestamp is provided to each deal whenever it is uploaded to blockchain, confirming transaction monitorability.

2.2.2. Stage of Establishing Vehicle Equipment

Adding a transaction to blockchain requires a significant amount of time before a vehicle can be connected on time and receive official certification. A temporary certificate is created using the following procedure:

(1) RSU_a occasionally transmits its signed identity certificate.

(2) After receiving the broadcast data, the vehicle user utilizes the optimal public key TA and RSU_a confirming the identification of the receiver.

(3) If the signature is valid, the RSU_a is found to be trustworthy, and the vehicles encrypt its properties (Attributes are divided into two parts: encrypted sensitive data is secured with PK_{TC} and common data verification is secured with RSU_a).

(4) The data is sent to RSU_a by the vehicle. In addition to decrypting the sensitive data, performing preparatory verification, also issuing a lightweight transient certificate ($address_{u_v}$ || convenience || addressRSU_a || RSU_a signature), RSU_a validates the signature. The certificate's validity term must be longer than how long it takes something to be recorded on blockchain.

(5) Later obtaining transient document, vehicle checks mark on it also utilizes it as a transient individuality in system to contribute to action.

(6) Then, as part of a blockchain transaction, the general vehicle attributes are added to the sensitive data that has been encrypted with a temporary certificate. After the agreement is complete, it is added to blockchain. TA also RSU are retained, also as full nodes, they may read and write to the blockchain.

3. Vehicle Data Categorization

Once the users register in the network, he submits their data U^i to the network. This data $U^i$is split into (a) General Information $G^i$and Sensitive Information S^i. This categorization assists in reducing the storage space as well as time spent on decryption and encryption process. General information G^icontains models, license plates, colors, and brands, whereas sensitive information S^i contains vehicle identification number (VIN) and vehicle owner information.

4. Proposed Data Encryption/ Data Decryption Model

4.1. Two level advanced Elliptic Curve Crypto Systems (2LAECC)

The identified sensitive information S^i is encrypted via a new Two-Level Advanced Elliptic Curve Cryptosystems (2LAECC), which is the conceptual combination of standard the Elliptic Curve Cryptosystems (ECC) and Advanced Encryption Standard (AES), respectively. In 2LAECC, the public key is generated using optimized ECC, and the encryption/decryption is carried out via the AES model. In the 2LAECC model, the private key is generated optimally via the new Enriched Bat Optimizer (EBO). Steps succeeded in the 2LAECC model are demonstrated:

Public Key Generation Using ECC

Step 1: As the prime number, pick any value v.

Step 2: To generate the public key, a random number $v(a)$.

Step 3: Wherein, $v(a)$< v, Calculate G for the point on the curve.

Step 4: Where G > v. Calculate the public key using Eq. (1)

$$p = v(a) * G \tag{1}$$

Where, p points to the Public Key; $v(a)$ and represents the Private Key

Step 5: Utilizing the new Enriched Bat Optimizer (EBO), the best private key among those generated is chosen.

Step 6: After calculations, deliver the optimal Public Key p.

Encryption/ Decryption Using AES.

Step 1: Consider the input file (S^i)

Step 2: Add the ECC-generated optimal key p.

Step 3: The input file (S^i) is encrypted using AES using the public key that is produced by ECC.

Step 4: Once (S^i)is encrypted using AES, the acquired cipher text E^i (encrypted data) is transmitted over the blocks of the blockchain.

Step 6: The generated same public key ' p ' is used at the receiving end to decode the encrypted data and recover the original data U^i.

4.2. Enriched Bat Optimizer (EBO)

This EBO is an extended version of the standard bat algorithm. The input (solution) to EBO is the generated keys of 2LAECC. The key points to the velocity of the agent (i.e. ${V_i}^t$). Since EBO gets trapped in local optima. It is not sufficient for optimal key generation. Therefore, EBO is introduced in this research work. The way that bats measure distances with echolocation has an impact on EBO. When hunting at night, bats frequently use quick, powerful sound impulses to locate barriers or targets. A bat's unique hearing system can be used to determine the object's size and location. The following is a summary of the EBO process:

Step 1: The population of the search agent is initialized, and the bat parameters are computed.

