



International Journal of Cloud Computing

ISSN online: 2043-9997 - ISSN print: 2043-9989

<https://www.inderscience.com/ijcc>

An enhanced two-level data sanitisation and elliptic curve cryptography encryption model for securing electronic healthcare data in a hybrid cloud platform

V. Ambica, A. Viji Amutha Mary

DOI: [10.1504/IJCC.2025.10070159](https://doi.org/10.1504/IJCC.2025.10070159)

Article History:

Received:	11 August 2023
Last revised:	02 December 2023
Accepted:	04 December 2023
Published online:	11 April 2025

An enhanced two-level data sanitisation and elliptic curve cryptography encryption model for securing electronic healthcare data in a hybrid cloud platform

V. Ambica*

Computer Science and Engineering,
Sathyabama Institute of Science and Technology,
Chennai, Tamil Nadu 600119, India

and

Vignana Bharathi Institute of Technology,
India

Email: venna.ambica@gmail.com

*Corresponding author

A. Viji Amutha Mary

Sathyabama Institute of Science and Technology,
Chennai, Tamil Nadu 600119, India

Email: vijiamuthamary.cse@sathyabama.ac.in

Abstract: A secure framework for storing EHR in the hybrid cloud platform is implemented. At first, the required medical data is gathered from the database of the hospitals and split into sensitive and insensitive parts. The sensitive part is first encrypted with the data sanitisation method. The keys obtained are optimally chosen by the modified uniform number-based red fox optimisation (MUN-RFO). Then, the insensitive part is encrypted by optimal key-based data encryption scheme (OKDES), in which the same MUN-RFO algorithm is utilised to choose the optimal keys. The sensitive and insensitive data is combined and stored in the Hybrid Cloud. From the result analysis, the cost function of the MUN-RFO-OKDES is lower by 0.022% of HBA-OKDES, 0.011% of DHOA-OKDES, 0.0025% of EFO-OKDES and 0.001% of RFO-OKDES at 5th iteration for dataset 2. Numerous simulations are carried out to prove the security provided by the given data storage model in a hybrid cloud.

Keywords: hybrid cloud platform; electronic healthcare data; optimal key-based data encryption scheme; OKDES; modified uniform number-based red fox optimisation; MUN-RFO; data sanitisation.

Reference to this paper should be made as follows: Ambica, V. and Mary, A.V.A. (2025) 'An enhanced two-level data sanitisation and elliptic curve cryptography encryption model for securing electronic healthcare data in a hybrid cloud platform', *Int. J. Cloud Computing*, Vol. 14, No. 1, pp.86–114.

Biographical notes: V. Ambica has completed her BE degree in Information Technology discipline in Maturi Venkata Subba Rao Engineering College in the year 2006 and MTech in Computer Science and Engineering discipline in Tirumala Engineering College in 2013. She is currently pursuing PhD in Computer Science and Engineering discipline in Sathyabama Institute of

Science and Technology and also working as an Assistant Professor in Vignana Bharathi Institute of Technology since 2014. She has published papers in journals and conferences. She has received awards for Teaching and Mentoring from various organisations. Her areas of interests include cryptography and network security, cloud computing and networking.

A. Viji Amutha Mary completed her BE degree in Computer Science and Engineering discipline in Dr. Sivanthi Aditanar College of Engineering in the year 2003 and MTech degree in Computer and IT discipline in Manonmaniam Sundaranar University in 2005. She completed her PhD in Computer Science stream in 2018 in Sathyabama Institute of Science and Technology. She is currently working as a Professor in Sathyabama Institute of Science and Technology since 2005. She has published around 100 papers in journals and conferences. She has published four books and around ten book chapters. She has currently four patents, three are granted and one in published state. She has received awards for teaching from various organisations. Her areas of interests include IoT, image processing, data structures, design and analysis of algorithms.

