Peer-to-Peer Networking and Applications (2023) 16:846–857
https://doi.org/10.1007/s12083-022-01429-x

An intelligent blockchain strategy for decentralised healthcare framework

Akanksha Goel[1,2] · **S. Neduncheliyan**[1]

Received: 8 August 2022 / Accepted: 29 November 2022 / Published online: 18 January 2023
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
Nowadays, securely sharing medical data is one of the significant concerns in blockchain technology. The existing blockchain approaches have faced high time consumption, low confidentiality, and high memory usage for transferring the file in a secure way because of attack harmfulness and large unstructured records. It has ended in security threat, so the integrity of the user data has been lost. Hence, a novel hybrid Deep Belief-based Diffie Hellman (DBDH) security framework was presented to protect medical data from malicious events. Incorporating a deep belief neural system continuously monitors the system and identifies the attacks. Initially, the IoMT dataset was collected from the standard site and imported into the system. Moreover, hash 1 was calculated for the original data and stored in the cloud server for verification. Then, the original data was encrypted with a private key for data hiding. The incorporation of homomorphic property helps to calculate hash 2 for encrypted data. Finally, in the verification module, both hash values are verified. In addition, cryptanalysis was performed by launching an attack to validate the performance of the designed model. Moreover, the estimated outcomes of the presented model were compared with existing approaches to determine the improvement score.

Keywords Blockchain technology · Diffie hellman approach · Deep belief neural system · Medical data · Cryptanalysis

1 Introduction

Internet of Things (IoT) and some other technologies like AI, i.e., Artificial Intelligence, blockchain method, and Mixed Augmented Reality [1], have the theory to remodel the smart ecosystem [2]. All the data shared in the mutual link includes living and non-living structures [3]. Due to the fast growth of this kind of technology Internet of Medical Things (IoMT) plays a significant role in our day-to-day life [4]. Some technologies like Bluetooth Low energy, wireless network sensor, and the 5G data network transform into standard technology that is a more intelligent network [5]. The development of IoT outspread in every section [6], which contains health maintenance, economics, administration, farming, and instruction [7]. The hiking number of IoT devices is not secured, which develops security issues [8]. The problems are attacks, registration done in the machine, and the risk integrated into the device [9]. The blockchain and AI-enabled decentralized healthcare systems are represented in Fig. 1.

IoT plays a significant role in the health maintenance department and is used to connect patients with the health department and monitor the patients [10]. It is of two concepts: the patient's data are secured and transparency. In 2018, some information was noted from the health department and human service office for Civil Rights [11]. Usually, the data exchanged in-between the health maintenance and medical detectors are centralized by an unauthorized server [12]. Blockchain technology can also address ordinary health care because of its unchangeable nature [13]. In the medical market, the Internet of Things is decentralized based on the usage of health maintenance [14]. In 2021 we concluded that nearly 28 billion had used IoT devices. According to the unequaled rate rise, the old age people population can be 16 times more than the whole population from 2025 to 2050 [15]. IoT has played a vital role in explaining health maintenance in IoMT [16].

✉ Akanksha Goel
akanksha.rkgit@gmail.com

S. Neduncheliyan
dean.cse@bharatuniv.ac.in

[1] School of Computing, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu 600073, India

[2] Dr. D.Y. Patil Biotechnology and Bioinformatics Institute, Pune 411033, India

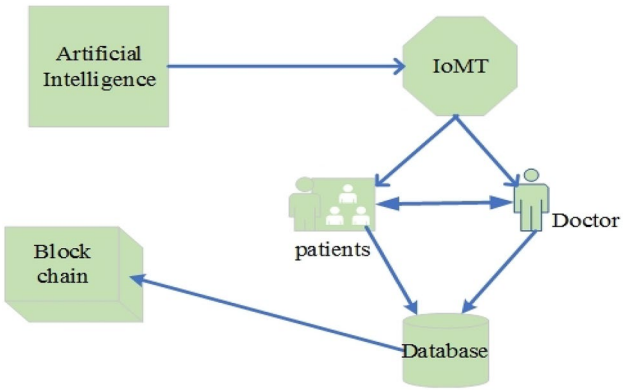


Fig. 1 Blockchain: AI-enabled decentralized healthcare

The IoT research explains the IoMT framework's architecture and its use in the healthcare department [17]. The issues that occur in decentralized architecture can be overcome by blockchain technology [18]. The above figure details that all dataset is stored in the blockchain.

The paper is arranged as follows, the recent literatures are described in Section 2, system model with problem is defined in Section 3. The solution for the described problem is defined in the Section 4. The outcome of the implemented proposed solution is elaborated in the Sections 5 and 6 concludes the paper.

2 Related work

A few recent works related to blockchain technology are listed below,

The patients were monitored by remote control and the information guide for a few years; the healthcare service was inexpensive. So, Puri et al. [19] say that the health maintenance department uses the AI model in IoT, and the framework decentralizes it. This experiment is analyzed in the real-time domain. The limitations here are the energy used for consumption, throughput, the fee used for a transaction, the average slowness, and the time that requests the information.

The world faces many chronic diseases and more medical costs during population growth. Hence, Sodhro et al. [20] describe how healthcare is based upon the Internet of Things (IoT), and the efficient model is decentralized by the energy to transmit the data. Some primary challenges faced in the Internet of Medical Things (IoMT) are energy consumption, battery charging, and the battery's lifetime.

During the period of COVID–19, all over the world, human's faced severe health issues. Thus, Bera et al. [21] say that in COVID – 19 periods, IoMT enabled a framework to monitor from home and is based upon blockchain technology. At the same time, Fog computing, as well as blockchain technology, plays a vital role in COVID -19 pandemic in monitoring the patient from home and is more secure in IoMT. Thus the Internet of Medical Things has allowed various IoT devices into the patient's body.

The fast growth of the Internet of Medical Things helps the intellectual development of the healthcare network in real-time life. So, Egala et al. [22] say that IoMT controls affectivity, and this technology is secure and private. Here, they have established hybrid computing with the help of blockchain technology, and the stored data is spread towards the blockchain and is based upon the cloud-centric IoMT network. The disadvantages are high breakage, the cost of storage, and the failure point being single.

The operation performed here is mobile edge computing and blockchain technology. It transforms the data through e-health resources. Therefore, Nguyen et al. [23] say that using the blockchain technology IoMT system develops the edge-health to decentralize. In this architecture, we are using an advanced decentralized healthcare system. By comparing to the real world, the results of this experiment give privacy for the data and guarantee security.