Step 2: Upgrade the global best position L^*, frequency of the pulses f_i, speed, and position of the i^{th} as per Eq. (2). The frequency of the pulses f_i is computed using the newly proposed expression (Eq. (2)). Here, the notation $f_{max}$and f_{min} points to the maximal and minimal frequency, respectively. The maximal frequency is set as 100, and the minimum frequency is 0. In addition, the velocity ${V_i}^{t+1}$of the serac agent is computed using the newly projected expression given in Eq. (3). In the proposed expression, the global best position and global worst position as well as position best of the solutions.

$$f_i = \frac{f_{max}+(f_{max}-f_{min})}{f_{min}} * \beta \tag{2}$$

$$ {V_i}^{t+1} = \left[\frac{V_i^t+(X_i^t+X_{best}^g)f_i}{X_{worst}^g}\right] * L_{best}^P \tag{3}$$

Where L_{best}^g represents the global best position, L_{worst}^g denotes the global worst position and L_{best}^P points to the position best.

$$ {L_i}^{t+1} = L_i^t + V_i^t \tag{4}$$

Where position at time t and L_i^t and V_i^t are velocity. ${V_i}^{t+1}$, ${L_i}^{t+1}$ are the velocity and position at time $t + 1$. β is a random number between 0 and 1. Since, L_{best}^g , L_{worst}^g and $L_{best}^P$are considered for finding the optimal position of the solution (i.e., optimal keys).

Step 3: If the random number is more than r_i, the following calculation gives a new answer for the bat.

$$L_{new} = L_{old} + \varepsilon A^t \tag{5}$$

where A^t is ordinary volume of all bats at time t, and ε is a random number between [1, 1].

Step 4: If the random number falls below A_i and $f(L_i) < f(L^*)$ Next the modified approach is approved. Then, update A_i and r_i as follows, respectively:

$$A_i^{t+1} = \alpha . A_i^t \tag{6}$$

$$r_i^t = r_i^0 [1 - e^{-\gamma}], \tag{7}$$

A_i^{t+1} and A_i^t denotes the loudness at time t , $t+1$ respectively. r_i^t and $r_i^0$are the initial pulse rate and pulse rate at time t respectively. α points to the constant parameter in range [0,1]. γ is a constant component, γ>0. As $t \rightarrow \infty, A_i^t \rightarrow 0$ and $r_i^t \rightarrow r_i^0$.

Step 5: Find present ideal solution L^* by ranking bats by their fitness.

Step 6: Return to Step 2 and output the globally optimal solution after the maximum number of iterations has been reached.

The encrypted sensitive data (S^i) and General information (G^i) are transmitted via the blockchain.

5. Blockchain based Data storage

5.1. Mechanism for Consensus

The consortium blockchain employs an AoR-based consensus technique. The blockchain is maintained by the commissioners.

5.1.1. Blockchain Role-Node definition

Ordinary nodes (U) authenticate their identity through cryptography and data via signatures. Regular nodes can freely join or leave. They can "observe" consensus but not partake in block-building. Users contribute to block distribution and message forwarding for internet credit incentives.

Commissioners (C): They collectively manage the consortium blockchain, assessing bids, approving blocks, and transactions. Each commissioner verifies a new block produced, with approval from 51% leading to block acceptance. Decisions are vote-based and commissioners are compensated.

Bidders (B): Deposits precede each auction round for bidders. The winner becomes vendee (V) and competes to create the next block. The vendee's credit is used for transaction value reassignment.

Vendee receives a reward post-task completion.