1 Introduction

The concept of maintaining confidentiality is complex and multifaceted in medical organisations (Liu et al., 2018). Electronic health record (EHR) gathers and preserves a variety of patient data, including confidential data about patients' conditions, medical interventions, and the outcomes of laboratory tests. EHRs are created and managed digitally inside the medical organisation or community (Anandkumar et al., 2022). Because of its sensitivity and possible 'legal and social' impacts on exposure, the shifting of EHR data to the cloud improves serious security issues (Marwan et al., 2018). E-health data covers private and sensitive information, including patient information and financial data like banking information and debit card information (Denis and Madhubala, 2021). The right to confidentiality is one of the public's fundamental rights in any country, and when it is broken, it can result in the revealing of personal patient information and economic damage (de Oliveira et al., 2020). Additionally, while considering both cloud computing and edge computing are presented in smart health with divergent security requirements. Here, a unique security issue has been recognised for cloud computing and edge computing-based smart health to attain cooperative privacy preservation for the respective wearable devices (Liu et al., 2019). The edge computing model depicts the interactions between diverse patients within the same place. The security and privacy challenges for wearable devices can be resolved with the help of edge computing models.

Numerous numbers of medical organisations adopt cloud platforms to strengthen the huge amount of EHR data (Ahmad et al., 2018b). Healthcare companies with no equipment can use the hybrid cloud for computing purposes. In the medical field, the patient's information is secured with the help of a hybrid cloud network (Hindistan and Yetkin, 2023). An enormous quantity of clinical and medical imaging data can be made available to third-party services by healthcare providers who desire to utilise their past technology but have few physical resources (Xu et al., 2018). In addition, the hybrid cloud creates privacy deficiencies for EHR data; therefore, it requires further safety precautions to protect the confidentiality of sensitive EHR data (Grover and Kushwaha,

2022). Security concerns arise due to the retention and exchange of EHR data via hybrid cloud computing. It has highlighted the requirement for a comprehensive security system based on maintaining confidentiality (Alphonsa and Amudhavalli, 2018). As access to EHRs is important for the quality of service and to enhance data occupancy, the privacy of cloud-based EHRs is considered essential.

The EHRs' data is encrypted before being sent to the cloud to maintain privacy (Boava and Iano, 2016). Traditional cryptographic methods are highly computational, require complex key management systems, and depend on the public key infrastructure (PKI), making them not affordable for cloud-based EHR data storage (Li et al., 2015). However, homomorphic encoding is a strong cryptographic technique that can be used in this situation; yet, it is costly in terms of computation. Secure processing is not suitable for the versatile use of EHRs because it is inefficient and impractical for some procedures (Yuan et al., 2018). The EHR data can be accessed with the help of different access control protocols. However, security precautions are unable to be employed directly in the cloud due to the scale and versatility of asset management (Zhang et al., 2018). Recently, many kinds of medicinal applications, particularly actual-time health surveillance for insurance purposes, identifying illnesses, and the evaluation of medical data, have been introduced as significant uses of health clouds. Sometimes, an unreliable third party maintains the data rather than the original data owner (Dai et al., 2020). As a result, the probability of several cloud security breaches has increased. There are numerous access control methods available to stop these attacks (Shin et al., 2022). In spite of effective access control measures, there are numerous instances where an approved user may identify sensitive information (Tao et al., 2022). In order to safeguard individual confidentiality, cloud databases need to use inference control techniques. Hence, the cloud-based EHR encryption system is proposed in this work.

The contribution of the developed cloud-based EHR security system is portrayed in upcoming sections.

- To implement the cloud-based EHR security system to secure the sensitive and insensitive part of the EHR data to prevent the leakage of EHR data in the social era and to prevent the hacking of data from unauthorised persons.
- To encrypt the sensitive part of the EHR data, the data sanitisation method is proposed. In this system, the optimal key is developed with the help of the offered modified uniform number-based red fox optimisation (MUN-RFO) algorithm, and this algorithm is also used to optimise the binary format key to lower the computation time and memory size and to enhance the preservation and hiding ratio during the encryption process.
- To encipher the insensitive part of the EHR data, the ECC is developed, and in this system also, the encryption process is done by the optimal key generated by the proposed MUN-RFO algorithm. The developed MUN-RFO algorithm is used to optimise the generated key to lower the time and memory size in the enciphering process.
- The resultant outcome achieved by the developed MUN-RFO-OKDES-based two-level EHR security system is compared with the old EHR security system to evaluate the accurateness of the developed security system.