Maleh et al. [24] have described privacy and security challenges using the blockchain model in digital applications. Hence, this research work has helped to find a suitable research direction for enhancing blockchain technology and enriching digital appliances' privacy.

Besides, the security of digital applications has been enriched using the machine learning strategy. So, Maleh et al. [25] have defined Machine Learning (ML) based blockchain security for digital applications. In this ML, training a large database is possible, which helps to find malicious users and actions from the large files. Hence, this model is helped to reduce data theft and other security issues.

The key steps of this present study are described as follows,

- Initially, the sensed medical parameter database was gathered from the standard site and trained for the python system.
- Then a novel DBPDH was designed for attack detection, attack neglection, and data hiding purposes.
- Moreover, the homomorphic concept has been implemented to check the confidential range of the stored data.
- Finally, cryptanalysis was performed to check the security range of the designed blockchain model.
- Then the parameters were calculated and compared with other models in terms of resource usage, encryption time, decryption time, confidential rate, execution time, and error rate.

3 System model and problem statement

Securing medical records are much-needed tasks for the healthcare system to maintain confidentiality. However, the attack's harmfulness and data vastness and complexity have made data protection a complicated mission. In addition, if the data is too large, it contains a wide range of noisy content that has complicated the crypto process. In the existing technique, the sensed dataset is stored in the medical cloud (Hospital, clinic), and an inefficient security mechanism is incorporated. In this system, the possibility of attacks is high, and attacks are not neglected. Thus, the information present in the dataset is injected.

In the past, ML and crypto models existed along with the blockchain strategy. But those approaches have required additional resources and computational time to execute the process. It has tended to maximize the algorithm complexity by taking more execution time. Hence, using the conventional security model protecting sensitive information like the medical database is too risky and, in some cases, is not workable.

Hence, an attack detection and prevention system is required for a healthcare framework. Figure 2 shows the existing model and its problem statement. These drawbacks in the current system motivate to present this article. The present research study has aimed to develop a prediction system and blockchain technology as the combined version for the IoMT to protect the data from third parties.

4 Proposed DBDH framework to secure medical data

A novel Deep Belief-based Diffie Hellman (DBDH) framework was proposed in this article to secure the sensed medical data. Hence, the presented model has been validated using the standard IoMT database. Then, a novel blockchain strategy is designed with suitable parameters to secure the specific data. The system processes the dataset and neglects the attacks present in it. Then, the hash 1 value is calculated for the original data.

Moreover, the data hiding was performed through encryption and decryption. In addition, the trustworthiness of the data has been verified by designing the homomorphism concept for the encrypted data. Then, the hash 2 value generated for the encrypted data is validated with the hash 1 value, and the confidential rate is measured. The architecture of the proposed DBDH model is shown in Fig. 3.

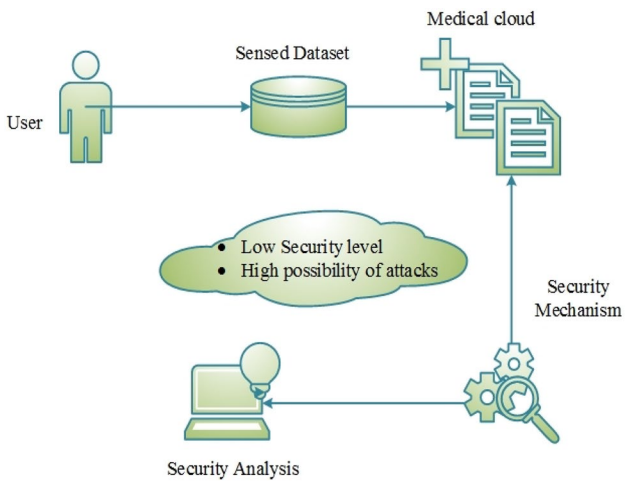


Fig. 2 System model with problem statement

4.1 Design of the DBDH model

The presented security framework integrates the attributes of the Deep Belief approach [26] and the Diffie Hellman technique [27]. To validate the developed framework IoMT dataset is collected and imported into the system. Then, a novel method was designed with a security mechanism to protect the dataset from attacks. The input dataset is initialized inside the system based on the concept of the deep belief approach. The dataset initialization function is expressed in Eq. (1).

$$F_D^*\left[M_{IoT}\right] = (md_1, md_2, md_3, ..., md_s) \tag{1}$$

Here, F_D^* refers to the initialization function for the input dataset, M_{IoT} indicates the collected IoT-based sensed dataset, md_1 is the data present in the dataset, and s indicates the total number of data present.

4.1.1 Attack detection and neglection

After initialization, the dataset is trained to detect and neglect the attacks. Initially, the attacks present in the dataset are tracked, and then it is neglected from the dataset. The attack tracking and neglection function is expressed in Eqs. (2) and (3).

$$A_{Tr}^{\circ}(M_{IoT}) = \frac{1}{\gamma}\sum_{i=1}^{s}(md,\ md^*) \tag{2}$$

$$N_a^{''}\left(M_{IoT}\right) = M_{IoT}(md) - M_{IoT}\left(md^*\right) \tag{3}$$

where, A_{Tr}° defines the attack detection function, γ indicates the attack tracking variables, $N_a^{''}$ represents the attack neglection function md, and md^* refers to the regular and attack data present in the dataset. In this process, the attacks present in the dataset are removed from the dataset.

4.1.2 Hash value calculation

After attack prediction and neglect, the dataset is converted into binary data. In the proposed design, the converted input data undergoes an encryption process for security purposes.

