**BLOCKCHAIN-BASED AUTHENTICATION AND SECURITY FRAMEWORK FOR HEALTHCARE-IOT USING BD-DSA AND PTC**

**1S.KANAGASANKARIa**

***1Research Scholar, Registration No:*** *21111262282001* ***Department of Computer Science,***

*Sri Sarada College for Women (Autonomous),*

*Tirunelveli-627011*

*Affiliated to Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli-627012, Tamil Nadu, India*

 **2Dr. V.VALLINAYAGI**

***2*** *Head & Associate Professor,*

 *Department of Computer Science,*

*Sri Sarada College for Women (Autonomous),*

 *Tirunelveli-627011*

 *2**vallinayagimahesh@gmail.com*

*1kanagasankari1975@gmail.com*

**ABSTRACT**

The Internet of Things (IoT) in the healthcare (HC) industry has various advantages, including real-time data transmission (DT) and the capacity to track the patient's physiological state over a range of time intervals. It is necessary to put in place adequate security measures to prevent cyberattacks. Numerous authentication mechanisms have been developed recently, but the physical security of healthcare IoT (HC-IoT) devices against node replacement and node tampering attacks, in particular, has not received much attention. Therefore, this paper proposes a blockchain (BC) based sensor node authentication scheme with enhanced security for healthcare IoT systems using novel Binomial Distribution based Digital Signature Algorithm (BD-DSA) and Permutation based Tamilian Cryptography (PTC) models. The proposed work starts by implanting the number of sensor nodes (SNs) in the patient's body to monitor their physiological state. Next, node initialization takes place. Then, these SNs are registered with the blockchain server to prevent patients' privacy. After registration, login and authentication via BD-DSA are done to prevent node tampering and node replacement attacks. Once authentication is successful, secure path creation is carried out for efficient DT without data loss or attacks. The path selection can be made using Jeffrey's Divergence adopted K-Means Clustering (JDKMA) algorithm and Reverse Mutation Emperor Penguin Colony Optimization (RM\_EPCO) algorithm. After establishing a secure path, the sensed patients' sensitive HC data are PTC encrypted and transmitted to the cloud server (CS). In the end, the outcomes obtained by the proposed framework are compared with some existing models to show their efficacy. The outcomes revealed better performance and outperformed state-of-art methods.

***Keywords-****Healthcare IoT, Blockchain, Implantable Medical Devices, Data Security, Jeffrey’s Divergence (JD), Authentication, and Secure Data Transmission.*

**I. INTRODUCTION**

Medical care services have been one of the most critical issues for people and governments due to the increasing growth of human populations [1]. Thus, modern HC assumes its current form with the development of technology like the IoT and the Cloud. Medical applications now allow real-time health monitoring and status updates [2]. IoT consists of intelligent gadgets that can communicate and share information. IoT is being developed by various intelligent sensory components and wearable smart devices, which are essential in areas including HC, mining, agriculture, industries, buildings, cities, automated systems, and transportation [3]. When IoT and HC devices are combined, it promotes clinical status reporting for patients who need continuous internal surveillance and security measures [4]. Patients can get HC treatments (like physical examinations) in a variety of HC centers in various locations. The HC IoT equips patients with heterogeneous resource-limited HC devices (like implanted and wearable things) to collect their health data everywhere [5]. They are unobtrusive, user-friendly, and equipped with advanced features such as wireless DT, real-time feedback, and built-in alerting mechanisms. These devices can provide vital data to HC providers, such as blood pressure, glucose levels, and breathing patterns [6]. Because of the open nature of DT channels, the collected data is essential and should be kept private because it affects patients' health and lives [7].

Because of the unattended nature of system components and wireless communication, IoT-HC systems are enormously susceptible to various attacks. In addition, most IoT components have lower capacities regarding computing and resources, and these cannot support complex security schemes [8]. Thus, security is vital, as the patient's information is very much confidential from a legal and ethical standpoint. So, when developing IoT in medical domains, maximum attention must be paid to data security [9]. The data security model provides security to the medical data with the help of cryptographic approaches that ensure the data's validity, integrity, and authenticity. In contrast, in data privacy models, the data can be accessed only by those who are authorized by the model to view and use it [10]. Numerous methods have been proposed to achieve the robust performance of IoT systems [11]. To eliminate intermediate security breaches when sending and receiving medical information through IoT devices, various machine learning strategies, including unsupervised, supervised, reinforcement learning strategies, and communication protocols, are used [12]. However, it raises numerous security concerns, as unauthorized access could have disastrous consequences for a patient. BC is a new technology that enables efficient and transparent communication among system-communicating entities [13].

It provides the foundation for building a dependable, secure, and efficient IoT infrastructure. BC technology can be used in the IoT information-sharing component. It enables the secure sharing of vital information captured by IoT devices [14, 15]. As a result, BC adoption has the potential to provide promising solutions that facilitate HC delivery and therefore develop the HC industry [16]. Various authentication protocols have been developed to protect privacy and security. However, a lack of security can have disastrous consequences such as data loss and theft. Many intruders seek an unsecured channel to access valuable HC data in the cloud network [17]. Therefore, the proposed work develops an efficientBC-based authentication and security framework in HC-IoT using BD-DSA and PTC. The research objectives of the proposed BC-based authentication and security system are enlisted as follows,

* A BD-DSA-based model is proposed using BC technology to perform efficient sensor node authentication for protecting the data.
* To secure the data from node tampering and node replacement attacks, secure path creation utilizing JDKMA and RM\_EPCO algorithms are proposed.
* A cryptographic encryption model named PTC is proposed to encrypt the sensed patient-sensitive information to transmit them to the cloud storage.
* All transactions, node details, and sensitive information are stored securely in the BC server.

