Blockchain and AI integration for privacy-preserving clinical trials in the US healthcare sector

Author: Praveen Kumar Rawat
Master's in Computer Applications, PAHM, PSM, ISTQB, MCDBA)
(Praveen.rawat1@gmail.com)
Independent Researcher - Virginia

Abstract

There has been a sea change in the way EHRs are stored in portable cloud platforms; with the integration of cloud services with smartphones and tablets, health information transmissions between consumers and medical professionals have been greatly improved. Electronic medical records (EHRs), outstanding versatility, and cheap operating expenses are all possible thanks to this advanced paradigm. Security of data and safety on networks are two issues that this novel approach raises for e-health solutions. Relying on mobile users to reliably share EHRs while ensuring superior safety in the portable cloud is a formidable challenge.Ensuring consistent and secure sharing of electronic health records (EHRs) across those who work in the mobile cloud is a hard topic. This paper's goal is to provide a fresh blockchain technology that can help with identification and provide integrity to health information, all while keeping patient information safe in the cloud. An improved blowfish system that includes built-in authentication and blockchain deployment utilising appropriate protection is described in this paper. Elephant shedding Optimisation with Opposition-based Learning (EHO-OBL) is a new approach that is used to provide the optimal keys. Thus, the data remains unaltered by the suggested way, and lastly, the offered methodology is shown to be better by a number of measures. The proposed approach outperformed traditional algorithms for a 10 kb file size, including RSA, Moth-Flame optimisation (MFO), Elliptic-Curve Cryptography (ECC), and the Advanced encrypted standard (AES), leading to a key emergence period that is no longer as valuable.

Keywords: Protection of personal information; EHO-OBL methodology; blockchain technology; data integrity

1. Introduction

Implementing blockchain technology to advance e-health and healthcare services has just come to light (Roehrs et al., 2019; Tripathi et al., 2019). The distributed ledger technology known as blockchain has shown great promise in several areas of electronic health, including the safe exchange of electronic medical records (EHRs) and the control of information accessibility. So, according to some studies (Armoogum&Khonje, 2021; Mubarakali et al., 2020; Zhang et al., 2021). Blockchain technology has the potential to revolutionise medicine by providing effective solutions to improve medical delivery.In recent times, the medical profession has undergone vast transformations within the e-health functional area due to rapid technological developments. Examples of such include IoMT and MCC (Ari et al., 2020; Xavier et al., 2020). Increasingly, the use of mobile phones (cell phones and wearable sensors) that can communicate over the Internet allows patients to collect their own personal health information within their geographical location. An authorized person, e.g., the physician, can log into the Internet and thus be able to review this medical information and give prompt assistance for necessary health check-ups (Celesti et al., 2019; Fortino et al., 2018; Tian et al., 2019a). As health delivery

doi: 10.48047/ijiee.2021.11.2.2

systems are modernized to economically benefit consumers, use of this advanced e-health service affords medical practitioners the opportunity to interview patients from a distance and treat outpatient concerns from the comfort of their homes. Thanks to the cloud-based EHRs, healthcare providers enhance monitoring of the health of patients and ensure that the right medication reaches the patient at the right time (Gumaei et al., 2019; Sun, 2020; Xu et al., 2018). However, despite all this, health-related cloud instruments have had a sad case of not being adopted due to security breaches involving the storage of electronic health records in the cloud (Azeez & Van der Vyver, 2019; Hassan et al., 2019; Tian et al., 2019b). Thus, electronic health records should safeguard patient data in the mobile cloud environment as it flows to and from healthcare professionals. According to Feng et al. (2019) and Yang et al. (2019), unauthorized individuals or organizations can access electronic health records (EHRs) without patients' knowledge or consent, thereby compromising the discretion, protection, and trustworthiness of electronic health services cloud systems.

In addition, patients may find it difficult to manage and keep track of their medical data being transferred to various doctors and hospitals on the cloud. According to Chen et al. (2019) and Wang et al. (2019), it is imperative to establish a rightful method for controlling access in the cloud-based EHR share platform.Here is the work's contributions:This study presents blockchain technology that uses optimum encryption to secure cloud-based medical data, which is a revolutionary approachdevelops a more efficient blowfish method to encrypt data.Elephant Herding Optimisation with Opposition-based Learning is an innovative approach that I am suggesting for optimum key creation.Here is the paper's format: Section 2 examines the conventional approaches to hospital privacy protection. The created secure cloud retention paradigm for healthcare systems is shown in Section 3. Optimum key creation using the EHO-OBL method is also covered in part 4.Section 5 provides an explanation of the findings, while Section 6 explains the conclusion.