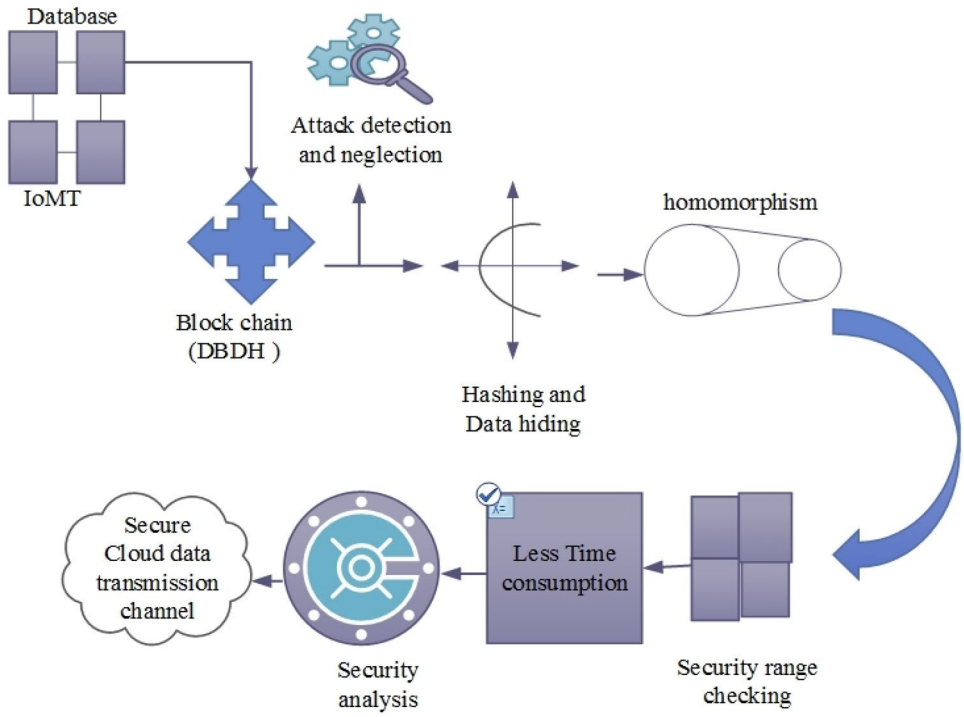


Fig. 3 DBDH framework

So, initially, the hash value is calculated for the original data. The function for hash value calculation is represented in Eq. (4).

$$H_{a1} = md(mod\ n) \tag{4}$$

The generated hash value is then stored in the cloud for further validation. The hash 1 is indicated as H_{a1} and n denotes the prime number.

4.1.3 Encryption

Crypto analysis includes encryption and decryption processes. Initially, a key is generated using the Diffie Hellman algorithm in the designed model, and the data is encrypted with the generated key. Here, the key is generated using the file number and public variables. The equation for key generation is expressed in Eq. (5).

$$K_S^* = u^i mod\ v \tag{5}$$

where, K_S^* indicates the generated key, u and v indicate the public variables, i denotes the file number. After key generation, the data is encrypted with a key. The encryption of data is represented in Eq. (6).

$$E_{\mathbf{N}}(md) = K_S^* \times md = C_t \tag{6}$$

where, $E_{\mathbf{N}}$ indicates the encryption function C_t and denotes the cipher text. In the encryption process, the original data is converted into another form by performing a multiplication operation with a generated key.

4.1.4 Homomorphism

After the encryption of data, a homomorphism is performed to calculate hash 2. Hash 2 is calculated for encrypted data to verify the user. The calculated hash value should match the hash 1 value calculated for the original data. The hash 2 calculation is expressed in Eq. (7).

$$H_{a2} = \frac{1}{2}\left(C_t(mod\ n)\right) \tag{7}$$

After homomorphism, the hash 1 and hash 2 values are checked to validate the user. The hash value is indicated as H_{a2}. If it does not match, the system displays it as "data injected." If the hash value matches, the system gives users access by sending a key to the user.

4.1.5 Decryption

After validating the hash values, the system sends the user a private key. To retrieve the original data, the user performs the division operation with the cipher text. The decryption equation is expressed in Eq. (8).

$$md \rightarrow C_t / K_S^* \tag{8}$$

In the decryption process, the user retrieves the original input data by decrypting the cipher text with a key.

Algorithm: 1 DBDH

```
start
{
        int M_IoT = md_1, md_2, md_3, ...., md_s;
        //initialization of input medical IoT dataset
        Attack_ detection()
        {
        A°_Tr → γ(md, md*)
//In the detection process, the ordinary and attack data are tracked
N''_a → −md* + md
//in the attack neglection function, the tracked attack data are neglected from the
system
}
Hash1_ Generation()
{
int H_a1 ;
    md(mod n) → H_a1
    // The hash 1 value is calculated for the original input data and stored in the server
}
Encryption ()
{
    int C_t , K*_S ;
    C_t = K*_S × md  //the plain text md is encrypted with a generated key
}
Homomorphism ()
{
    in  H_a2;
    C_t → mod n → H_a2;
    //hash 2 is calculated for encrypted data using homomorphism property to validate
    the user
}
Validation ()
{
    if (H_a1 = H_a2)
{
    //Verification is Successful, the system sends encrypted data along with key
Decryption ()
{
    D_N → C_t ⇒ md
    //plain text is retrieved by decrypting the cipher text with key
}
}
        else (Data Injected);
        //if the hash values do not match, it shows "data injected."
        }
}
end
```

Thus, the designed model secures the medical files using blockchain and cryptoanalysis. Moreover, the developed model is presented in pseudo-code format in Algorithm 1.

In addition, attacks are launched to validate the system's performance. The workflow of the designed model is illustrated in Fig. 4.

5 Result and discussion

A blockchain-based security framework was developed to protect medical data from attacks. This model combines the features of the deep belief neural system and the Diffie Hellman algorithm. The IoMT dataset containing the disease and symptoms data is gathered and imported into the system. Initially, the presented model identifies and neglects the attacks present in the dataset. Moreover, hash 1 is calculated for the original data and stored in the cloud server. In addition, the input data is encrypted with a private key. In addition, hash 2 is calculated for the encrypted data. Finally, hash 1 and hash 2 are verified in the verification module. If the hash values match, the verification is successful, and the private key is sent to the user for decryption. The designation of the implementation parameters is listed in Table 1.