The rest of the paper is structured as follows: Section 2 depicts the literature survey about the proposed framework, Section 3 reveals the detailed analysis of the proposed framework, Section 4 presents the results and discussions of the proposed methodology, and Section 5 concludes the paper with future scope.

**II. LITERATURE SURVEY**

**Xu Cheng et al.** [18] presented a BC-based Medical Cyber-Physical System (MCPS) that described the security requirements in the authentication process of medical data users. The author used intractable problems and bilinear mapping to solve the security threats during the authentication process. The model enabled medical data sharing and met several security needs during user authentication. **Pandi Vijayakumar et al. [19]**suggested an anonymous authentication framework for IoT-based Wireless Body Area Networks (WBANs) with location privacy preservation. The doctor and the patient were authenticated by each other anonymously to ensure their legitimacy. Furthermore, the Trusted Authority (TA) protected the location of the patient and the doctor. The analysis revealed that the scheme outperformed the previous schemes regarding security and computation costs during anonymous authentication. **Jafar A. Alzubi [20]**recommended a BC-based model for medical IoT devices that employed the Lamport Merkle Digital Signature (LMDS). The LMDS model constructed a tree to perform authentication of the IoT devices. A Centralized Healthcare Controller (CHC) used Lamport Merkle Digital Signature Verification (LMDSV) to determine the source of the LMDSG. The LMDS provided greater security for medical IoT devices with lesser computation time and overhead. **Muhammad Tahir et al.** [21] used a probabilistic model that created an authentication and authorization framework for BC-enabled IoT networks. The framework employed random numbers in the authentication process that was linked via joint conditional probability. Thus, it established a secure connection among IoT devices for future data collection. The framework provided robust and mutual authenticity, improved access control, and reduced communication and computational overhead costs. **Seunghwan Son et al.** [22] suggested a BC-based authentication mechanism for Telecare medical information system (TMIS). The study used ciphertext policy attribute-based encryption (CP-ABE) that controlled the access of HC data stored on the CS and BC. The model provided more security and efficiency than related protocols.

Fore-healthsecurity**, Xinyin Xiang et al.** [23] designed a permissioned BC-based identity management and user authentication (PBBIMUA) model. Each e-health user had a distributed ledger, and the transactions of the model encouraged smart contract registration. The smart contracts maintained the public key records for efficient identity and used the user's biometrics as a key distribution strategy. The system used a smart contract to support anonymous authentication of the users. The results revealed that the system was more efficient than known methods. To provide security to the Internet of Medical Things (IoMT), **Randhir Kumar and Rakesh Tripathi** [24] used BC and interplanetary file systems (IPFS) technology. The model grouped the nodes into a cluster form and used smart contracts for authenticating patients and medical devices. After authentication, the cluster layer stored the device-generated information, which was transmitted securely to the consortium BC. The BC-based mechanism for data storage provided data privacy because it used a hash-based storage mechanism. **Kristen N. Griggs et al.** [25] presented BC-based smart contracts to offer secure medical sensor management and analysis. The private BC constructed a system with the help of the Ethereum protocol. The SNs were communicated with smart contracts that maintained the records of all events of the SNs on the BC. The approach allowed real-time patient monitoring and medical interventions by sending notifications to HC patients and medical professionals. **Lijun Xiao and colleagues** [26] developed a secure framework for private BC-based WBANs. The model generated two groups of private BCs to store SN registration data and patient physiological data. The storage of the registration and physiological data in private BC reduced the complexity of regional data management. On this basis, the system generated a BC network's blind signature. The results demonstrated that the developed scheme was more advanced and effective than existing models.

**Geetanjali Rathee *et al.***[27] used BC technology to support multimedia data processing in IoT-HC. The model stored every activity of the IoT devices inside the BC, providing secrecy and transparency to the patients and intermediates. The model also traced the activity of the intermediates in DT. **Asad Abbas *et al.*** [28] suggested a BC-assisted secure data management framework (BSDMF) for IMoT. The BSDMF provided secure DT between implantable medical devices and personal servers and between cloud servers and personal servers. The approach ensured secure DT and data management between the linked nodes in IMoT. **Rajakumar Arul** ***et al.*** [29] designed the Multi-Modal Secure Data Dissemination Framework (MMSDDF) to provide secure data access and control in the IoMT. The patient’s data were transmitted to the BC, which authenticated each patient in the network. If any third party accessed the BC during data exchange, the BC alerted the patient and the IoMT-HC system. The results demonstrated that the MMSDDF method outperformed other existing methods in accuracy.