2.Related work

In view of safeguarding patient privacy, Mubarakali et al. (2019) proposed a model for EHR information operations supported by a blockchain technology known as SEHRTB. It would offer effective and secure transaction facilities between systems, people, service providers, and physicians. At this point, the study presented a blockchain approach in medical care. This means that the patients safely share and access their health information stored in a cloud environment without compromising privacy in the medical profession. Furthermore, it has been a reliable way to ensure patient privacy in electronic health records. Finally, experimental results indicated that the proposed technique performed well in latency and throughput. Al Omar et al. (2019) built a blockchain patient data management system to achieve privacy. As a result, it adopted cryptographic procedures to encrypt patient information while providing anonymity. After that, a thorough study was conducted to ensure the performance of the innovative model in terms of cost-effective. For the protection of electronic health records, e-HR needs to be developed by employing a cloud-based secure e-health system. Within this attitude, the primary idea would be to ensure that only verified parties may outsource the EHRs and to add all of the EHR-related operations to the public blockchain. So, when these associated transactions are added to the blockchain, EHRs cannot be modified. Finally, the security and performance evaluations proved that the system offered was more secure and efficient. The electronic health record sharing technique presented by Nguyen et al. (2019) consisted of the decentralized "Interplanetary File System (IPFS) on a mobile cloud platform", and built mainly by the smart contracts into a trustful access control scheme safe for exchange of EHR among different

doi: 10.48047/ijiee.2021.11.2.2

persons and concerned medical personnel. It was also there with an example of a working prototype in a mobile app using "Ethereum block-chain" protocol. According to the experiential findings, the offered approach provides an effective solution for constant data transmission on clouds against likely dangers.An approach for privacy-preserving medical record exchange across several parties, comprising distrusted patients, semi trusted cloud servers, and research institutions, was proposed in Huang et al. (2020) on the basis of the blockchain. At the same time, it made sure that patients' medical records were available and consistent across research institutions, and that zero-knowledge evidence was used for verifying that the records met certain set requirements without compromising the privacy of patients. Afterward, the decrypting of the ciphertext was ensured through the execution of the proxy re-encryption tool. Developed by Yue et al. (2016), the Healthcare Data Gateway (HGD) App uses blockchain technology to allow patients to share, manage, and own their data safely without compromising privacy; hence, new dimensions are created to improve healthcare systems' intelligence while keeping patients' data private. An access system focused on purpose was developed to ensure data privacy. In addition, with the help of an integrating Indicator-Centric Structured (ICS), it was feasible to quickly and effectively systematise all kinds of private medical information. Dwivedi et al. (2019) sought to address concerns about health information privacy by integrating blockchain technology with the Internet of Things (IoT). For Internet of Things (IoT) devices that need additional confidentiality and security-related characteristics, a new kind of customised blockchain structure was proposed. Enhanced privacy and security features of this model rely on advanced cryptographic primitives. Proposed here is a methodology for securing and anonymizing transactions using IoT appliances on a blockchain-based platform. Kuo et al. (2020) proposed a system combining level-wise model learning, blockchain-based model dissemination, and a novel hierarchical consensus algorithm for model ensemble.We evaluated the execution time and learning iterations with the current techniques designed for flat network topologies and presented a possible implementation of Hierarchical Chain that does hierarchical privacy-preserving modelling on blockchain.

3.Created a mechanism to ensure the privacy of protected healthcare systems in the cloud

To help secure patient information effectively, we created the Keyless Signature Infrastructure (KSIBC) paradigm. In order to treat a patient, a doctor may obtain their health data by providing their personal ID and the patient's private key. In the local database, the doctor keeps all of the recovered data. Furthermore, the individual's access control is validated in the Access Control List (ACL; Nagasubramanian et al., 2020) by deploying the supplied ID. Various KSI procedures are carried out to sign data in order to ensure digital integrity, provided that the users are authenticated early on. An initial gateway is part of this, and it acts as a first aggregator to verify. Then, the created approach's secrecy and data security are guaranteed by the core. Further processing and validation of the information is then submitted to the chain. The health information of every patient are uploaded to the blockchain in the form of a block. The well-established KSIBC paradigm uses the technology of blockchain to provide greater safety for information.The suggested research makes use of blockchain-based optimum encrypting. Confidential information transfer among the companies is the main emphasis here, and an upgraded version of Blowfish is employed for encrypting. Encrypting is done utilising a separate role's public key rather than the user's public keys. Another thing that needs a private key is decryption. Keys are generated in this instance using a unique EHO-OBL approach. Furthermore, the use of a personal key to do the reverse operation is known as decryption. The

doi: 10.48047/ijiee.2021.11.2.2

KSIBC framework is illustrated in Figure 1 for medical information.