5.2. Process of Consensus

Several ordinary nodes are assumed as N_o, several commissioners chosen from ordinary nodes are assumed to be N_m, and each auction interval is assumed to be T_i. Vendee is chosen through the time T_v, also a new block must be created over time T_u, $T_v + T_u \ll T_i$. A legitimate block receives at least $(N_m/2) + 1$ commissioners' signatures and documents for the whole auction transaction. A consensus round is a name given to this procedure. The original recipient has lost the chance to create the next block, therefore if no legitimate block is generated within T_u, the 2nd greatest bid creates the block as the winner, and so on. The system can eventually reach an agreement as soon as one bidder does it effectively.

The following actions are necessary to generate a new block:

S1: Each node in the chain is given a specific amount of involvement credits at the start, allowing them to trade with one another and produce verified transaction details. They check the transaction details concurrently. They provide the transaction information to the commission if the transactions are accurate. After each round of auction, a credit bonus is granted to each online assignment.

S2: Every commissioner keeps track of transaction information and keeps legal information in the transactions pool.

S3: To divide the block to all commissioners, the vendor gathers every legitimate transaction in the transaction pool.

S4: is the due date for the block. Commissioner checks information in a raw block after getting it. The block must be signed for confirmation if the commissioner allows it. The vendee acquires the timestamp data from the NTP server after getting at least $(N_m/2) + 1$ signatures. The block is published on the network and signed by the vendee if the timestamp is earlier than $T_{new\ block}$.

$$T_{new\ block} = prior\ block\ time + T_v + T_u \tag{8}$$

The committee allows the credit given by the vendee. Timestamps that are later than $T_{new\ block}$ indicate inefficient new block generation. The auction mechanism takes the place of the vendee, and the stated job must be finished by the new cutoff time $T_{new\ block} = T_{new\ block} + T_u$. The previous vendee who did not finish the job is held accountable. Nodes are protected by this technique from the ineffective operation and harmful purposes.

S5: Following the receipt of the legitimate block, the vendee removes unlawful transactions from the transaction pool. Additionally, each node awaits the start of the subsequent round of the auction at a time T_i. If $T_{new\ block} > T_i$, the network has terminated or all bidders are unable to generate the new block in time.

6. Malicious User Identification

At the blockchain receiver's end, sensitive data (S^i and G^i) is collected. Prior to sharing information (and) with the intended recipient, validation occurs via computed dual-trust scores (direct and indirect). Trusted recipients receive data; otherwise, no information is shared. Trust relies on interactions between entities, depicted in Figures 2 and 3.

Direct-Trust: Direct trust stems from observed interactions, evaluating trustees based on specific parameters. Both direct and indirect trust factors combine in vehicle evaluation.

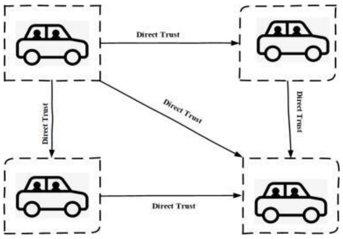


Figure 2: Direct Trust

Indirect-Trust: Indirect trust is based on trusted neighbors' opinions about the target node (trustee), derived from past interactions. Reputation and experience explain indirect trust, with experience measuring the trustor's belief in the trustee's task competence.

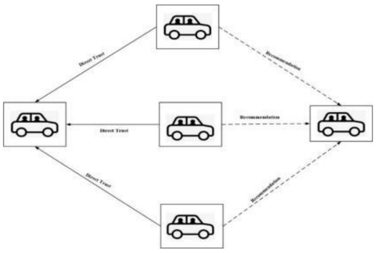


Figure 3: Indirect Trust

7. Results and Discussion

7.1. Experimental Setup

The proposed method was implemented using MATLAB and assessed using dataset1 [24], dataset2 [25], and dataset3 [26]. The model's performance was compared with existing methods including AES, ECC, DES, and RSA, focusing on encryption and decryption times, as well as security.