Privacy is a significant issue in IoT due to the massive medical sensor data. However, unauthorized access to messages transferred between system nodes is the primary weakness in the above-mentioned existing techniques, and unauthorized access to SNs may result in inconsistent or fabricated medical reports. Simple security methods are ineffective, and attackers can target sensor data to modify it and inject attacks. There is a chance that the system will be hacked, and patient data will be misused. As a result, providing security in communication sessions between IoT devices becomes the most critical and challenging task, as it must account for the vulnerability to intruder attacks. The shortcomings in some of the existing techniques like unauthorized access to SNs, unauthorized access to messages transferred between system nodes, attacks on wearable sensors, hacking patient data, and misusing them are overcome in this work by proposing an efficientBC -centered authentication and security framework in HC -IoT using BD-DSA and PTC. The proposed work uses the BD-DSA-based sensor node authentication technique to prevent unauthorized access to SNs. Also, JDKMA and RM\_EPCO-based secure path is created between SNs to protect the transfer of medical data between unauthorized system nodes. PTC is adopted in this work to encrypt the data more securely to prevent it from alterations from intruders. Finally, BC technology plays a significant role in the proposed framework, which protects patients' HC data privacy.

**III. PROPOSED METHODOLOGY**

The modern HC industry uses smart IoT-enabled medical devices to monitor, collect and transmit biomedical data such as blood pressure, blood sugar levels, electrocardiography (ECG), body temperature, etc. The medical data sensed by the smart devices are sent to nearby gateways and remote servers for processing and visualization. Because the data is sensitive, it must provide a secure data exchange to protect against various security attacks. This paper builds an efficientBC-centered authentication and security framework in HC-IoT using BD-DSA and PTC techniques. The proposed work consists of the following steps: Patient with IoT sensors, Sensor node registration, login, Authentication with BD-DSA, secure path creation by clustering SNs using JDKMA, optimizing the paths via RM\_EPCO algorithms, data encryption by PTC, and at last, the data is securely stored in the BC. The block diagram of the proposed framework is cited below in Figure 1.



**Figure 1:** Block diagram of the proposed model

**3.1 Sensor Node Initialization**

At the start,  number of SNs (temperature sensor, heart-rate monitoring sensor, glucose monitoring sensor, etc.) is implanted in the patient's body to monitor the physiological health condition of the patient are. Primarily, these nodes are initialized with the BC server by creating blocks to record transactions and store sensor data securely. The number of SNs entrenched in the patient’s body is expressed as,

 (1)

**3.2 Node Registration**

After initializing the SNs, before data sensing each node registers its details with the blockchain server. Since the details are stored in the BC, it prevents the privacy and unauthorized access of SNs. Here, the SNs use their node ID (), node type (), node location (), etc. for registration. On registration of SNs, a digital signature is created using the BD-DSA algorithm.

**3.3 Signature creation and authentication using BD-DSA**

Here, a digital signature (DS) is created for each SN concerning the node details such as, for authentication. A DS includes three processes. Initially, the key generation process was carried out that generates the private key randomly from a set of possible private, and the model outputs both private and public keys. Secondly, a signing process produces a signature, and thirdly signature verification process verifies the signature by accepting or rejecting the message's claim to authenticity. One disadvantage of DSA is that the prime divisor for signature creation and verification is generated randomly, affecting the model's overall performance. To solve this issue, Binomial Distribution (BD) is adopted to generate the prime divisor. Hence, the proposed one is called BD-DSA. The signature generation process for SNs is detailed below,

***a. Key generation***

* A prime number  is chosen first called the prime divisor using the binomial distribution function  given by,

 (2)

 Where,  refers to the probability of success and failure on a single trial, represents a number of times with a specific outcome, and  mentions the number of trials. Another prime number is also selected such that,

 (3)

* After that, an integer  is selected that satisfies the following conditions,

 (4)

 (5)

* Then, the private key is generated as and the public key becomes  which is computed as,

 (6)

**b. Signature generation**

* For generating the digital signature, node details, , and  are given as input and converted into the hash function  using the following equation (7),

 (7)

* Next, the hash value is transmitted as input to the signing function which produces the result as , calculated as,

 (8)

 (9)

 In the aforesaid equation, signifies the random number and models the digital signature.

**c. Signature verification**

* During hash verification, the same hash function is used to generate the hash digest, and then it is passed into the verification function by computing the variable  such that,

 (10)

* Then the values of are estimated as,

 (11)

 (12)

* At last, the signature verification  component is evaluated by,

 (13)

 Here,  is compared with the received in the bundle, if both matches, the verification becomes successful and the sensor node starts sensing the data.

**3.4 Secure path creation**

In this phase, the secure paths are created by clustering the entrenched SNs using JDKMA and then optimizing the paths via RM\_EPCO algorithms. Through the generated optimal paths, the sensed HC data are transmitted to the BC server without any attack on the data. This way of establishing the paths secures the HC IoT data against node tampering and node replacement attacks.