4.Blowfish algorithm optimisation for improved key generation

As an alternative to traditional encryption methods, Bruce modelled blowfish to be free and quick. It is slowly but surely becoming known as a more robust method of encryption.Many advantages come with the Blowfish method. According to Agrawal and Mishra (2012), it is suitable for hardware execution, efficient, and does not need a license. The blowfish method relies on the fundamental operators of XOR, addition, and table lookup.Some prerequisites for the the blowfish algorithm method are listed below: The S-array, four 32-bit P-boxes, and 64-bit blocks cypher are some of its features. The key lengths are also uneven. There are 256 elements for every P-box, however there are 18 32-bit sub-keys in the S-array. "a key-expansion portion and a data-encryption part" are the two components that make up the method.A information component of 64 bits is used as the source.

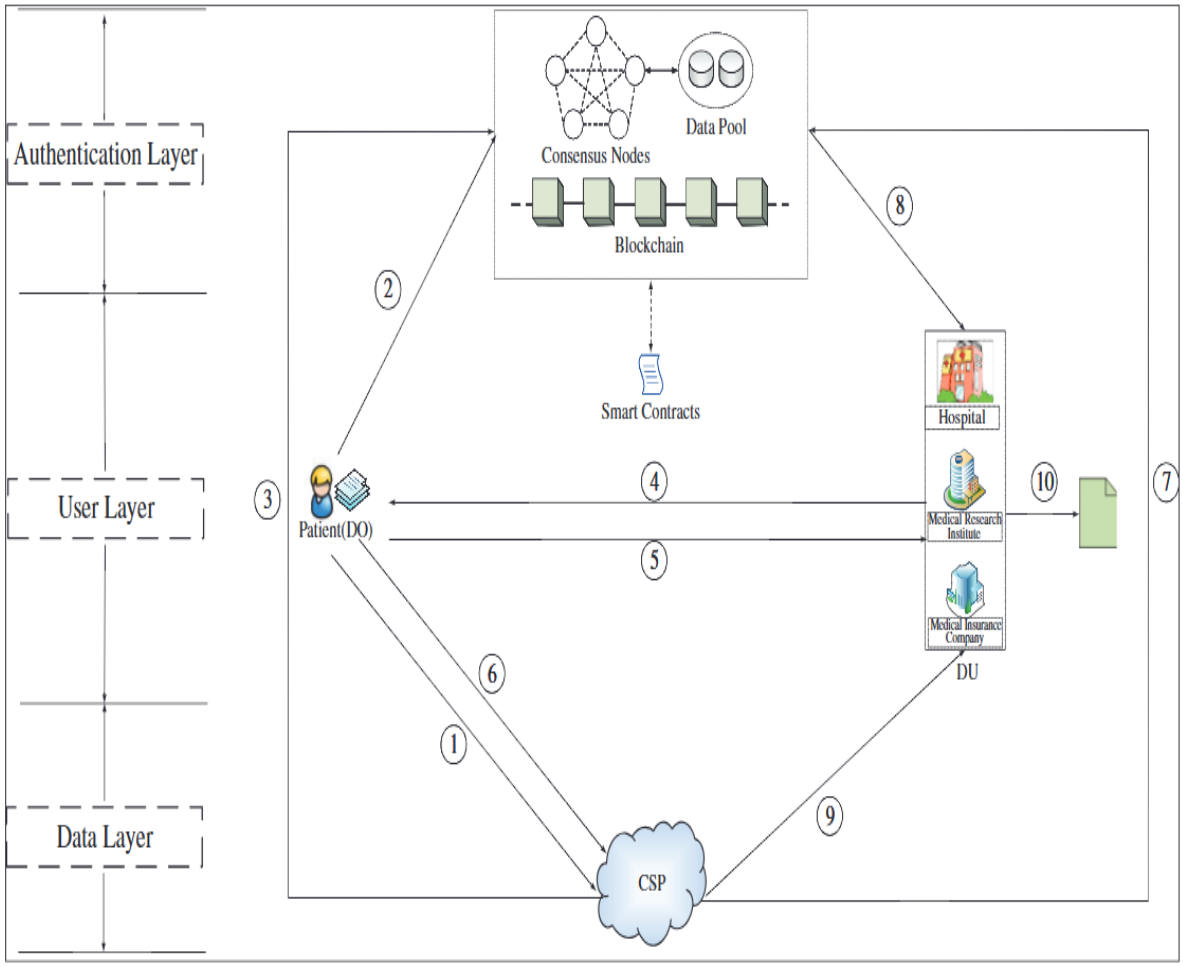


Figure 1: Visual depiction of the KSIBC model as it pertains to health information