7.2. Examining encryption time

Table 1 presents the results of the proposed model's encryption time evaluation:

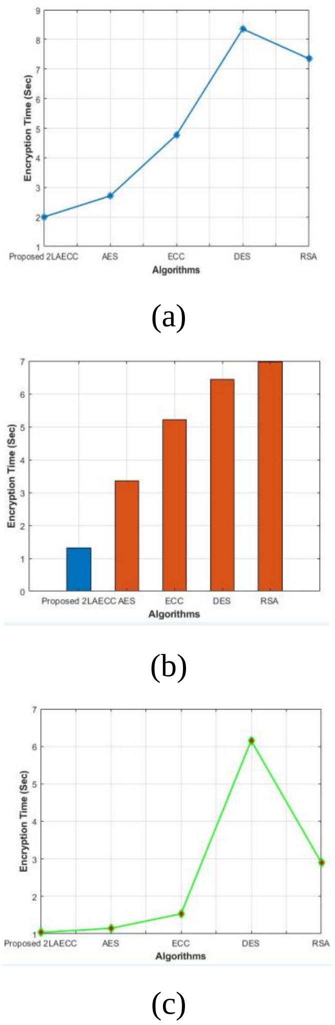
Dataset 1: The proposed 2LAECC model exhibited an Encryption Time of 1.9963, outperforming AES (2.7092), ECC (4.771), DES (8.354), and RSA (7.348). This improvement is attributed to the optimal key selection for encryption, supported by the efficient EBO convergence. Enhanced encryption ensures high data transmission security.

Dataset 2: The proposed 2LAECC model showcased an Encryption Time of 1.3208, surpassing AES (3.363), ECC (5.219), DES (6.435), and RSA (6.968). The optimal key selection and EBO convergence contributed to the faster encryption process, ensuring robust data security.

Dataset 3: The proposed 2LAECC model achieved an Encryption Time of 1.037, outperforming AES (1.146), ECC (1.533), DES (6.153), and RSA (2.897). The optimal key selection and EBO convergence accelerated encryption, reinforcing data security.

Table 1. Encryption of existing and Proposed methods

Dataset 1		Dataset 2		Dataset 3	
Methods	Encryption Time (Sec)	Methods	Encryption Time (Sec)	Methods	Encryption Time (Sec)
AES	2.7092	AES	3.363	AES	1.146
ECC	4.771	ECC	5.219	ECC	1.533
DES	8.354	DES	6.435	DES	6.153
RSA	7.348	RSA	6.968	RSA	2.897
2LAECC	1.9963	2LAECC	1.320	2LAECC	1.037



(a)

(b)

(c)

Figure 4: Graphical Representation of Encryption Time for (a) Dataset 1 (b) Dataset 2 (c) Dataset 3

7.3. Analysis of Decryption Time

Dataset 1:Decryption time assessment is presented in Table 2, revealing the outcomes. The proposed model achieved the shortest decryption time (0.8563), outperforming existing models due to its optimal key selection. Additionally, encrypting/decrypting only sensitive data contributes to reduced decryption time.

Dataset 2: Table 2 displays decryption time evaluation for Dataset 2, with the proposed model achieving the shortest time (2.095). Optimal key selection and encryption/decryption of sensitive data contribute to the proposed model's efficiency.

Dataset 3: Table 2 showcases decryption time assessment for Dataset 3, with the proposed model achieving the shortest time (1.057). Optimal key selection and encryption/decryption of sensitive data result in reduced decryption time compared to existing models.

Table 2. Decryption of existing and Proposed methods

Dataset 1		Dataset 2		Dataset 3	
Methods	Decryption Time (Sec)	Methods	Decryption Time (Sec)	Methods	Decryption Time (Sec)
AES	3.002	AES	3.772	AES	3.202
ECC	1.235	ECC	5.769	ECC	2.068

DES	7.993	DES	6.545	DES	8.006
RSA	8.147	RSA	6.434	RSA	7.044
2LAECC	0.856	2LAECC	2.095	2LAECC	1.057

7.4. Analysis of Security

Dataset 1: The main objective is to enhance data transfer security. The proposed model's security analysis is compared with existing models. Results show the planned model achieves the highest security level, making it more suitable for data transmission. The planned model's security level is 98.53%, surpassing AES=79%, ECC=85%, DES=73.9%, and RSA=70.94%. Security has been a significant challenge in existing works [1] [16] [18] [20] [23], but the projected model has excelled, establishing itself as superior. Therefore, the suggested model is the optimal choice for secure data transmission in BIoV. Figure 6 illustrates security graphically.