**3.4.1 Clustering by JDKMA**

K-means algorithm is one of the simplest, non-supervised partitioning clustering algorithms which divides the given data object into different clusters through the iterative, converging to a local minimum. In KMA, at first, the centroid points are calculated, and then it takes each point to the cluster with the nearest centroid from the adjacent data point. The Euclidean distance-based similarity measure is used to assign each data point to its nearby centroid. The similarity measure has been one of the essential factors in clustering for discovering the natural grouping of a given dataset by identifying hidden patterns. However, the Euclidean distance calculation is quite complex and is not appropriate for handling the complicated and non-Euclidean structure of the input data. To overcome this downside, in the proposed work Jeffrey-Divergence (JD) based similarity measure is used instead of the original Euclidean norm because the divergence function implicitly results in handling complicated and non-Euclidean data structures. Due to this modification, the proposed KMA is named JDKMA. The clustering process using JDKMA is discussed further,

* Consider,  be the number of SNs which is clustered into the number of clusters , and  be the initial cluster centroids generated randomly.
* Then, the JD between each data point  and the initial cluster centroids is calculated to allocate each  to its closest . The JD calculation is mathematically formulated below,

 (14)

* The criterion function is calculated by taking the mean of all the clusters of the target object. This can be defined as follows,

 (15)

Where, indicates the average of clusters. Finally, the number of clusters (grouped SNs) based on the distance is notated as,

 (16)

From the above-grouped nodes, optimal paths are established using the RM\_EPCO algorithm.

**3.4.2 Optimizing the paths via RM\_EPCO**

Emperor Penguin Optimizer (EPO) is a popular metaheuristic model that mimics emperor penguins' huddling behaviour (EPs). The huddling procedure is answerable for better diversification, contributing to the EPO's superior global search capability. EPs live on open ice and breed during the winter months. During the breeding season, EPs congregate in massive colonies that number in the hundreds of thousands. The only species that huddles to survive the Antarctic winter is the Emperor penguin (EP). The huddling behaviour of EPs is divided into four stages: generate and determine the EP huddle boundary, calculate the temperature profile around the huddle, Determine the distance between EPs and reposition the effective mover. The EPO's successful moving actions provide better intensification, which enhances the EPO's superior local search ability. It provides a smooth transition from diversification to intensification (or global search) (or local search). However, the standard EPO suffers from premature convergence when solving complex optimization problems and tends to fall into local optima. Therefore, the proper balance between exploration and exploitation stages is needed to ensure the approximation of globally optimum values. Hence the Reverse Mutation (RM) process is used to prevent premature convergence and falling into a locally optimal solution. As a result, the convention EPO becomesRM\_EPCO. The step-by-step process is explained further,

**Step 1:** Initially, EPs randomly construct the huddle boundary (clustered SNs). The wind is determined to find the huddle boundary around a polygon as it flows around the huddle. The wind, on the other hand, moves faster than an EP. The concept of complex variables is used to describe an EP's randomly generated huddle boundary. Let, denote as the velocity of the wind and as its gradient, then

 (17)

 The vector  is joined with wind velocity to generate complex potential,

 (18)

 Where,  stands for the imaginary constant, and  determines the polygon plane’s analytical function. Then, the fitness of each EP is calculated to identify the best solution.

**Step 2:** To conserve energy and maximize the ambient temperature in the huddle, emperor penguins form a huddle.This can be mathematically modeled by considering the temperature when the polygon radius  and, when. This temperature profile is in charge of the exploration and exploitation of emperor penguins in various locations. The temperature profile around the huddle is evaluated by,

 (19)

 (20)

 Where,  denotes the current iteration and maximum iteration respectively.

**Step 3:** After the construction of the huddle boundary,computethedistance between EP and the best obtained optimal solution. The current best optimal solution is the one with the closest fitness value to the optimum. The other search agents (or EPs) will adjust their positions based on the current best optimal solution, which is defined mathematically as follows:

 (21)

 Here,  denotes fittest optimal penguin,  are the vectors that avoids the collision between neighbors, models the penguin's social forces responsible for movement towards the best solution, and symbolizes the position vector of the EP. The vectors  are estimated in below equations,

 (22)

 (23)

 (24)

 In the aforesaid equations, mentions the movement parameter that avoids collisions by mapping the gap between search agents,  denotes the polygon grid accuracy that compares the difference between the EPs, and  determines the random number between 0 and 1. The social forces responsible for movement towards the best optimal solution is computed in equation (25),

 (25)

 In this equation,  specifies the expression function, are the control parameters to have better exploitation and exploration.

**Step 4:** Finally, update the positions of the EP according to the best obtained optimal position (mover). This mover is in charge of changing the positions of other search agents in a given search space, as well as leaving its current position. In the proposed work, position updation is carried out using a reverse mutation process.