The organisation of the MUN-RFO-OKDES-based two-level EHR security system is structured as follows. In Section 2, the several existing EHR security system and their advantages and disadvantages are shown in detail. Section 3 depicts the healthcare data management in cloud architecture, and the collection of EHR is shown in a brief manner. Section 4 presents the data sanitisation, and sensitive data encryption using the optimised key and the developed MUN-RFO algorithm. In Section 5, ECC with optimal key for encrypting insensitive data and data uploading in the cloud is formulated in detail. The outcome and the discussion of the explored MUN-RFO-OKDES-based two-level EHR security system are depicted in Section 6. The conclusion of the explored MUN-RFO-OKDES-based two-level EHR security system is portrayed in Section 7.

2 Literature survey

2.1 Related works

In 2018, Yang et al. developed a Med share-based cloud system to prevent the interoperability problems caused by clinicians. The proposed system was used to encrypt the sensitive details of the patients from hacking activities. The secret details of patients were also controlled with the help of the Med share system. By using the developed model, the sensitive details of the patients could be shared with another person without any effusion issues. It provided two-step authentications on sensitive details of the patients. To this end, the proposed system was compared with various techniques to prove its effectiveness.

In 2021, Kanwal et al. have implemented a privacy preservation system using cloud environments. The researchers identified the internal structure of the medical data by using the proposed system. The EHR data from the hospital management was shared with the assistance of the developed privacy-preserving extensible access control markup language (XACML)-based access control model (PPX-AC) system. Moreover, the security attacks were less in the proposed approach in comparison with the traditional techniques. Here, the security attacks in the developed model were identified with the help of high-level Petri nets (HLPN). At last, the proposed system was correlated with the various privacy preservation techniques to determine the efficacy of the developed model.

In 2021, Pachala et al. offered a multi-cloud system in the cloud environment to enhance the privacy of medical data. In this system, the failures presented by the cloud data were determined with the help of the Byzantine technique. The encryption and decryption of data in the cloud environment were enhanced with the assistance of DepSky architecture. At last, the storage of data after the encryption process was controlled with the help of Shamir's secret sharing technique. Lastly, the performance of encryption, decryption, and data storage of the proposed system was compared with the ancient techniques to validate the efficacy of the developed model.

In 2019, Liu et al. implemented a cooperative privacy preservation system for encrypting medical data. This system was mainly adopted in space-aware and time-aware contexts for monitoring the data authentication system. The MinHash-based authentication system was developed for space-aware edge computing mode to enhance the efficiency of the data preservation process. Further, the fine-grained access control

system was implemented by time-aware cloud computing mode. Finally, the accuracy of the developed system was determined by comparing it with the traditional techniques.

In 2019, Kundalwal et al. put forth hybrid privacy preservation techniques to offer enhanced protection for medical data. Here, the privacy of the individual was verified by the two techniques, such as k-anonymity and query set size restriction. The attack that occurred on the sensitive data was prevented by the query set size restriction technique. The linking attacks that occurred in the medical data could be restricted by the k-anonymity system. The privacy of the data could be enormously increased by adopting the above two techniques because they follow a set of rules for privacy preservation. At last, the proposed system was compared with the various privacy preservation techniques in order to determine its effectiveness.