Dataset 2: Similar to Dataset 1, the primary aim is to enhance data transfer security. The proposed model's security analysis demonstrates it achieves the highest security level, surpassing AES=83.2%, ECC=88.4%, DES=70.3%, and RSA=73.5%. The projected model has effectively addressed security challenges present in existing works [1] [16] [18] [20] [23], solidifying its superiority. Thus, the proposed model is the most optimal approach for security. Figure 6 depicts security graphically, and Table 3 compares the security of Existing Methods and the Proposed.

Dataset 3: Again, the main focus is on elevating data transfer security. Results reveal the planned model attains the highest security level, surpassing AES=92.64%, ECC=91.64%, DES=85.64%, and RSA=87.36%. The projected model's success in overcoming security challenges in existing works [1] [16] [18] [20] [23] cements its prominence. Consequently, the suggested model stands out as the most optimal approach for secure data transmission in BIoV. Table 3 offers a comparison of security between Existing Methods and the Proposed.

Table 3. Security of existing and Proposed methods

Dataset 1		Dataset 2		Dataset 3	
Methods	Decryption Time (Sec)	Methods	Decryption Time (Sec)	Methods	Decryption Time (Sec)
Methods	Security (%)	Methods	Security (%)	Methods	Security (%)
AES	79	AES	83.2	AES	92.64
ECC	85	ECC	88.4	ECC	91.64
DES	73.9	DES	70.3	DES	85.64
RSA	70.94	RSA	73.54	RSA	87.36

7.5. Analysis of Trust score

Dataset 1:

The trust score is assessed, and the outcomes are screened in Table 4. As per the results, the suggested pattern has received trust score (4.5/5) for dataset 1. The suggested model has received the highest trust score (4.8/5) for dataset 2. The proposed model has received the trust score (4.7/5) for dataset 3. However, confidence score of existing pattern is lower. Confidence score's graphical depiction for datasets 1, 2, and 3 is described in Fig. 7.

Table 4. Trust score of existing and Proposed methods

Dataset 1		Dataset 2		Dataset 3	
Dataset 1	Dataset 2	Dataset 3	Dataset 1	Dataset 2	Dataset 3
Methods	Trust Score (out of 5)	Methods	Methods	Trust Score (out of 5)	Methods
AES	3.7	AES	AES	3.7	AES
ECC	3.72	ECC	ECC	3.72	ECC
DES	3	DES	DES	3	DES
RSA	3.01	RSA	RSA	3.01	RSA

7.6. Analysis of Throughput

Dataset 1: The throughput of the suggested model is assessed, and the resulting data are displayed in Table. 5. The suggested model (2LAECC) has recorded the throughput as 73.45%, which outperforms the current models of AES (65.45), ECC (58.48), DES (47.002), and RSA (41.86).

Dataset 2: The throughput of the suggested model is assessed, and the resulting data are displayed in Table. 5. The suggested model (2LAECC) has recorded the throughput as 77.57%, which outperforms the current models of AES (69.36), ECC (55.64), DES (49.35), and RSA (43.54).

Dataset 3: The throughput of the suggested model is assessed, and the resulting data are displayed in Table. 5. The suggested model (2LAECC) has recorded the throughput as 72.36%, which outperforms the current models of AES (61.58), ECC (53.64), DES (44.69), and RSA (39.94). The visual depiction of throughput for datasets 1, 2, and 3 is described in Fig. 8.