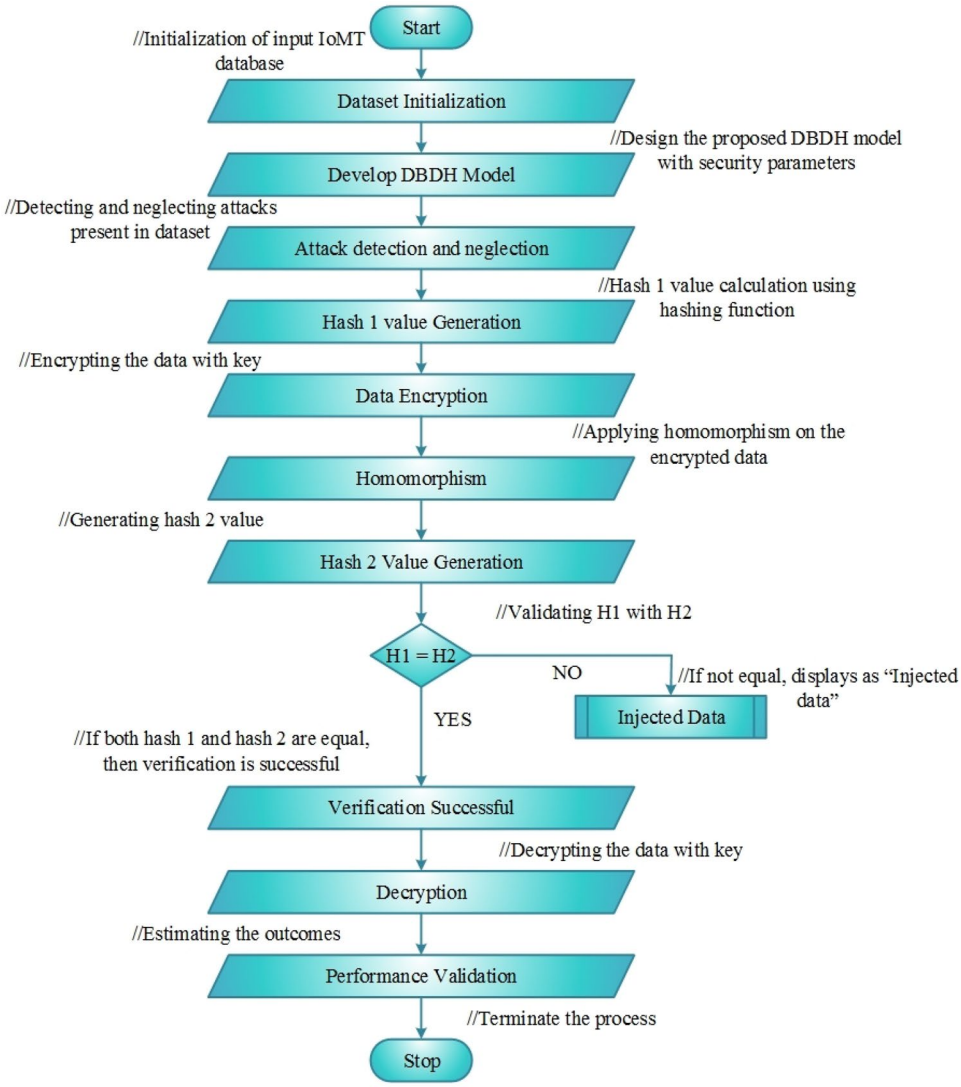
In addition, a DoS attack is launched in the system to validate the system's performance. Moreover, the outcomes of the developed model are estimated in dual cases as before and after the attack. Finally, a comparative analysis was performed to determine that the presented approach attained more significant outcomes than existing approaches.

5.1 Case study

The developed case study explains the functioning of the presented blockchain approach. Initially, the IoMT database was collected from the standard site and imported into the system. The input dataset contains symptoms and disease features. Then, the gathered dataset is initialized in the system. After data initialization, the DBDH framework was designed with security parameters. The developed model detects and neglects the attacks present in the dataset. Then, the hash 1 value is calculated for the original binary data for validation purposes. The generated hash value is stored in the cloud server for verification.

After hash calculation, the original data is encrypted with the generated private key. Moreover, homomorphism was performed on the encrypted data to calculate the hash 2 value. Then, the generated hash 2 value is verified with the hash 1 value stored in the cloud server. If the hash value matches, then user 1 sends the private key to user 2. User 2 decrypts the data with the private key. If the hash values are not matched, it shows "Data injected." The workflow of the developed model is illustrated in Fig. 5. In addition, to validate the performance of the developed model, a DoS attack was launched in the system. Moreover, the performance metrics are estimated in dual cases as before the attack and after the attack.

Fig. 4 Flowchart of DBDH



5.2 Cryptanalysis

After cryptanalysis, an attack is launched in the system to validate the performance of the presented approach. Here, a Denial of Service (DoS) attack is launched to determine the outcomes of the designed model in dual phases before and after the attack. The variation between the results of before and after attacks is minimal because the integration of deep belief continuously monitors the system and neglects the attacks.

After launching attacks, the confidentiality and error rate is estimated for before and after attack cases. Figure 6 displays the confidential and error rate before and after the attack. Before the attack, the confidentiality rate attained was high compared to after the attack. The confidential rate before and after an attack is 0.9593 and 0.9552, respectively, as shown in Fig. 6a. In addition, the error rate before and after the attack is 0.0406 and 0.044, respectively, as shown in Fig. 6b.

5.3 Comparative analysis

The comparative assessment was performed to manifest that the developed model attained higher performances than others. The existing techniques, such as an Encrypted Scheme based on Curve Integration (ESECI) [28], Deep-based Sensitive Aware Elliptic Curve Cryptography with Harmony

Table 1 Description of Implementation parameters

Designation of execution parameters	
Parameters	Description
Platform	Python
Version	3.10
OS	Windows 10
Dataset	Disease Symptom Data
Attack Launched	DoS

Search optimization (DbSAEC_HSO) [29], and Educational Records Secure Storage and Sharing (ERSS) [30]. Here, the computational complexity was measured as encryption time, decryption time and execution time.

5.3.1 Encryption and decryption time

Encryption time is the time the system takes to convert original text into cipher text. Similarly, decryption time is the time taken to restore the original data from encrypted data. Generally, it is measured at the end of the encryption process. It is mainly calculated to validate that the designed model has consumed less time to encrypt and decrypt the files.

The encryption and decryption time of the proposed methodology is compared with existing approaches to validate that the presented system consumes less time to encrypt and decrypt the data. The comparison of encryption and decryption time is shown in Fig. 7. The existing blockchain approaches, such as ESECI, DbSAEC_HSO, and ERSS attained high encryption times of 70 ms, 50 ms, and 25 ms, respectively. But, the designed model achieved a low encryption time of 3.55 ms. Similarly, the decryption time of existing approaches is high, that is, 90 ms, 53 ms, and 35, respectively. But, the designed blockchain approach attained a low decryption time of 3.6 ms. Thus, the developed model earned less time to encrypt and decrypt the data.

5.3.2 Execution time

The time consumed by the system to execute the entire process is defined as the execution time. The execution time of the presented approach is compared with conventional security approaches.

The execution time achieved by the existing blockchain-based security approaches such as ESECI, DbSAEC_HSO, and ERSS is 30 ms, 50 ms, and 15 ms, respectively. But the presented DBDH approach attained a low execution time of 12 ms. The comparison of execution time is shown in Fig. 8. This comparative assessment proves that the designed security approach consumes less time to execute the entire process.

5.3.3 Confidential rate

The rate at which the original data preserved in the system that is confidential records are protected is defined as the confidential rate. The confidential rate earned by the designed model is compared with existing approaches to determine the security level of the presented method.