In 2020, Abirami and Bhanu recommended a crypto-deep neural network for securing and sharing medical data with another person. Here, the impersonation attack presently in the medical data was identified with the help of crypto-deep neural network cloud security (CDNNCS). The proposed network was comprised of various parts like a cloud agent, cloud server, data centre, and web server for performing the encryption operation. The proposed system utilised the linear algebraic equation system for encrypting the data in the cloud environment. Finally, the efficacy of the developed system was analysed in terms of delay, jitter, throughput, and goodput, and it was proved that the performance of the developed model was better than classical techniques.

In 2018a, Ahmad et al. developed an outsourced encryption policy based on cipher text attributed policy (OS-ABE), and it was used to determine the computational tasks during the enciphering and deciphering process. Here, the sensitive data could be shared with the corresponding person and clinicians without any leakage. Here, the anonymity server was adopted to prevent the attacks caused on the medical data. The experimental outcome revealed that the formal security of the developed model was superior to the existing techniques and algorithms.

In 2021, Kumar and Prabhudeva invented dual-layer security that secured medical data from unauthorised users. Initially, the anonymity attack was prevented by a strong authentication system embedded in the proposed network. After that, the lightweight encipher process was adopted to encipher the medical data. After that, the encrypted data was synchronised with the help of a data-reduplication mechanism so the medical data could be highly secured without any information loss. Finally, analysis was carried out on the developed model, and it showed the computational time of the developed model was lower than the classical techniques. Moreover, the time needed to encipher and decipher the data was very low in the proposed system in comparison with the classical techniques.

2.2 *Problem statement*

The cryptography schemes used to prevent healthcare data in a hybrid cloud platform are usually expensive and require complex key management keys. Also, the time required and processing of the data in advanced cryptography schemes may be intensive, and there is a possibility of the inclusion of noise in the actual data, so the accuracy of the shared data may become less. So, an efficient way to preserve the patient's confidential information in the hybrid cloud platform is essential. The advantages and disadvantages of the existing security policies for sharing medical data in a hybrid cloud are provided in Table 1. The MedShare (Yang et al., 2018) model is highly dependable and scalable. It

helps in sharing medical information among various health providers, along with preventing the privacy of the patient. However, the implementation expense of this method is high. PPX-AC, MR-MSA-ANGLE, and policy anonymisation (Kanwal et al., 2021) show good performance regarding access control parameters. It gives fine-grained access control. But, the anonymisation may lead to the induction of noise into the data. DepSky, BFTMCD, and Shamir secret sharing (Pachala et al., 2021) show enhanced performance regarding the time required for decryption, the time required for encryption, utilisation of memory, and the average of precision values. Yet, this method is not applicable to advanced access control protocols, thus compromising its accuracy. CP-ABE, MinHash, and Bloom filter (Liu et al., 2019) models achieved a high rate of integrity and confidentiality. This method also provides high privacy protection, mutual authentication, and forward security. But, this method only handles the users in which the attributes are grouped as a single set, K-anonymity, and result set overlap restriction algorithm (Kundalwal et al., 2019) model prevents attacks like impersonation, inference, and linking attacks. The loss of information in this model is low. The processing time per tuple required by this model is lower than the conventional prevention methods. Yet, the process of maintaining the balance between the utilisation and protection of data is difficult. CDNNCS (Abirami and Bhanu, 2020) model achieves good communication with the best prevention and security. This model also enhances trust in the cloud environment. Yet, the dynamic behaviour of nodal communication is not considered in this model. The behavioural aspect of the user is also not considered in this work. CP-ABE (Ahmad et al., 2018a) verifies the trust of the crowd-sourcing participants, thus improving its privacy. This method gives enhanced protection while sharing the data. However, the quality of the data after sharing is distorted in this method. ACM-PPC (Kumar and Prabhudeva, 2021) method is cheaper, and the computational complexity in this model is less. This method also minimises the overhead of data with a lightweight encryption scheme. But, the privacy of the textual data alone is guaranteed by this method. So, an advanced privacy prevention scheme for preventing healthcare data while maintaining confidentiality needs to be developed for the hybrid cloud platform using advanced deep learning techniques aided by cryptography schemes.