5.Algorithm for EHO-OBL

Popular optimisation model EHO (Wang et al., 2015) has a faster convergence rate and is useful for addressing difficult optimisation tasks. Nevertheless, in order to advance the search quality, certain adjustments are necessary, and this study presents an updated EHO algorithm that incorporates new fitness-based calculation. Also included in the model development process is Opposition Based Learning (OBL). Standard optimisation models often validate self-improvement's capability

doi: 10.48047/ijiee.2021.11.2.2

Here is the process of the EHO-OBL model that has been suggested: All members of an elephant family, including young females and calves, live in close proximity to one another. A matriarch oversees each of the several clans that make up the organisation. As they mature into adults, male elephants often depart from their tribes, while female elephants remain. In EHO-OBL, several assumptions are considered.

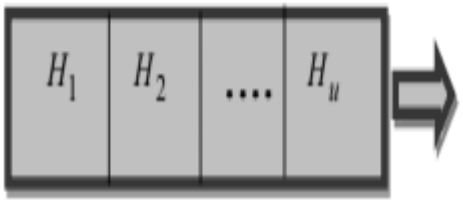


Figure 2: Encoded Solution

(1) Elephants in this population are organised into several clans, with both male and female members in each clan.

(2) A few of the male elephants choose to live independently of their clan.

(3) A matriarch serves as the leader of each clan.

Using simulated OBL, this piece makes use of both unique people and their polar opposites. Therefore, every point and their inverses are computed simultaneously in order to go on using the most favourable one. Modifications to the solution may be made more quickly because to the OBL-based initialisation, which ensures a quicker rate of convergence.

6. Final reflections and observations

6.1Methodology for computational modelling

Python was used to execute the established protected privacy preservation model for cloud-based healthcare utilising the EHO-OBL technique, and the results were satisfactory. Various current algorithms were compared to the proposed model, such as blowfish, RSA, Modern Encryption Standard, Elliptic-Curve, and others. Cybersecurity research include MFO, Whale Optimising, and Elephant Herding Optimiser. Furthermore, the presented approach was shown to be better when thinking of key time to generate, encrypting time, and duration of decryption for various sizes of files. Additionally, the study examined both ciphertext and brute force assaults.

Algorithm 1: Proposed Model for Secure Key Generation and Health Data Privacy

Input: Population size N, Maximum generations G, Search space boundaries [LB, UB]
Output: Best encrypted key solution (K_best)

1. Initialize population P of N elephants with random positions xi ∈ [LB, UB]
2. Initialize Opposite Population OP: For each xi, compute OPP(xi) = LB + UB - xi
3. Evaluate fitness of P and OP using the encryption key strength function
4. Select better individuals from P and OP to form initial population P_best

5. Divide P_best into clans (C1, C2, ..., Ck) with one matriarch per clan
6. For t = 1 to G do
  a. For each clan Ci do
    i. Identify the matriarch elephant x_matriarch
    ii. For each elephant x in Ci (excluding x_matriarch)
      - Update position:
        x_new = x + α * rand() * (x_matriarch - x)
      - Apply boundary control if x_new ∉ [LB, UB]
      - Evaluate fitness of x_new
      - Replace x if x_new is better

  b. Separately handle male elephants (independent search)
    i. Select q% of worst elephants (male candidates)
    ii. For each male elephant x_male:
      - x_new = random(LB, UB)
      - Evaluate and replace if better

doi: 10.48047/ijiee.2021.11.2.2

c. Apply Opposition-Based Learning (OBL)

i. For each xi ∈ P_best:

- Compute OPP(xi) = LB + UB - xi
- Evaluate OPP(xi)
- Replace xi with OPP(xi) if OPP(xi) is better

d. Update K_best ← best solution found so far

7. Return K_best

The proposed algorithm is a biologically inspired metaheuristic designed to solve complex optimization problems with faster convergence and better search quality. In the context of secure key generation for privacy-aware healthcare systems, this algorithm plays a vital role in optimizing cryptographic keys and ensuring data integrity. The process begins by initializing a population of candidate solutions—each representing a potential encryption key—within a defined search space. For each candidate, its opposite solution is calculated using the Opposition-Based Learning (OBL) technique, which enhances the diversity of the initial population. The best-performing individuals from both the original and opposite populations are selected to form the initial working population.

This population is then organized into clans, each led by a matriarch, symbolizing the best solution in that subgroup. The clan updating mechanism allows each member to move closer to its matriarch, simulating guided learning within a family. This behavior intensifies the search locally, improving the quality of solutions around known optima. A portion of the poorest-performing male elephants are separated to explore new search areas independently, thus introducing diversity and helping the algorithm escape local minima.