The confidential rate is shown in Fig. 9. The Confidential rate achieved by the existing approaches, such as ESECI, DbSAEC_HSO, and ERSS is 79%, 76%, and 84%, respectively. The presented method estimates the

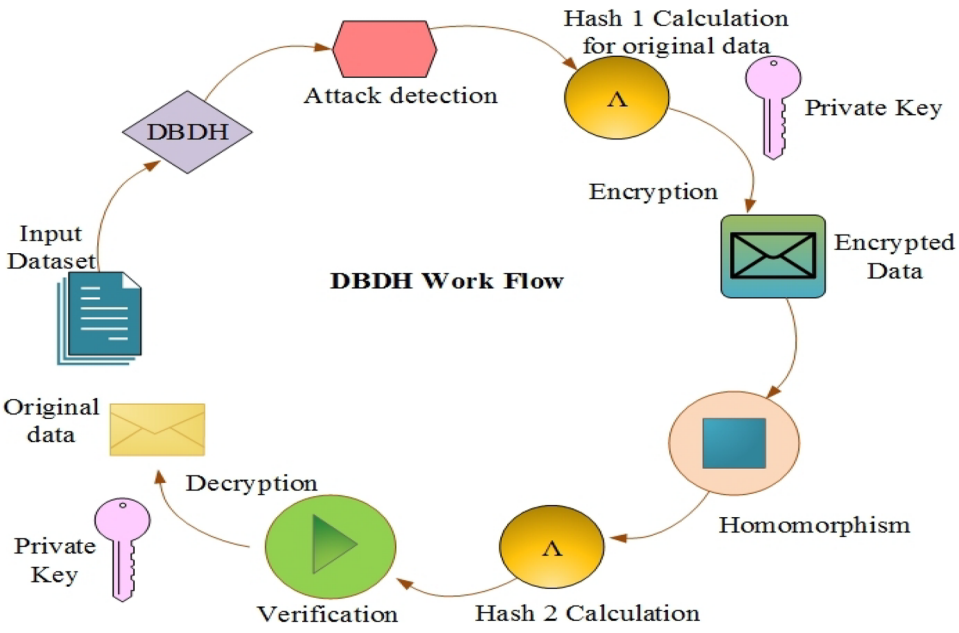
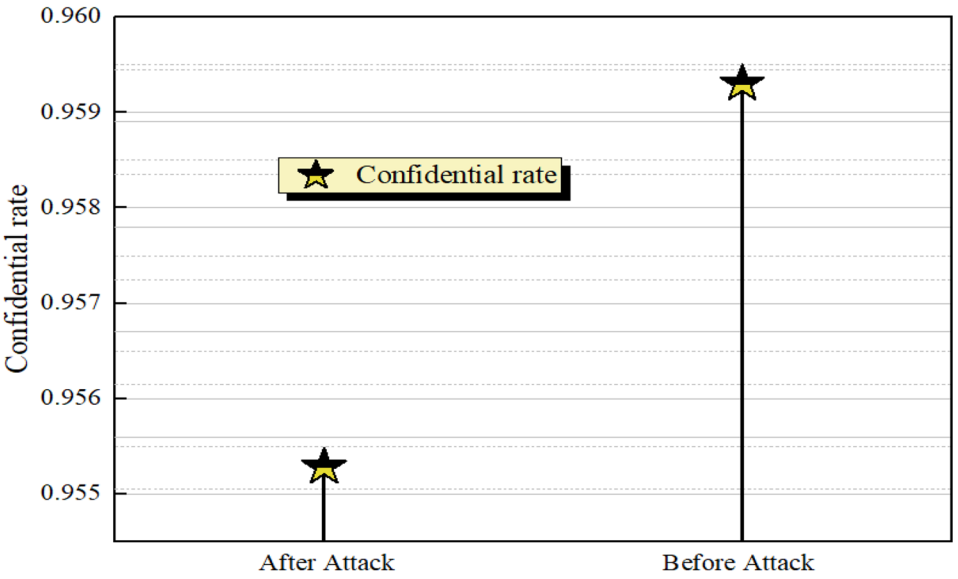
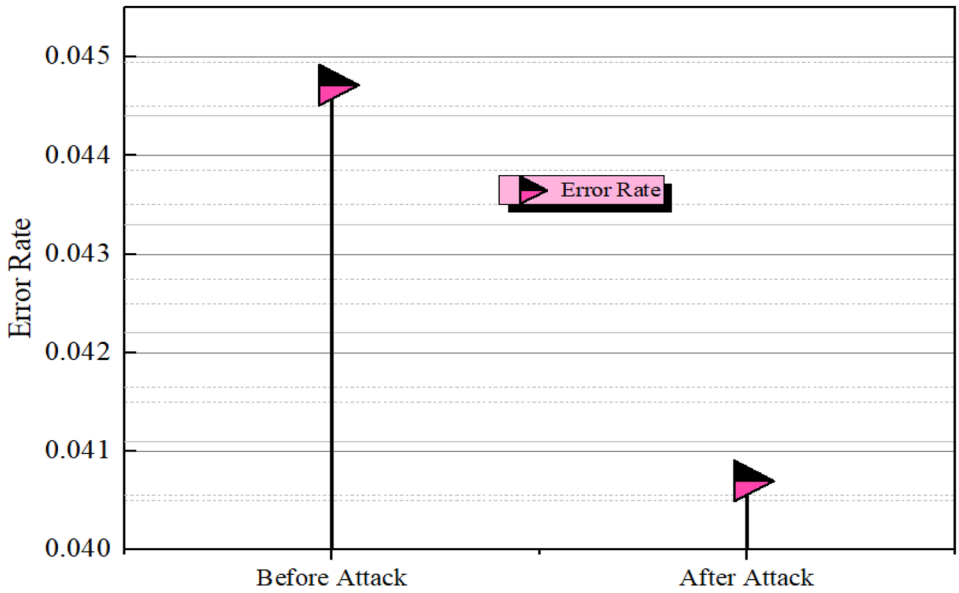


Fig. 5 Work flow of DBDH



(a) Confidential rate before and after the attack



(b) Error Rate before and after the attack

Fig. 6 Outcomes before and after attack **a** Confidential Rate, **b** Error rate

confidential rate in dual cases with and without attacks. The confidential rate of the proposed model with and without attack is 95.52% and 95.93%, respectively. The deep belief neural features in the presented model monitor and neglects attacks. Thus, the confidential rate is high in the designed model.

5.3.4 Error rate

The error rate obtained by the system is compared with conventional approaches to validate that the presented model earned less error rate than others. The comparison of error rates is shown in Fig. 10.