2.2.1 Motivation based on the existing federated learning approaches

In Almadhor et al. (2023), need to analyse more details about the applications based on diverse smartphone devices. Additionally, it is not applicable to multiple datasets which can generate problems like privacy issues and a lack of data in the medical platform. In Khan et al. (2023a), it needs to estimate the statistical test of the recommended model which will help to ensure the effectiveness of the proposed algorithm. In Khan et al. (2023b), applying a large amount of data using artificial intelligence approaches in the medical platform is challenging work. In Menon et al. (2023), it is not applicable for the diverse large datasets. It needs to analyse more user input which will be utilised to keep the application focused on the patient. In the given research work, the author has developed intelligent techniques like MUN-RFO and optimal key-based data encryption scheme (OKDES) to resolve the above-mentioned issues. The simulation outcomes of the offered approach revealed it is statistically significant and also it has the ability to be applicable to large datasets. The performance improvements for the designed approach are helpful for healthcare applications like biological research, EHR administration, and medicine management.

Table 1 Features and challenges of existing privacy prevention schemes in hybrid cloud

<i>Author [citation]</i>	<i>Methodology</i>	<i>Features</i>	<i>Challenges</i>
Yang et al. (2018)	MedShare	• This model is highly dependable and scalable. • It helps in sharing medical information among various health providers, along with preventing the privacy of the patient.	• The implementation expense of this method is high.
Kanwal et al. (2021)	PPX-AC, MR-MSA-ANGLE, and policy anonymisation	• It shows good performance regarding access control parameters. • It gives fine-grained access control.	• The anonymisation may lead to the induction of noise into the data.
Pachala et al. (2021)	DepSky, BFTMCD, and Shamir's secret sharing	• It shows enhanced performance regarding the time required for decryption, the time required for encryption, utilisation of memory, and the average precision values.	• This method is not applicable to advanced access control protocols, thus compromising its accuracy.
Liu et al. (2019)	CP-ABE, MinHash, and Bloom filter	• This model achieved a high rate of integrity and confidentiality. • This method also provides high privacy protection, mutual authentication, and forward security.	• This method only handles the users in which the attributes are grouped as a single set.
Kundalwal et al. (2019)	k-anonymity, and ResultSet overlap restriction algorithm	• This model prevents attacks like impersonation, inference, and linking attacks. • The loss of information in this model is low. • The processing time per tuple required by this model is lower than the conventional prevention methods.	• The process of maintaining the balance between the utilisation and protection of data is difficult.
Abirami and Bhanu (2020)	CDNNCS	• This model achieves good communication with the best prevention and security. • This model also enhances trust in the cloud environment.	• The dynamic behaviour of nodal communication is not considered in this model. • The behavioural aspect of the user is also not considered in this work.

Table 1 Features and challenges of existing privacy prevention schemes in hybrid cloud (continued)