Table 5. Throughput of existing and Proposed methods

Dataset 1		**Dataset 2**		**Dataset 3**	
Methods	Throughput	Methods	Methods	Throughput	Methods
AES	65.45	AES	AES	65.45	AES
ECC	58.48	ECC	ECC	58.48	ECC
DES	47.002	DES	DES	47.002	DES
RSA	41.86	RSA	RSA	41.86	RSA
2LAECC	73.45	2LAECC	2LAECC	73.45	2LAECC

7.7. Analysis of Delivery Ratio

Dataset 1: The recommended model's delivery ratio is evaluated, and the outcomes are demonstrated in Table. 6. Suggested model's study of delivery ratio is assessed and contrasted with the models already in use. The anticipated model's delivery ratio of 0.988 is higher than that of AES (0.954), ECC (0.950), DES (0.900), and RSA (0.870).

Dataset 2: The proposed model's analysis of the delivery ratio is evaluated and compared to the existing models. Analyzing the obtained results reveals that the predicted model has the greatest delivery ratio, making it evident that it is considerably more appropriate for data transfer. The anticipated model's delivery ratio of 0.988 is higher than that of AES (0.954), ECC (0.950), DES (0.900), and RSA (0.870).

Dataset 3: The suggested model's study of the delivery ratio is assessed and contrasted with the models already in use. The anticipated model's delivery ratio of 0.988 is higher than that of AES (0.954), ECC (0.950), DES (0.900), and RSA (0.870). The graphical depiction of the delivery ratio for datasets 1, 2, and 3 is described in Fig. 9.

Table 6. Delivery Ratio of existing and Proposed methods

Dataset 1		**Dataset 2**		**Dataset 3**	
Methods	Delivery Ratio	Methods	Delivery Ratio	Methods	Delivery Ratio
AES	0.954	AES	0.964	AES	0.924
ECC	0.950	ECC	0.973	ECC	0.903
DES	0.900	DES	0.889	DES	0.853
RSA	0.870	RSA	0.891	RSA	0.974
2LAECC	0.988	2LAECC	0.998	2LAECC	0.981

8. Conclusion

This paper has developed a novel authentication model using a hybrid cryptographic algorithm to address the security issues present in BIoV. The suggested model has four steps: Data categorization, encryption, blockchain-based data transport, and user authentication. The collected user’s data has been categorized as sensitive as well as non-sensitive. Then, the sensitive data has been encrypted via the newly developed Two-Level Advanced Elliptic Curve Cryptosystems (2LAECC). In the 2LAECC model, the private key is generated optimally via the new Enriched Bat Optimizer (EBO). The non-sensitive data has not been sanitized. The encrypted sensitive data and the general data are transmitted via the blocks of the blockchain. At the receiver end, the receiver is verified before being given to the concerned party. Through the computation of dual-trust scores, the receiver is validated. The actual information is forwarded to the recipient only if it is determined that they are a trustworthy individual; otherwise, no information is sent to them. Finally, the metrics such as encryption time, decryption time, and security, are employed to assess how effective the given approach is. For dataset 1: the security level registered by planned pattern is 98.53%, it is better than AES=79%, ECC=85%, DES=73.9%, and RSA=70.94%. For dataset 2: security level registered by planned pattern is 98.3%, it is better than AES=83.2%, ECC=88.4%, DES=70.3%, and RSA=73.54%. For dataset 3: the security level registered by planned pattern is 99.02%, it is better than AES=92.64%, ECC=91.64%, DES=85.64%, and RSA=87.36%. Therefore, the projected model is suggested as the most optimal approach for secured data transmits in BIoV.

Author contributions

Girija V: Conceptualization, Methodology, Software, Field study Data curation, Writing-Original draft preparation, Software, Validation., Field study, Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Sharma, V., 2018. An energy-efficient transaction model for the blockchain-enabled Internet of Vehicles (IoV). IEEE Communications Letters, 23(2), pp.246-249.

[2] Zhao, Y., Wang, Y., Wang, P. and Yu, H., 2021. PBTM: A privacy-preserving announcement protocol with blockchain-based trust management for IoV. IEEE Systems Journal.

[3] Campanile, L., Iacono, M., Marulli, F. and Mastroianni, M., 2021. Designing a GDPR-compliant blockchain-based IoV distributed information tracking system. Information Processing & Management, 58(3), p.102511.