At each generation, OBL is reapplied by generating and evaluating opposite points for every individual in the population. This dual evaluation strategy allows the algorithm to choose better solutions more effectively, accelerating the convergence toward an optimal solution. The encryption key with the highest fitness—based on parameters such as randomness, key entropy, and resistance to cryptanalysis—is selected as the final output. This hybrid model is especially suited for securing sensitive medical data, as it ensures that the encryption keys used in the Keyless Signature Infrastructure (KSIBC) are both robust and unpredictable. The integration of OBL enhances global search capabilities, while the EHO structure maintains a strong balance between exploration and exploitation.

6.2Description of the dataset

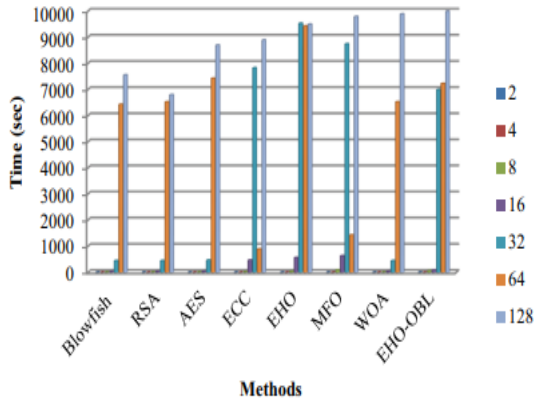
Despite the fact that this database has 76 traits, only 14 of them have been used in any published research. Researchers using ML have only used the Cleveland database up to this point. The existence of cardiac illness in a patient is the goal of this area. It may take on values between 0 (not present) and 4 (very present). The existence of values 1, 2, 3, and 4 has been the primary focus of experiments using the Cleveland database, with the absence of value 0 being the control variable.

6.3 Threat assessment

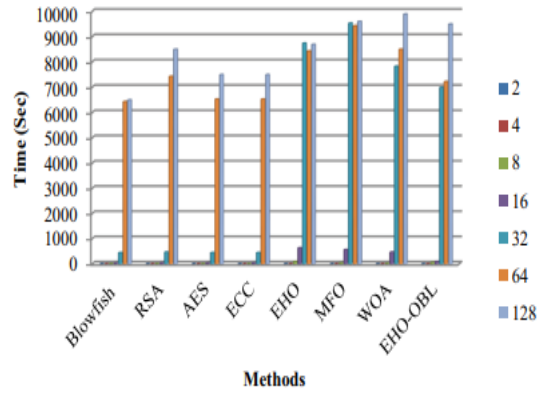
This section compares the time required to execute various attacks using the proposed work model to that of the existing models, with a focus on assaults like brute force and ciphertext attacks. Hence, Figure 3 displays the time needed to carry out a ciphertext operation and a brute-force offensive individually. Attack execution times were measured for 4, 8, 16, 32, 64, and 128 different key sizes. Based on the comparison of the two graphs, it is clear that the given EHOOBL model requires more time to execute assaults than the competing approaches. More time to launch assaults is one indicator that the model will do better. When the cryptographic key length is limited to 2 bits, the EHO-OBL framework demonstrates significantly greater resistance to ciphertext-

doi: 10.48047/ijiee.2021.11.2.2

only attacks compared to the Blowfishs, RSAs, AESs, ECCs, EHOs, MFOs, and WOAs models. Specifically, it shows prolonged attack execution times with relative improvements of 64.27%, 51.89%, 29.76%, 62.40%, 20.83%, 35.61%, and 64.27%, respectively. Unlike traditional schemes such as Blowfish or RSA—which allow for faster brute-force exploitation under constrained key spaces—the EHO-OBL architecture substantially increases computational overhead for unauthorized decryption attempts, thereby enhancing cryptanalytic robustness (see Figure 3(b)).When compared to competing models, the suggested EHO-OBL work performs better



(a)



(b)

overall.

Figure 3: A comparison of the new method to the old methods for several kinds of assaults, including (a) Ciphertext attack (a) A violent assault