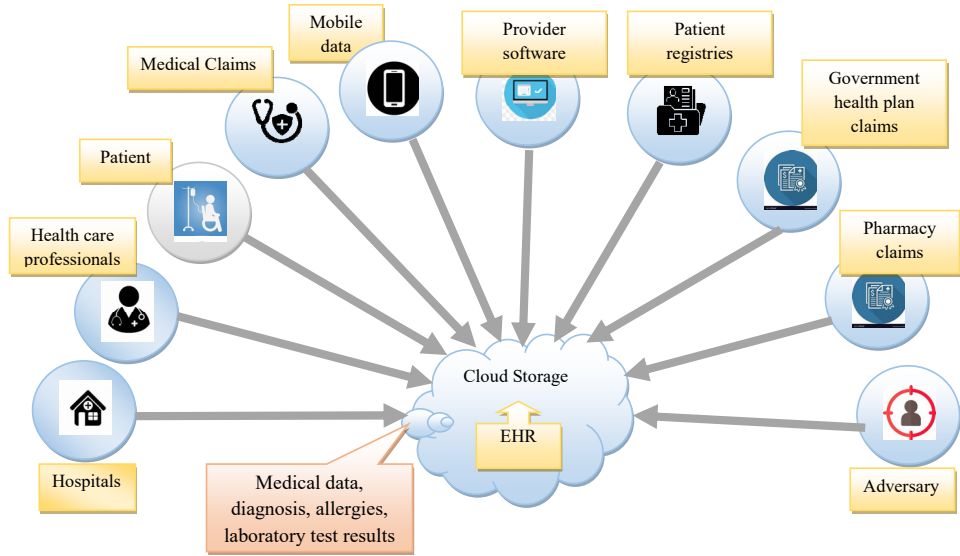
<i>Author [citation]</i>	<i>Methodology</i>	<i>Features</i>	<i>Challenges</i>
Ahmad et al. (2018a)	CP-ABE	• The trust of the crowd-sourcing participants is verified using this protocol, thus improving its privacy. • This method gives enhanced protection while sharing the data.	• The quality of the data after sharing is distorted in this method.
Kumar and Prabhudeva (2021)	ACM-PPC	• This method is cheaper, and the computational complexity in this model is less. • This method also minimises the overhead of data with a lightweight encryption scheme.	• The privacy of the textual data alone is guaranteed by this method.

3 Developed two level data encryption scheme to secure electronic healthcare data in a cloud platform

3.1 Healthcare data management in cloud architecture

EHR contains the medical data of the patients in an electronic form. The cloud system is considered as one of the most effective ways of storing EHR data in a cost-effective way. People from various countries can easily access the data stored in the various servers of the cloud. The amount of EHR data is increased in huge amounts due to the development of medical industries. Hence, there is a need to store this EHR data in a safe way in the cloud platform. Cloud architecture is used in worldwide for maintaining the healthcare details of patients. This structure can provide more medical conveniences to patients. The cloud system is taken for easy admittance and outsourcing of gathered data. The cloud system is composed of a large number of parts and some of the components like storage space, security system and management system, etc. Due to the usage of cloud architecture, the data stored in the cloud can be easily accessed. Additionally, the cloud architecture is adopted for log time storage purposes. The data stored in the cloud platform is divided into two types' confidential data and public data. This data is preserved by the access control system of the cloud platform. Moreover, this access control system is adapted to maintaining the confidential information of the patient from being stolen. The data stored in the cloud system is easily outsourced to the person situated in any region in the world. A detailed illustration of the healthcare data management in the cloud is depicted in Figure 1.

Figure 1 Detailed diagram of healthcare data management in the cloud (see online version for colours)



In the current environment, the healthcare data is enormously increased due to the huge development of the medical industry. Moreover, maintaining a huge amount of medical information in a manual way consumes more time. These challenges are overcome by the cloud architecture. In recent days, healthcare providers have preferred cloud architecture for storing the medical data of the patient, documentation, and easy retrieval process. Due to the usage of cloud systems, medical amenities are sufficiently provided to the patients without any time delay. In the cloud system, the sensitive and insensitive information of the patient, like laboratory test results, treatment to be carried out, and contact details, is stored for easy access. This cloud system is also used to maintain the medical details of the patients for a long period. But, it has certain security issues. The medical information stored in the cloud system may be highly prone to outflow and hacking issues and several types of cyber attacks. So, it is necessary to provide proper encryption to the information stored in the cloud architecture. More techniques are developed to provide security to the medical information stored in the cloud platform. But, the existing techniques take more time for the encryption and decryption process. Therefore, it takes more cost. To rectify these issues, a cloud-based two-level EHR security system is developed.

3.2 Collection of electronic healthcare data

Dataset 1 (Diabetes dataset)

The required EHR data are gathered from the link of '<https://www.kaggle.com/datasets/akshaydattatraykhare/diabetes-dataset> with access: 2023-6-25'. This dataset is obtained from the National Institute of Diabetes and Digestive and Kidney Diseases. By using this dataset, the diabetes disease present in the patient can be easily identified. For a huge database, several attributes are adapted to determine the diabetes diseases present in the woman's body.