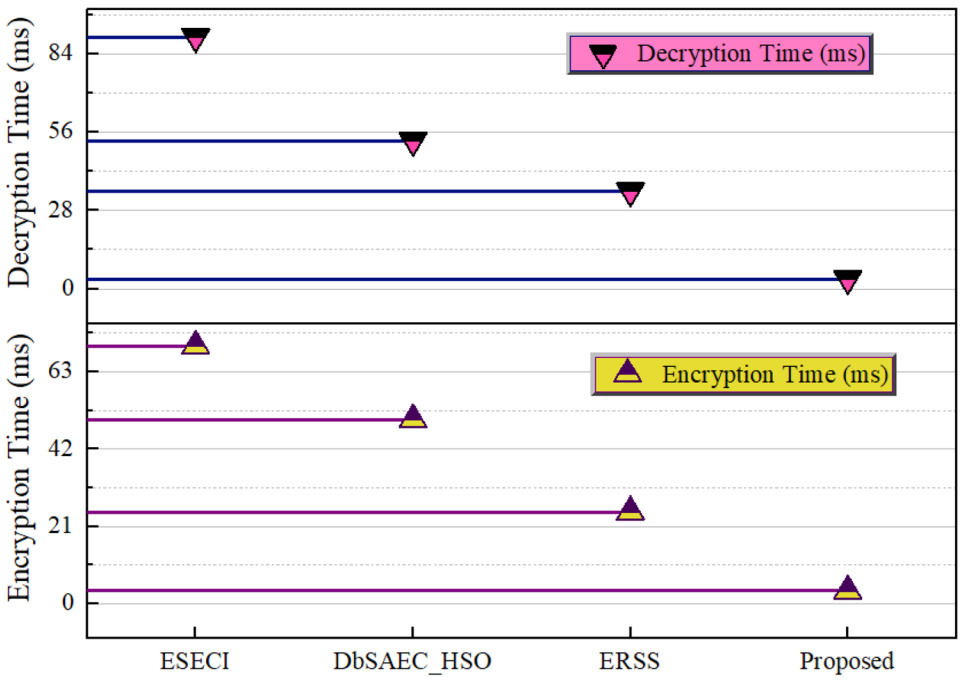


Fig. 7 Comparison of encryption and decryption time

The error rate earned by the presented approach is determined in two cases: with and without attack. The error rate obtained by the designed model with and without attack is low, 0.0447, and 0.0407, respectively. But the existing blockchain-based security approaches attained a high error rate of 2.4%, 4%, and 1.1%, respectively.

In addition, the overall statistical comparative analysis was performed to verify that the designed model attained better outcomes than others. This proves that the presented model consumed less time to encrypt and decrypt the data, earned a high confidential rate, and obtained a low error rate. Table 2 tabulates the comparative statistical analysis of different blockchain-based approaches.

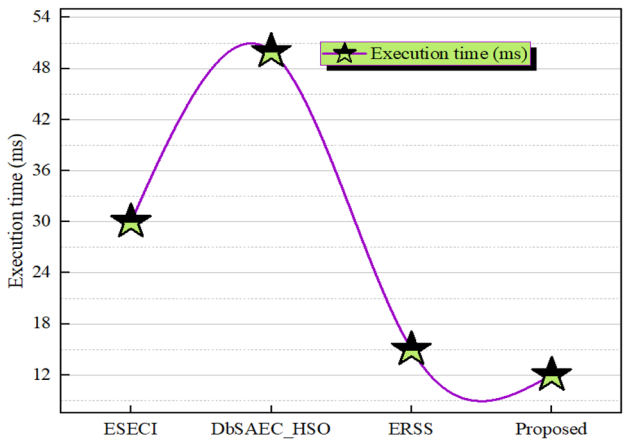


Fig. 8 Comparison of execution time

5.4 Discussion

The overall observation of the presented article is described in the discussion. The motive of the designed model is to protect medical data from malicious events. This framework shares medical data securely in an authenticated manner. The IoMT dataset containing the health and symptom dataset is considered to validate the model. The collected dataset is imported and initialized in the system to identify its malicious events. Then, hash1 is estimated for the original dataset and stored in the server (Table 3).

Moreover, the original data is encrypted with a private key, and hash 2 is calculated for encrypted data. Furthermore, the hash 1 and hash 2 values are validated in the verification module. If the hash value matches, the key is sent to the user for the decryption process. On the other hand, if the hash values are not matched, it shows as "Data Injected." Moreover, disease classification was performed in dual cases (with and without attack) to validate the presented approach.

At last, a comparative analysis was performed to verify the outcomes of the designed model by comparing it with existing approaches. Table 1 presents the performance assessment of the proposed system. The overall performance and comparative analysis prove that the developed security model achieved better results than existing approaches.