* In the reverse mutation process, initially, the initial permutation takes plain text (EPs position) as an input. Then reversion happens in which the original base pair sequence may be restored. Therefore, the output will be the mutated position. These steps are repeated until is updated or the number of iteration is reached. The position updation equation for EPO is expressed as,

 (26)

 Where, denotes the EP’s newly updated position. The huddling behavior of EPs is recomputed during the iteration process once the mover has been re-located. In this way, the optimal paths  from the clustered SNs are created for secure DT. The pseudocode of the proposed RM\_EPCO is revealed further,



**Figure 2:** Pseudocode of proposed RM\_EPCO

**3.5 Data Security by PTC**

The next step in the proposed work is data security. In this phase, the sensed patient medical data undergoes encryption for secure transmission. Tamilian Cryptography (TC) is one of the most widely used encryption models that encrypts the messages using natural language, which reduces encryption time and improves performance. TC is divided into three phases: translation, mapping, and encryption, and it makes data much more secure than existing techniques. TC initially translated the input data into Tamil and then mapped the data to an arbitrarily created 2-bit combination of English alphabets. This process results are named intermediate cipher (inter cipher). After finishing the translation and mapping processes, the inter cipher (IC) is encrypted using the Advanced Encryption Standard (AES) to enhance the data confidentiality. AES is a symmetric cipher model that employs the same key for both encryption and decryption. Substitution Bytes (SB), Shift Rows (SR), Mix Columns (MC), and AddRoundKey (ARK) are the four primary operations. Every message block in AES is encrypted using the four operations listed above, which increases the model's time complexity. To overcome this problem and encrypt the message in sufficient time, the proposed work replaces the mix columns transformation of the conventional AES with permutation-based column shifts, which reduces time complexity and also increases security. This permutation-based column shits in the encryption operation of TC is named PTC. Let, be the input sensor message that needs to be encrypted using the proposed PTC technique. The steps followed by the PTC are as follows

***Translation***

Primarily, the plan text (input message) is translated into the Tamil language  by using a Google application programming interface translator. For translating the numerical message, the number is converted into words, and then it is converted into a Tamil word. A language translator converts a text written in one language into another. It is a very useful tool for understanding text written in an unknown language. Thus, the translated message is modeled below,

 (27)

***Mapping***

Next to translation, each Tamil alphabet is mapped into two 32-bit English alphabet combinations to attain an IC. Each occurrence of a letter does not have the same mapping; for each Tamil alphabet, there are two 2-bit combinations; every occurrence may have one of the two 2-bit combinations. To make the algorithm effective, this 2-bit combination of alphabets is chosen using a logistic chaotic mapping function. By doing so, it is very difficult for the attackers to retrieve the data from the translated message. Logistic chaotic mapping  for selecting the 2-bit combination of English alphabets becomes,

 (28)

 Where,  denotes the iteration number, and is a chaotic constant. Thus, the intermediate cipher (translated message) becomes,

 (29)

**Encryption with AES**

In this phase, the intermediate cipher is encrypted by generating a random round key. Afterward, the input intermediate cipher is XOR-ed with  to generate the cipher transformation. It is mathematically formulated by,

 (30)

Where,  represents the transformation of the cipher key. Then, using an S-box, substitute byte transformation replaces every data block byte with another block. Following that, each row of the state matrix is given a cyclic shift to the right side based on its location. The first row is left alone. Each byte in the second row is shifted to the left by one position. The third and fourth rows are also shifted two and three positions, respectively. As a result, each output block of this step will be made up of bytes from four input block columns.

 A permutation is used in this work instead of a mixed column. Permutation, also known as P-box, is a bit-shuffling model that transposes bits across S-box inputs. This operation is based on column shifts, which occur on different cyclic columns with different offsets, allowing for suitable state permutations. Finally, ARK is executed, which moves one column at a time. ARK gives each column matrix a round keyword. The ARK stage performs matrix addition operations. SBs, SR, Permutation, and ARK are performed in all rounds of encryption except the last. In addition to the rounds of Inverse SR, Inverse SB, Inverse ARK, and Inverse Permutation Transformation, the decryption operation follows the same process as the encryption operation. An inverse permutation is no longer performed in the final round.

**3.6 BLOCKCHAIN**

Finally, the encrypted data is stored in a BC for further security. BC is a decentralized, shared, and public digital ledger used for storing transactions in various modes. A BC typically consists of two components: transactions, the events performed by system members, and blocks, which record the transactions and ensure their unaltered arrangement. Furthermore, it must be a stable, scalable platform where previous records cannot be altered. When a new transaction is added to the chain, it must be validated by all network participants. The collection of blocks in the BC contains four components: transaction details, the hash value of the existing block, the hash value of a recent block, and a timestamp. As a result, an intruder cannot modify any records of BC because each block is made up of a cryptographic value from the previous block. The blocks in the BC are made up of the block header and the block body. The block header includes the hash value created by the Secure Hash Algorithm (SHA-256), the previous hash, and the current hash, merkle tree (stores group of transactions in each block), nonce (a number generated by proof of work operations on miner nodes to produce a hash value less than a target difficulty level), and timestamp. As a result, a BC functions as a secure and distributed ledger that effectively, persistently, and verifiably archives all transactions between any two parties in an open networked system. Figure 3 illustrates the BC structure.

****

**Figure 3:** Structure of BC

**IV. RESULTS AND DISCUSSION**

Here, the performance of the presented BC-based authentication and security framework for HC-IoT devices is compared with conventional techniques to assess the efficacy of the proposed research model. The proposed work is implemented in the PYTHON working platform. Authentication, secure path creation, and data security are major techniques developed in the proposed framework to improve the security of medical data. As a result, a novel BD-DSA and PTC are used. This paper takes into account 150 patients in order to retain HC data. The simulation parameters of the current research model are tabulated in table 1. The performance of these techniques is detailed as follows.