[4] Wang, X., Zeng, P., Patterson, N., Jiang, F. and Doss, R., 2019. An improved authentication scheme for the internet of vehicles based on blockchain technology. IEEE Access, 7, pp.45061-45072.

[5] Cheng, L., Liu, J., Xu, G., Zhang, Z., Wang, H., Dai, H.N., Wu, Y. and Wang, W., 2019. SCTSC: A semi-centralized traffic signal control mode with attribute-based blockchain in IoVs. IEEE Transactions on Computational Social Systems, 6(6), pp.1373-1385.

[6] Wang, Y., Tian, Y., Hei, X., Zhu, L. and Ji, W., 2021. A novel IoV block-streaming service awareness and trusted verification scheme in 6g. IEEE Transactions on Vehicular Technology, 70(6), pp.5197-5210.

[7] Singh, P.K., Singh, R., Nandi, S.K., Ghafoor, K.Z., Rawat, D.B. and Nandi, S., 2020. Blockchain-based adaptive trust management in internet of vehicles using smart contract. IEEE Transactions on Intelligent Transportation Systems, 22(6), pp.3616-3630.

[8] Elkhalil, A., Zhang, J. and Elhabob, R., 2021. An efficient heterogeneous blockchain-based online/offline signcryption systems for internet of vehicles. Cluster Computing, 24(3), pp.2051-2068.

[9] Chen, C., Wu, J., Lin, H., Chen, W. and Zheng, Z., 2019. A secure and efficient blockchain-based data trading approach for internet of vehicles. IEEE Transactions on Vehicular Technology, 68(9), pp.9110-9121.

[10] Xu, Z., Liang, W., Li, K.C., Xu, J. and Jin, H., 2021. A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles. Journal of Parallel and Distributed Computing, 149, pp.29-39.

[11] Eddine, M.S., Ferrag, M.A., Friha, O. and Maglaras, L., 2021. EASBF: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles. Journal of Information Security and Applications, 59, p.102802.

[12] Ma, Z., Wang, L. and Zhao, W., 2020. Blockchain-driven trusted data sharing with privacy protection in IoT sensor network. IEEE Sensors Journal, 21(22), pp.25472-25479.

[13] Gao, J., Agyekum, K.O.B.O., Sifah, E.B., Acheampong, K.N., Xia, Q., Du, X., Guizani, M. and Xia, H., 2019. A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks. IEEE Internet of Things Journal, 7(5), pp.4278-4291.

[14] Vangala, A., Bera, B., Saha, S., Das, A.K., Kumar, N. and Park, Y., 2020. Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems. IEEE Sensors Journal, 21(14), pp.15824-15838.

[15] Lin, H., Garg, S., Hu, J., Kaddoum, G., Peng, M. and Hossain, M.S., 2020. Blockchain and deep reinforcement learning empowered spatial crowdsourcing in software-defined internet of vehicles. IEEE Transactions on Intelligent Transportation Systems, 22(6), pp.3755-3764.

[16] Kang, J., Xiong, Z., Niyato, D., Ye, D., Kim, D.I. and Zhao, J., 2019. Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. IEEE Transactions on Vehicular Technology, 68(3), pp.2906-2920.

[17] Cui, L., Chen, Z., Yang, S., Ming, Z., Li, Q., Zhou, Y., Chen, S. and

Lu, Q., 2020. A blockchain-based containerized edge computing platform for the internet of vehicles. IEEE Internet of Things Journal, 8(4), pp.2395-2408.

[18] Chai, H., Leng, S., Chen, Y. and Zhang, K., 2020. A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles. IEEE Transactions on Intelligent Transportation Systems, 22(7), pp.3975-3986.

[19] Datset1, collected from "https://archive.ics.uci.edu/ml/datasets/Automobile ", 2022-08-30

[20] Datset2, collected from "https://github.com/IhabMoha/datasets-for-VANET ", 2022-08-30

[21] Datset3, collected from "https://github.com/IhabMoha/datasets-for-VANET ", 2022-08-30.