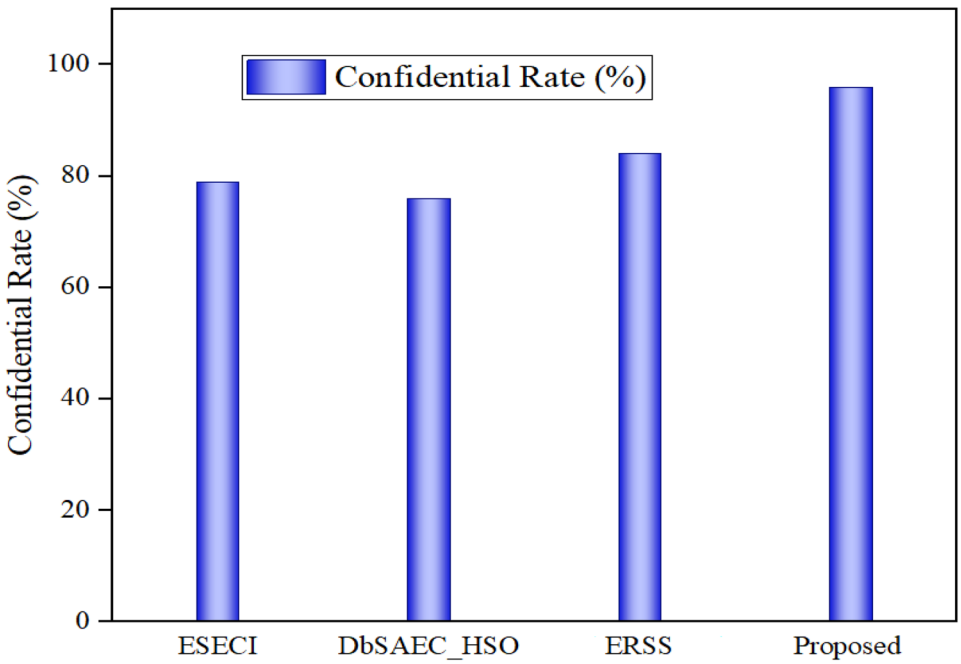


Fig. 9 Comparison of confidential rate

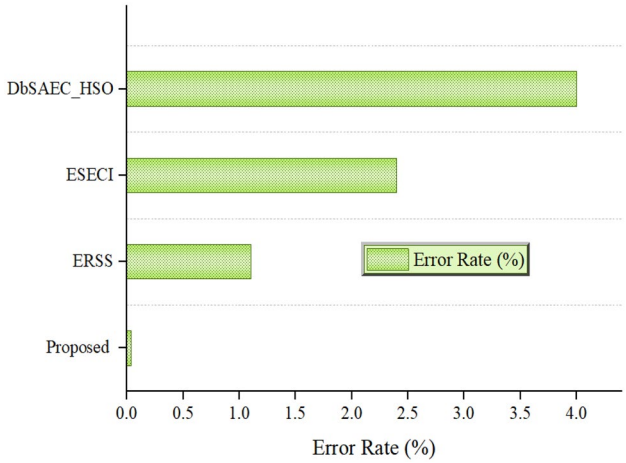


Fig. 10 Comparison of error rate

Table 3 Performance assessment

Metrics	Performance
Encryption Time (ms)	3.55
Decryption Time (ms)	3.6
Execution Time (ms)	12
Confidential rate (With attack)	95.52
Confidential Rate (Without Attack)	95.93
Error Rate (With Attack)	0.0447
Error Rate (Without Attack)	0.0407

Table 2 Statistical comparative analysis of different approaches

Methods	Encryption time (ms)	Decryption time (ms)	Execution time (ms)	Error rate (%)	Execution time (ms)	Confidential rate (%)
ESECI	70	90	30	2.4	30	79
DbSAEC_HSO	50	53	50	4	50	76
ERSS	25	35	15	1.1	15	84
Proposed (DBDH)	3.55	3.6	12	0.04	12	95

6 Conclusion

A novel DBDH approach was developed to secure the medical data stored in a cloud server. The designed model continuously monitors the system and detects malicious events. Hence, to validate the presented approach, an IoMT dataset was collected and imported into the system. Initially, the hash1 value was determined for validation purposes and stored in the server. Moreover, the encryption process was performed with a key to convert the original text to cipher text. In addition, the homomorphic property was integrated into the presented approach to calculate hash 2. Finally, the hash values are verified in the verification module. Furthermore, crypt analysis is performed by launching a DoS attack to validate the system's performance. The designed model was implemented in Python software, and the results were evaluated. Finally, the outcomes of the developed model are compared by comparing the results of the presented approach with existing algorithms. The comparative analysis shows that in the designed model, the encryption and decryption time are reduced by 21 ms, the confidentiality rate was enhanced by 11.5% than the compared models, and the execution time was minimized by 3 ms. In addition, the proposed model has reduced the error score by 1%. Thus, the designed model enhances the security of the blockchain system and protects the data from malicious events.

Authors' contribution Authors A.G. and S.N. have contributed equally to the work.

Funding This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.

Disclosure of potential conflict of interest The authors declare that they have no potential conflict of interest.

Ethical approval All applicable institutional and/or national guidelines for the care and use of animals were followed.

Informed consent For this type of analysis formal consent is not needed.

References

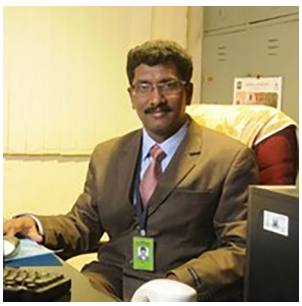
1. Das D, Banerjee S, Ghosh U, Biswas U, Bashir AK (2021) A decentralized vehicle anti-theft system using Blockchain and smart contracts. Peer Peer Netw Appl 14:2775–2788. https://doi.org/10.1007/s12083-021-01097-3
2. Karode T, Werapun W (2022) Robustness against fraudulent activities of a blockchain-based online review system. Peer Peer Netw Appl 15:92–106. https://doi.org/10.1007/s12083-021-01225-z
3. Mahmud H, Rahman T (2021) An Application of blockchain to securely acquire, diagnose and share clinical data through smartphone. Peer Peer Netw Appl 14:3758–3777. https://doi.org/10.1007/s12083-021-01210-6
4. Hussien HM, Yasin SM, Udzir NI, Ninggal MIH, Salman S (2021) Blockchain technology in the healthcare industry: Trends and opportunities. J Ind Inf Integr 22:100217. https://doi.org/10.1016/j.jii.2021.100217
5. Razdan S, Sharma S (2021) Internet of medical things (IoMT): Overview, emerging technologies, and case studies. IETE Tech Rev 1–14. https://doi.org/10.1080/02564602.2021.1927863
6. Adil M, Khan MK, Jadoon MM, Attique M, Song H, Farouk A (2022) An AI-enabled hybrid lightweight authentication scheme for intelligent IoMT based cyber-physical systems. IEEE Trans Netw Sci Eng. https://doi.org/10.1109/TNSE.2022.3159526
7. Ayache M, Gawanmeh A, Al-Karaki JN (2022) DASS-CARE 2.0: Blockchain-based healthcare framework for collaborative diagnosis in CIoMT ecosystem. 2022 5th Conference on Cloud and Internet of Things (CIoT), IEEE. https://doi.org/10.1109/CIoT53061.2022.9766532
8. Gao Y, Lin H, Chen Y, Liu Y (2021) Blockchain and SGX-enabled edge-computing-empowered secure IoMT data analysis. IEEE Internet Things J 8(21):15785–15795. https://doi.org/10.1109/JIOT.2021.3052604
9. Rahman MZU, Surekha S, Satamraju KP, Mirza SS, Lay-Ekuakille A (2021) A collateral sensor data sharing framework for decentralized healthcare systems. IEEE Sens J 21(24):27848–27857. https://doi.org/10.1109/JSEN.2021.3125529
10. Awad A, Fouda MM, Khashaba MM, Mohamed ER, Hosny KM (2022) Utilization of mobile edge computing on the internet of medical things: A survey. ICT Express. https://doi.org/10.1016/j.icte.2022.05.006
11. Muhammad G, Alshehri F, Karray F, El Saddik A, Alsulaiman M, Falk TH (2021) A comprehensive survey on multimodal medical signals fusion for smart healthcare systems. Inf Fusion 76:355–375. https://doi.org/10.1016/j.inffus.2021.06.007
12. Wu G, Wang S, Ning Z (2021) Blockchain-enabled privacy-preserving access control for data publishing and sharing in the internet of medical things. IEEE Internet Things J 9(11):8091–8104. https://doi.org/10.1109/JIOT.2021.3138104
13. Das AK, Bera B, Saha S, Kumar N, You I, Chao HC (2021) AI-Envisioned blockchain-enabled signature-based key management scheme for industrial cyber-physical systems. IEEE Internet Things J 9(9):6374–6388. https://doi.org/10.1109/JIOT.2021.3109314
14. Greco L, Percannella G, Ritrovato P, Tortorella F, Vento M (2020) Trends in IoT based solutions for health care: Moving AI to the edge. Pattern Recognit Lett 135:346–353. https://doi.org/10.1016/j.patrec.2020.05.016
15. Yang L, Yu K, Yang SX, Chakraborty C, Lu Y, Guo T (2021) An intelligent trust cloud management method for secure clustering in 5G enabled internet of medical things. IEEE Trans Industr Inform. https://doi.org/10.1109/TII.2021.3128954
16. Aoun A, Ilinca A, Ghandour M, Ibrahim H (2021) A review of Industry 4.0 characteristics and challenges, with potential improvements using block chain technology. Comput Ind Eng 162:107746. https://doi.org/10.1016/j.cie.2021.107746
17. Zeyer A (2021) Coping with structural uncertainty in complex living systems. Science| Environment| Health, pp 11–29. Springer, Cham. https://doi.org/10.1007/978-3-030-75297-2_2
18. Goyal S, Sharma N, Bhushan B, Shankar A, Sagayam M (2021) Iot enabled technology in secured healthcare: applications, challenges and future directions. Cognitive internet of medical