**Table 1:** Simulation parameters

|  |  |
| --- | --- |
| **Parameters** | **Values** |
| Simulation area | 650 m \* 650 m  |
| Total number of IoT devices | 150 |
| Total number of patients | 150 |
| Transmission of IoT devices | 25m |
| Response time | 2 – 5 s |
| Simulation time | 150s |
| Transactions | 1000 per round |

**4.1 Performance Assessment of the Proposed Framework**

The experimental outcomes of the proposed research framework are contrasted with some of the existing models in the literature, namely, LMDS [20], Linear [21], BSDMF [28], and MMSDDF [29]. The comparison is made in terms of performance metrics such as Communication time (CT), communication overhead (CO), security level (SL), authentication time (AT), authentication accuracy (AA), and data confidentiality rate (DCR). The superiority measurements are made further,



**Figure 4:** Communication Time

The CT achieved by the proposed and existing techniques is depicted in Figure 4. The graphical analysis demonstrates that the proposed work achieved lower CT compared to existing techniques. The CT varies according to the number of patients. The amount of time spent communicating is defined as CT. It also refers to the time spent on signature generation and verification.The lower time shows the better performance of the techniques. With this view, for the minimum number of patients, i.e. for 30 patients, the CT achieved by the proposed work is 2282ms. The existing LMDS, Linear, BSDMF, and MMSDDF achieve higher CT, 2874ms, 3285ms, 3784ms, and 4236ms, respectively, for the same 30 patients. For the maximum number of patients considered here, i.e., 150 patients, the proposed work provides a CT of 5272ms. Similarly, the proposed technique provides lower CT for the other counts of patients (60, 90, and 120) compared to others. Therefore, it is assumed that the proposed work is better than the existing methodologies.



**Figure 5:** Analysis of communication overhead

The overhead incurred during communication is referred to as communication overhead (CO). CO is calculated based on the memory used during signature generation and the memory used at the time of signature verification. Figure 5 depicts the CO performance analysis of proposed and existing methods for various patient populations. The CO of the models are plotted in fig. 5. The proposed model attains the COs of 12KB, 14KB, 19KB, 23KB, and 27KB for the patient counts 30, 60, 90, 120, and 150. The existing models obtain the highest CO compared to the proposed work.

**Table 2:** Security strength assessment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Techniques/ Performance Evaluation** | **30** | **60** | **90** | **120** | **150** |
| **LMDS** | 87.32 | 86.57 | 87.12 | 86.54 | 87.32 |
| **Linear** | 89.65 | 89.75 | 90.32 | 89.74 | 89.65 |
| **BSDMF** | 91.32458 | 91.32 | 92.45 | 91.23 | 91.78 |
| **MMSDDF** | 93.81 | 93.25 | 94.23 | 93.45 | 93.45 |
| **Proposed** | 95.89 | 95.23 | 96.23 | 95.78 | 96.32 |

Table 2 compares the results of security level of the proposed and existing models. The higher value of security level shows the better performance of the models. When the number of patients is 150, the security strength of the proposed work is 96.32%, while the existing methods such as MMSDDF, BSDMF, Linear, and, LMDS achieve the security level of 93.45%, 91.78%, 89.65%, and 87.32% for the same 150 patients. Correspondingly, when the number of patients is 60, the proposed method shows higher security of 95.23%. Nevertheless, the conventional methods say MMSDDF, BSDMF, Linear, and, LMDS attains the security level of 93.25%, 91.32%, 89.75%, and 86.57%. Therefore, in this, it is clear that the proposed technique presents a higher security level compared to other state of art approaches.



**Figure 6:** Authentication Time

 The time taken by the models for authenticating the IoT devices is plotted in figure 6. When the number of SNs increases, the authentication time of the models also increases. For a maximum number of nodes (150), the authentication time attained by the proposed research framework is 2375ms. In contrast, the existing schemes such as LMDS, Linear, BSDMF, and MMSDDF attains authentication time of 4215ms, 3862ms, 3175ms, and 2651ms which are lower than the current model. Similarly, for all counts of nodes, the proposed approach attains the lowest time for authenticating the HC-IoT devices.

**Table 3:** Authentication accuracy (AA) and data confidentiality rate (DCR)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Techniques/ Performance Evaluation** | **30** | **60** | **90** | **120** | **150** |
| AA **(%)** | **DCR(%)** | AA**(%)** | **DCR(%)** | AA**(%)** | **DCR(%)** | AA **(%)** | **DCR (%)** | AA **(%)** | **DCR(%)** |
| **LMDS** | 87.89 | 86.63 | 87.32 | 87.62 | 88.22 | 86.24 | 87.65 | 87.22 | 88.12 | 87.14 |
| **Linear** | 89.84 | 89.63 | 89.87 | 89.21 | 90.32 | 88.62 | 90.31 | 89.54 | 89.63 | 89.74 |
| **BSDMF** | 91.32 | 92.56 | 91.78 | 91.564 | 92.66 | 92.11 | 91.87 | 91.65 | 92.63 | 91.45 |
| **MMSDDF** | 93.54 | 94.23 | 93.85 | 93.45 | 93.45 | 94.56 | 94.14 | 93.84 | 94.35 | 94.65 |
| **Proposed** | 95.23 | 96.78 | 96.32 | 95.74 | 95.48 | 96.37 | 96.85 | 96.89 | 95.78 | 96.32 |