The collected information from the standard benchmark dataset is signified as da_m^c , and $m = 1, 2, \dots, M$ here, m is the total amount of gathered data from the standard dataset.

3.3 Data splitting

The cloud system consists of several numbers of nodes. They gather the information from the patient, and consequently, they are stored in the cloud system. The gathered EHR data da_m^c is divided into two main parts sensitive data $da_m^{sensitive}$ and insensitive data $da_m^{insensitive}$. The sensitive data comprised information on the patient's personal details, treatment to be carried out, and laboratory test results of the patients. Moreover, the insensitive data comprised minor details of the patients like contact details, etc. Both parts of EHR must be enciphered in a safe manner for security purposes.

4 Level 1: optimal key-based data sanitisation algorithm for providing security by encrypting sensitive data

4.1 Data sanitisation

The data present in the cloud platform is hidden with the assistance of data sanitisation (Marwaha and Singh, 2019) techniques. So it restricts the usage of data from unethical persons. The sanitised data can be used for several actions like training, development and testing, etc. The sanitised data looks like the original data. But, here, some information is hidden for security purposes. Data sanitisation (Ahamad et al., 2020) follows some of the techniques to hide sensitive information, and they are discussed in underneath sections.

- Data masking: Here, the information present in the input data is replaced by the mask term, and they are signified as W .
- Swapping: Here, the row of the given input data is swapped by different content, but they are sought like original content that has been swapped from the given input data.
- Record shuffling: Here, the data situated in the column is swapped to the row. But it looks like original data.
- Number discrepancy: It is suitable only for numerical numbers. Here, the percentage of real value is calculated to replace the data present in the input value.

In all of the above techniques, binary conversion is adopted for the generation of key matrices and for cloud information. Here, the optimal key required to do this sanitisation process is done by the developed MUN-RFO algorithm. To get the sanitised data, the achieved binary data is sent to the XOR operation. The sanitised data produced from this process is depicted in equation (1).

$$Cr' = Cr + J_2 \quad (1)$$

Here, the innovative data is represented as Cr , and the sanitised data is signified as Cr' , the optimal key generated in this process is represented as J_2 . The enciphered data can be

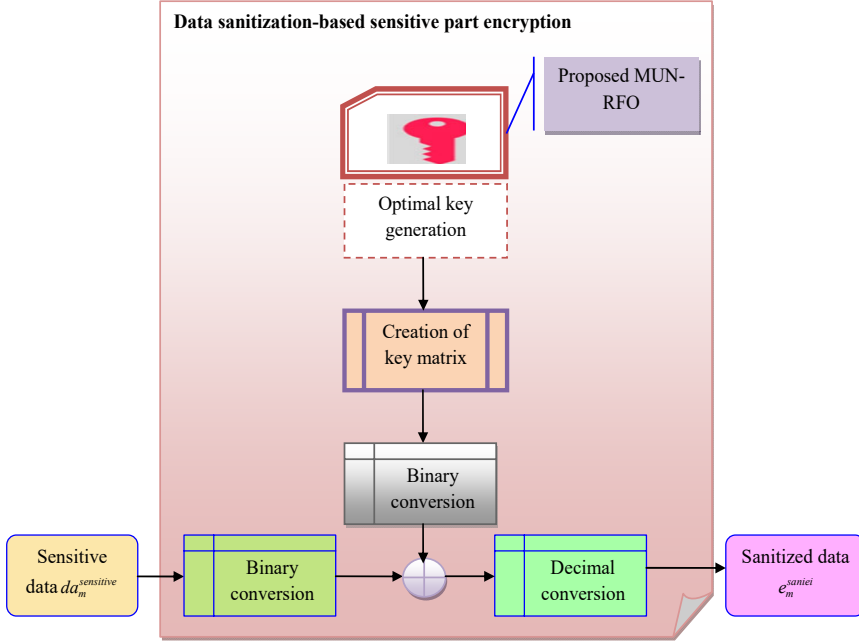
deciphered by the optimal key generated with the assistance of the proposed MUN-RFO algorithm.

$$\hat{Cr} = Cr' + J_2 \quad (2)$$

Here, the deciphered data is indicated as $\hat{Cr}$.