things for smart healthcare, pp 25–48. Springer, Cham. https://doi.org/10.1007/978-3-030-55833-8_2
19. Puri V, Kataria A, Sharma V (2021) Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0. Trans Emerg Telecommun Technol e4245. https://doi.org/10.1002/ett.4245
20. Sodhro AH, Al-Rakhami MS, Wang L, Magsi H, Zahid N, Pirbhulal S, Nisar K, Ahmad A (2021) Decentralized energy efficient model for data transmission in IoT-based healthcare system. 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), IEEE. https://doi.org/10.1109/VTC2021-Spring51267.2021.9448886
21. Bera B, Mitra A, Das AK, Puthal D, Park Y (2021) Private blockchain-based AI-envisioned home monitoring framework in IoMT-enabled COVID-19 environment. IEEE Consum Electron Mag. https://doi.org/10.1109/MCE.2021.3137104
22. Egala BS, Pradhan AK, Badarla V, Mohanty SP (2021) Fortified-chain: a block chain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet Things J 8(14):11717–11731. https://doi.org/10.1109/JIOT.2021.3058946
23. Nguyen DC, Pathirana PN, Ding M, Seneviratne A (2021) Bedgehealth: A decentralized architecture for edge-based iomt networks using block chain. IEEE Internet Things J 8(14):11743–11757. https://doi.org/10.1109/JIOT.2021.3058953
24. Maleh Y, Shojafar M, Alazab M, Romdhani I (2020) Blockchain for cybersecurity and privacy: architectures, challenges, and applications
25. Maleh Y, Shojafar M, Alazab M, Baddi Y (2021) Machine intelligence and big data analytics for cybersecurity applications. Springer, Cham. https://doi.org/10.1007/978-3-030-57024-8
26. Wang Y, Pan Z, Yuan X, Yang C, Gui W (2020) A novel deep learning based fault diagnosis approach for chemical process with extended deep belief network. ISA Trans 96:457–467. https://doi.org/10.1016/j.isatra.2019.07.001
27. Costello C (2020) B-SIDH: supersingular isogeny Diffie-Hellman using twisted torsion. International Conference on the Theory and Application of Cryptology and Information Security, Springer, Cham. https://doi.org/10.1007/978-3-030-64834-3_15
28. Velmurugadass P, Dhanasekaran S, Anand SS, Vasudevan V (2021) Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. Mater Today: Proc 37:2653–2659. https://doi.org/10.1016/j.matpr.2020.08.519
29. Pourvahab M, Ekbatanifard G (2019) Digital forensics architecture for evidence collection and provenance preservation in iaas cloud environment using sdn and blockchain technology. IEEE Access 7:153349–153364. https://doi.org/10.1109/ACCESS.2019.2946978
30. Li H, Han D (2019) EduRSS: A blockchain-based educational records secure storage and sharing scheme. IEEE Access 7:179273–179289. https://doi.org/10.1109/ACCESS.2019.2956157

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Mrs. Akanksha Goel Assistant Professor in the department of Artificial Intelligence and data science in Dr. D. Y. Patil Biotechnology and Bioinformatics institute, Pune-India. She has 12 years of teaching experience. Completed B. Tech in Information Technology in 2009 and M. Tech in Information Technology in 2011 and M. Tech in Computer science and engineering in 2019. Currently Pursuing Ph.D from School of Computing, Bharath Institute of Higher Education and Research, Chennai 600073 under Research Supervisor Dr S. Neduncheliyan. Her main research area includes Artificial Intelligence, Wireless Sensor Networks, Internet of Things and Wireless Communication.



Dr. S. Neduncheliyan Subbu Professor and Dean - School of Computing, Bharath Institute of Higher Education and Research, Tamil Nadu, India, He holds B.E in Computer Science and Engineering in 1989 from University of Madras, M.S (Engg) in A. I Robotics from School of Electrical and Electronics Engineering from Universiti Sains Malaysia, Penang, Malaysia in 1999 and Ph.D in Information and Communication Engineering from Anna University, Chennai in 2009 .He is having more than 30 years teaching experience in abroad as well as in India. He has published more than 102 research papers in various International and National Journals and Conferences. He has supervised more than 54 M.E and 10 Ph.D thesis. He has organized 27 webinars and invited as a resource person for 12 webinar. He is recipient of Indira Gandhi Excellent Award' 2013, International Business Council, New Delhi, Outstanding Educator & Scholar Award 2014, NFED, Coimbatore, India, Best Research Supervisor Award 2015, Grabs Educational Charitable Trust, Chennai, India, Best NSS Unit Award 2017, Anna University, Chennai, India, South Indian Achiever Award 2020, Kalam Dream Trust, Chennai, 28th January 2020 / Chennai, Life Time Achievement Award 2020, Bestow Edutrex International Award, 5th September 2020 / Bombay. He is having Fellowship from IETE and Membership from IET. His main research area includes Wireless Sensor Networks, Robotics, Internet of Things and Wireless Communication.