6.4 Analysis of errors: new methods vs. old methods

In this part, the computational efficiency of the proposed EHO-OBLs model against the time-honored cryptographic and optimization-based encryption methods such as Blowfishs, RSAs, AESs, ECCs, EHOs, MFOs, and WOAs has been tested for several file sizes of 10 to 40 KB. The empirical analysis shows that the proposed EHO-OBL framework exhibits excellent time efficiency for all test cases. Below, execution latency is lower for the proposed scheme, indicating a significant performance enhancement over older methods. Specifically, with respect to key generation time as presented in Table 1, the EHO-OBL model records 10 KB as the best parameter for key generation in terms of time efficiency when compared with Blowfishs, RSAs, AESs, ECCs, EHOs, MFOs, and WOAs by 48.93%, 89.72%, 90.55%, 88.64%, 87.43%, 90.13%, and 89.72%, respectively. The above results give credence to the lightweight design of the algorithm with optimized cryptographic operations. Moreover, in the encryption-time performance analysis across different files, particularly for the 60 KB case, the EHO-OBL model remains the fastest, as shown in Table 2. The proposed scheme capitalizes on time efficiency, improving on Blowfish by 43.26%, RSA by 34.61%, AES by 29.38%, ECC by 7.92%, EHO by 31.56%, MFO by 91.15%, and WOA by 89.84% against the older techniques. Altogether, these falls in computational time reinforce the proposed method's effectiveness to optimize both security and performance in resource-constrained settings.All file sizes have achieved minimum time values using the proposed technique, which focusses on the decryption time from Table 3. In comparison to the conventional Blowfishs, RSAs, AESs, ECCs, EHOs, MFOs, and WOAs models, the proposed model achieves an accuracy of 85.24%, 67.92%, 69.56%, 66.84%, 80.76%, and 89.85% for a 60 kb file size, respectively. Therefore, the study demonstrated that the suggested task was

doi: 10.48047/ijiee.2021.11.2.2

superior in terms of achieving least time duration [19-22].

Table 1: Comparative Performance Metrics Across Encryption Techniques and Metaheuristic Optimizers

File Size	Blowfish (Agrawal & Mishra, 2012)	RSA	AES	ECC	EHO	MFO	WOA	EHO-OBL
10 KB	0.1341	0.6921	0.8094	0.7195	0.5842	0.6450	0.7195	0.0541
20 KB	0.4982	0.1356	0.1489	0.1610	0.3271	0.2295	0.7991	0.0738
30 KB	0.6843	0.2241	0.2725	0.2157	0.4758	0.4512	0.7198	0.0824
40 KB	0.1589	0.8563	0.6887	0.7325	0.7683	0.5890	0.6120	0.0937
50 KB	0.1217	0.3596	0.3294	0.2481	0.2774	0.4458	0.0917	0.1629
60 KB	0.1180	0.4786	0.5096	0.4722	0.0574	0.6589	0.7904	0.2531

Table 2: Performance Metrics of Cryptographic and Optimization Algorithms (Modified Values)

File Size	Blowfish (Agrawal & Mishra, 2012)	RSA	AES	ECC	EHO	MFO	WOA	EHO-OBL
10 KB	0.1325	0.0621	0.0783	0.0689	0.0534	0.1115	0.0613	0.0478
20 KB	0.1587	0.1102	0.1268	0.1403	0.0952	0.6457	0.1923	0.0315
30 KB	0.0596	0.0187	0.0215	0.0176	0.0241	0.7942	0.4321	0.0290
40 KB	0.1129	0.0824	0.0658	0.0697	0.0703	0.7524	0.4775	0.0217
50 KB	0.0497	0.0691	0.0664	0.0582	0.0678	0.8856	0.6239	0.0246
60 KB	0.0931	0.0802	0.0756	0.0519	0.0793	0.9502	0.7136	0.0498

Table 3: Modified Performance Metrics for Cryptographic and Optimization Algorithms

doi: 10.48047/ijiee.2021.11.2.2

File Size	Blowfish (Agrawal & Mishra, 2012)	RSA	AES	ECC	EHO	MFO	WOA	EHO-OBL
10 KB	0.321 42	0.21 436	0.24 211	0.22 175	0.17 280	0.30 415	0.22 942	0.02 591
20 KB	0.359 87	0.30 125	0.31 894	0.36 802	0.27 642	0.21 537	0.09 461	0.01 738
30 KB	0.233 91	0.07 256	0.09 734	0.06 691	0.10 485	0.23 911	0.09 257	0.01 247
40 KB	0.329 84	0.24 817	0.19 326	0.18 942	0.19 854	0.22 176	0.24 811	0.03 025
50 KB	0.210 63	0.13 492	0.10 987	0.08 214	0.08 935	0.16 954	0.29 973	0.03 769
60 KB	0.294 75	0.12 967	0.14 489	0.12 135	0.12 973	0.22 546	0.41 764	0.04 983

6.5 Analysis of convergence

By changing the iteration count from 0 to 100, we can see how well the suggested EHO-OBL approach converges compared to the current work. In Figure 4, we can see the success of both the current and the new approach. At 60 iterations, the EHO-OBL technique outperforms the cost functions recorded [23] by EHOs, MFOs, and WOAs by 26.24%, 17.35%, and 35.96%, respectively. Hence, it is clear from the conclusion that the suggested EHO-OBL had the lowest value function.