 Table 3 compares the AA and DCR of the proposed and existing frameworks. The AA is the ratio of the number of SNs authenticated correctly to the total count of SNs. DCR refers to the number of medical data securely transmitted over the SNs. The results show that both the AA and DCR obtained by the proposed work are high compared to other existing approaches. That is, for 90 SNs, the proposed framework attains the AA of 94.48% and DCR of 96.37%. On the other hand, the existing MMSDDF attains the AA of 93.45% and DCR of 94.56% for the exact count of 90 SNs, which is very low compared to the proposed model. Similarly, when comparing the AA and DCR of the other existing techniques with the presented approach, the current model achieves the best performance by achieving higher values for both AA and DCR, which shows the efficacy of the proposed model for HC-IoT data security.

**V. CONCLUSION**

This paper proposes an efficient BC-based authentication and security framework for HC-IoT devices with the help of BD-DSA and PTC techniques. The proposed model’s performance is contrasted with the existing techniques to inspect the efficiency of the proposed method. The study uses the following performance metrics to analyze the performance of the models: communication time, communication overhead, authentication time, authentication accuracy, security strength, and data confidentiality rate. The proposed technique achieves higher authentication accuracy of 95.48%, confidentiality rate of 96.37%, lower authentication time of 2375ms, communication time of 2282ms, and security strength of 96.32%. Considering these metrics, it is evident that the proposed method obtains effective results and accomplishes efficient data security in the HC system. In future, the work will be extended by using advanced techniques for attack detection of HC data.