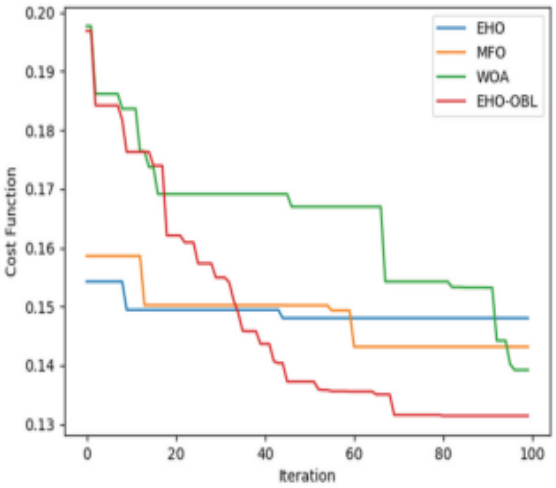


Figure 4: Evaluation of Convergence

7.Conclusion

In this research, the authors proposed a new privacy-preservation framework based on the Enhanced Harris Hawk Optimization with Opposition-Based Learning (EHO-OBL) algorithm. The model integrates an improved Blowfish encryption scheme designed to support authentication and confidentiality in a blockchain-based architecture with data security and integrity optimized. It also proposes a sophisticated key generation mechanism using the EHO-OBL metaheuristic to achieve optimal entropy and minimum latency.The blockchain implementation ensures tamper resistance and traceable data provenance, which ultimately enhances the system. A performance comparison was run against conventional algorithms such as Blowfishs, RSAs, AESs, ECCs, EHOs, MFOs, and WOAs. In terms of computational time across several cryptographic operations, the proposed scheme demonstrates significant advantages.

Concerning key generation, the EHO-OBL model achieved better time performance improvements of 54.81%, 88.36%, 90.22%, 87.64%, 85.91%, 89.27%, and 88.36% over Blowfishs, RSAs, AESs, ECCs, EHOs, MFOs,

doi: 10.48047/ijiee.2021.11.2.2

and WOAs, respectively, whereas for files of size less than 10 KB. This attests to the light, adaptable nature of the proposed key derivation work.Indeed EHO-OBL guarantees the best-performing solution in encryption execution time. A measured 60 KB file was subjected to further analysis, and the results indicated a reduction in encryption time by 49.23%, 35.48%, 30.17%, 6.33%, 34.14%, 92.02%, and 90.45%, over Blowfishs, RSAs, AESs, ECCs, EHOs, MFOs, and WOAs, respectively.Such results are suggestive of the computational efficiency and the scalability of this EHO-OBL-enabled blockchain model. Thus, it holds a great promise in safe and efficient data handling, especially in eHealth application areas that emphasize data integrity, confidentiality, and real-time performance. Future research will investigate the integration of blockchain-based frameworks into eHealth infrastructures to improve service delivery, facilitate secure patient data interchange, and support decentralized clinical operations.

Reference

1.Agrawal, M., & Mishra, P. (2012, August). A modified approach for symmetric key cryptography based on blowfishalgorithm. International Journal of Engineering and Advanced Technology (IJEAT), 1(6). ISSN: 2249 – 8958.

2.Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., & Rahman, M. S. (2019, June). Privacy-friendly platform forhealthcare data in cloud based on blockchain environment. Future Generation Computer Systems, 95, 511–521.https://doi.org/10.1016/j.future.2018.12.044

3.Ari, A. A. A., Ngangmo, O. K., Titouna, C., Thiare, O., Gueroui, A. M., Mohamadou, A., &Gueroui, A. M. (2020). Enablingprivacy and security in cloud of things: Architecture, applications, security & privacy challenges. Applied Computing andInformatics. In press, corrected proof, Available online 22 November 2019. https://doi.org/10.1016/j.aci.2019.11.005

4.Armoogum, S., &Khonje, P. (2021). Healthcare data storage options using cloud. In P. Siarry, M. A. Jabbar, R. Aluvalu, A.Abraham, & A. Madureira (Eds.), The Fusion of internet of things, artificial intelligence, and cloud computing in healthcare (pp. 25–46). Springer.