**VI.REFERENCES**

1. Guangyu Xu, “IoT-Assisted ECG Monitoring Framework with Secure Data Transmission for Health Care Applications”, IEEE Access, vol. 8, pp. 74586–74594, 2020, doi:10.1109/ACCESS.2020.2988059.
2. Shuchi Juyal; Sharma, Sachin; Harbola, Aditya; Shukla, Amal Shankar, “Privacy and Security of IoT based Skin Monitoring System using Blockchain Approach”, IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), pp. 1–5, 2020, doi:10.1109/CONECCT50063.2020.9198409.
3. Ata Ullah, Muhammad Azeem;Humaira Ashraf;Abdulellah A. Alaboudi;Mamoona Humayun;NZ Jhanjhi, “Secure Healthcare Data Aggregation and Transmission in IoT—A Survey”, IEEE Access, 2021, doi:10.1109/access.2021.3052850.
4. Taher M. Ghazal, “Internet of Things with Artificial Intelligence for Health Care Security. Arabian Journal for Science and Engineering”, 2021, doi: 10.1007/s13369-021-06083-8.
5. Wenjuan Tang; Ren, Ju; Deng, Kun; Zhang, Yaoxue, “Secure Data Aggregation of Lightweight E-healthcare IoT Devices with Fair Incentives”, IEEE Internet of Things Journal, pp. 1–1, 2019, doi:10.1109/JIOT.2019.2923261.
6. Ashutosh Dwivedi, Srivastava, Gautam; Dhar, Shalini; Singh, Rajani, “A Decentralized Privacy-Preserving Healthcare Blockchain for IoT”, Sensors, vol. 19, no. 2, pp. 326, doi: 10.3390/s19020326.
7. Bayat Fotouhi M, M., Das, A. K., Far, H. A. N., Pournaghi, S. M., & Doostari, M. A., “A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. Computer Networks”, vol. 177, pp. 107333, doi:10.1016/j.comnet.2020.10733.
8. Faris A. Almalki and Ben Othman Soufiene, “EPPDA: An Efficient and Privacy-Preserving Data Aggregation Scheme with Authentication and Authorization for IoT-Based Healthcare Applications”, Wireless Communications and Mobile Computing, 2021, <https://doi.org/10.1155/2021/5594159>.
9. Gia Nhu Nguyen;Nin Ho Le Viet;Mohamed Elhoseny;K. Shankar;B.B. Gupta;Ahmed A. Abd El-Latif; (2021). Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model . Journal of Parallel and Distributed Computing, (), –. doi:10.1016/j.jpdc.2021.03.011.
10. Wencheng Sun; Cai, Zhiping; Li, Yangyang; Liu, Fang; Fang, Shengqun; Wang, Guoyan, “Security and Privacy in the Medical Internet of Things: A Review”, Security and Communication Networks, pp. 1–9, 2018, doi:10.1155/2018/5978636.
11. Mrinai M Dhanvijay; Patil, Shailaja C., “Internet of Things: A Survey of Enabling Technologies in Healthcare and its Applications”, Computer Networks, 2019, doi:10.1016/j.comnet.2019.03.006.
12. Mohamed Shakeel, P.; Baskar, S.; Sarma Dhulipala, V. R.; Mishra, Sukumar; Jaber, Mustafa Musa, “Maintaining Security and Privacy in Health Care System Using Learning Based Deep-Q-Networks”, Journal of Medical Systems, vol. 42, no. 10, pp. 186, 2018, doi:10.1007/s10916-018-1045-z.
13. Sourav Saha; Sutrala, Anil Kumar; Das, Ashok Kumar; Kumar, Neeraj; Rodrigues, Joel J. P. C, “On the Design of Blockchain-Based Access Control Protocol for IoT-Enabled Healthcare Applications”, IEEE International Conference on Communications (ICC), pp. 1–6, 2020, doi:10.1109/ICC40277.2020.914891.
14. Abou-Nassar, Eman M; Iliyasu, Abdullah M.; El-Kafrawy, Passent M; Song, Oh-Young; Bashir, Ali Kashif; El-Latif, Ahmed A. Abd (2020). DITrust Chain, “Towards Blockchain-based Trust Models for Sustainable Healthcare IoT Systems”, IEEE Access, pp. 1–1, 2020, doi:10.1109/ACCESS.2020.2999468.
15. Ahmed Farouk; Alahmadi, Amal; Ghose, Shohini; Mashatan, Atefeh, “Blockchain platform for industrial healthcare: Vision and future opportunities”, Computer Communications, 2020, doi:10.1016/j.comcom.2020.02.058.
16. Dinh C. Nguyen; Pathirana, Pubudu N.; Ding, Ming; Seneviratne, Aruna, “Blockchain for Secure EHRs Sharing of Mobile Cloud based E-health Systems”, IEEE Access, pp. 1–1, 2019, doi:10.1109/ACCESS.2019.2917555.
17. Abdullah Al Omar, Bhuiyan, Md Zakirul Alam; Basu, Anirban; Kiyomoto, Shinsaku; Rahman, Mohammad Shahriar, “Privacy-friendly platform for healthcare data in cloud based on blockchain environment”, Future Generation Computer Systems, 2019, doi:10.1016/j.future.2018.12.044.
18. Abdullah Al Omar, Bhuiyan, Md Zakirul Alam; Basu, Anirban; Kiyomoto, Shinsaku; Rahman, Mohammad Shahriar, “Privacy-friendly platform for healthcare data in cloud based on blockchain environment”, Future Generation Computer Systems, 2019, doi:10.1016/j.future.2018.12.044.
19. Xu Cheng; Chen, Fulong; Xie, Dong; Sun, Hui; Huang, Cheng, “Design of a Secure Medical Data Sharing Scheme Based on Blockchain”, Journal of Medical Systems, vol. 44, no. 2, 2020, doi:10.1007/s10916-019-1468-1.
20. Vijayakumar P; Obaidat, Mohammad; Azees, Maria; Islam, Sk Hafizul; Kumar, Neeraj, “Efficient and Secure Anonymous Authentication with Location Privacy for IoT-based WBANs”, IEEE Transactions on Industrial Informatics, 2019, doi:10.1109/TII.2019.2925071.
21. Muhammad Tahir; Sardaraz, Muhammad; Muhammad, Shakoor; Saud Khan, Muhammad, “A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics”, Sustainability, vol. 12, no. 17, 2020, doi: 10.3390/su12176960.
22. Seunghwan Son; Lee, Joonyoung; Kim, Myeonghyun; Yu, Sungjin; Das, Ashok Kumar; Park, Youngho, “Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain”, IEEE Access, vol. 8, pp. 192177–192191, 2020, doi:10.1109/access.2020.3032680.
23. Xinyin Xiang; Wang, Mingyu; Fan, Weiguo, “A Permissioned Blockchain-based Identity Management and User Authentication Scheme for E-health Systems”, IEEE Access, 2020, doi:10.1109/access.2020.3022429.
24. Randhir Kumar; Rakesh Tripathi, “Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology”, The Journal of Supercomputing, 2021, doi:10.1007/s11227-020-03570-x.
25. Kristen N. Griggs; Ossipova, Olya; Kohlios, Christopher P.; Baccarini, Alessandro N.; Howson, Emily A.; Hayajneh, Thaier, “Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring”, Journal of Medical Systems, vol. 42, no. 7, 2018, doi:10.1007/s10916-018-0982-x.
26. Lijun Xiao; Han, Dezhi; Meng, Xiangwei; Liang, Wei; Li, Kuan-Ching, “A Secure Framework for Data Sharing in Private Blockchain-Based WBANs”, IEEE Access, vol. 8, pp. 153956–153968, 2020, doi:10.1109/access.2020.3018119.
27. Geetanjali Rathee; Sharma, Ashutosh; Saini, Hemraj; Kumar, Rajiv; Iqbal, Razi, “A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology”, Multimedia Tools and Applications, 2019, doi:10.1007/s11042-019-07835-3.
28. Asad Abbas;Roobaea Alroobaea;Moez Krichen;Saeed Rubaiee;S. Vimal;Fahad M. Almansour, “Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things”, Personal and Ubiquitous Computing, 2021, doi:10.1007/s00779-021-01583-8.
29. Rajakumar Arul;Yasser D. Al-Otaibi;Waleed S. Alnumay;Usman Tariq;Umar Shoaib;M. D. Jalil Piran, “Multi-modal secure healthcare data dissemination framework using blockchain in IoMT”, Personal and Ubiquitous Computing, 2021, doi:10.1007/s00779-021-01527.