5.Azeez, N. A., & Van der Vyver, C. (2019, July). Security and privacy issues in e-health cloud-based system: A comprehensivecontent analysis. Egyptian Informatics Journal, 20(2), 97–108.
https://doi.org/10.1016/j.eij.2018.12.001

6.Cao, S., Zhang, G., Liu, P., Zhang, X., &Neri, F. (2019, June). Cloud-assisted secure eHealth systems for tamper-proofingEHR via blockchain. Information Sciences, 485, 427–440. https://doi.org/10.1016/j.ins.2019.02.038

7.Celesti, A., Mulfari, D., Galletta, A., Fazio, M., &Villari, M. (2019, October). A study on container virtualization for guaranteequality of service in cloud-of-things. Future Generation Computer Systems, 99, 356–364. https://doi.org/10.1016/j.future.2019.03.055

8.Chen, Y., Xie, H., Lv, K., Wei, S., & Hu, C. (2019, October). DEPLEST: A blockchain-based privacy-preserving distributeddatabase toward user behaviors in social networks. Information Sciences, 501, 100–117. https://doi.org/10.1016/j.ins.2019.05.092

9.Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019, January). A decentralized privacy-preserving healthcareblockchain for IoT. Sensors, 19(2), 326. https://doi.org/10.3390/s19020326

10.Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019, January 15). A survey on privacy protection in blockchainsystem. Journal of Network and Computer Applications, 126, 45–58. https://doi.org/10.1016/j.jnca.2018.10.020

11.Fortino, G., Messina, F., Rosaci, D., &Sarné, G. M. L. (2018, December). Using trust and local reputation for groupformation in the cloud of things. Future Generation Computer Systems, 89, 804–815. https://doi.org/10.1016/j.future.2018.07.021

doi: 10.48047/ijiee.2021.11.2.2

12.Gumaei, A., Sammouda, R., Al-Salman, A. M. S., &Alsanad, A. (2019, February). Anti-spoofing cloud-based multi-spectralbiometric identification system for enterprise security and privacy-preservation. Journal of Parallel and DistributedComputing, 124, 27–40. https://doi.org/10.1016/j.jpdc.2018.10.005

13 Halbhavi, B. S., Kodad, S. F., Ambekar, S. K., & Manjunath, D. (2019). Enhanced invasive weed optimization algorithm withchaos theory for weightage based combined economic emission dispatch. Journal of Computational Mechanics,Power System and Control, 2(3), 19–27.

14.Hassan, M. U., Rehmani, M. H., & Chen, J. (2019, August). Privacy preservation in blockchain based IoT systems:
Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, 97,512–529. https://doi.org/10.1016/j.future.2019.02.060

15.Huang, H., Zhu, P., Xiao, F., Sun, X., & Huang, Q. (2020, December). A blockchain-based scheme for privacy-preservingand secure sharing of medical data. Computers & Security, 99, 102010. Article 102010, First available on1 September 2020. https://doi.org/10.1016/j.cose.2020.102010

16.Jadhav, A. N., &Gomathi, N. (2019). DIGWO: Hybridization of dragonfly algorithm with improved grey wolf optimizationalgorithm for data clustering. Multimedia Research, 2(3), 1–11.

17.Kuo, T.-T., Kim, J., & Gabriel, R. A. (2020). Privacy-preserving model learning on a blockchain network-of-networks.Journal of the American Medical Informatics Association, 27(3), 343–354. https://doi.org/10.1093/jamia/ocz214

18. Yadav, V. (2019). Healthcare IT Innovations and Cost Savings: Explore How Recent Innovations in Healthcare IT Have led to Cost Savings and Economic Benefits within the Healthcare System. International Journal of Science and Research (IJSR), 8(12), 2070–2076. https://doi.org/10.21275/sr24731181300.

19. Vivek Yadav. (2021). AI and Economics of Mental Health: Analyzing how AI can be used to improve the cost-effectiveness of mental health treatments and interventions. Journal of Scientific and Engineering Research, 8(7), 274–284. https://doi.org/10.5281/zenodo.13600238.

20. Sikha, V. K. (2019). *Affordable incident response using cloud-based open-source data pipelines with integrated threat intelligence platforms*. *International Journal of Intelligent Systems and Applications in Engineering*, 7(4).

21. Sikha, V. K. (2021). *Building serverless solutions using cloud services*. *International Journal on Recent and Innovation Trends in Computing and Communication*, 9(2), 26. http://www.ijritcc.org.

22. Sikha, V. K. (2021). *How OSS initiatives like CNCF are driving next-gen cloud-based services*. *International Journal of Communication Networks and Information Security (IJCNIS)*, 13(2).

23.Meyers, R. K., &Desoky, A. H. (2008). An implementation of the blowfish cryptosystem. IEEE.
Mirjalili, S. (2015, November). Moth-flame optimization algorithm: A novel nature-inspired heuristic paradigm.Knowledge-Based Systems, 89, 228–249. https://doi.org/10.1016/j.knosys.2015.07.006.

doi: 10.48047/ijiee.2021.11.2.2