The schematic illustration of the data sanitisation for encrypting the sensitive data is shown in Figure 2.

Figure 2 Schematic illustration of the data sanitisation for encrypting sensitive data (see online version for colours)



4.2 Sensitive data encryption using optimised key

The sensitive part $da_m^{sensitive}$ of the EHR data contains information such as laboratory test details of the patient, personal information, type of treatment to be carried out, etc. The sensitive part of the EHR must be preserved from the unethical person. This data is encrypted with the help of the optimal key generated in the data sanitisation process. The optimal key is generated in data sanitisation by the developed MUN-RFO algorithm. The optimal key generated by the developed algorithm is used for encrypting the immense amount of EHR data. The encryption process is rapidly done by the optimal key generated in this process. Consequently, the enciphered data is deciphered by the same optimal key generated during the data sanitisation process. This method is useful for encrypting a huge amount of data. The enciphered data achieved from this process is denoted as e_m^{saniei} .

The objective function of a data sanitisation-based sensitive part encryption system using EHR is indicated in equation (3).

$$sen_{ob} = \arg \min_{\{J_2^{sani}\}} \left(\frac{comtime + memsize}{\frac{1}{preratio} + \frac{1}{hidratio}} \right) \quad (3)$$

Here, the key in the binary format created at the data sanitisation process is indicated as J_2^{sani} in $[0, 1]$. The computation time, memory size, preservation ratio, and hiding ratio in the data sanitisation process are signified as is *comtime*, *memsize*, *preratio* and *hidratio*. The expression to determine *comtime*, *memsize*, *preratio* and *hidratio* is formulated as follows:

$$memsize = \frac{\text{total count of memory bits}}{8} \quad (4)$$

$$preratio = \frac{\text{total count of zero index}}{\text{preserved data}} \quad (5)$$

$$hidratio = \frac{\text{total span of non-zero index}}{\text{total count of indexes}} \quad (6)$$

Computation time: The time consumed to finish the encryption process is represented as computation time.

4.3 Developed MUN-RFO

The developed MUN-RFO algorithm is adopted in data sanitisation and ECC for generating the optimal key, and this optimal key is used for enciphering and deciphering the data in data sanitisation and ECC techniques. The proposed MUN-RFO algorithm is used to optimise the key in both data sanitisation and ECC technique to preserve the sensitive and insensitive part of EHR data from unethical persons. The RFO is a heuristic-assisted meta-optimisation technique, and it is mainly adopted to determine the maximal and minimal test functions, and also it has a rapid convergence rate. But it does not provide satisfactory results for a huge volume of data. These limitations are defeated by the developed MUN-RFO algorithm. The main purpose of the proposed MUN-RFO algorithm is to reduce the time and memory size and to enhance the preservation ratio and the hiding ratio during the encryption process. The execution of the proposed MUN-RFO algorithm is noticeably dependent on the mean, best fitness, and uniform random number, and its value is stuck in the middle of $[0, 1]$. But, it does not give a satisfactory outcome so, the value of random is upgraded in the developed MUN-RFO algorithm, and it is expressed by equation (7).

$$k = \frac{100 \circ \text{mean } fi}{\text{bestfi}} \quad (7)$$

Here, the mean and the best fitness are indicated as *mean fi*, and *bestfi* respectively, the term *k* signifies the arbitrary random number.

Red fox optimisation (RFO) (Khorami et al., 2021)

This algorithm is designed on the basis of the hunting and escaping behaviour of red foxes. RFO is adopted to determine the solutions for optimal issues. Moreover, this algorithm is utilised to introduce the pseudo-optimal solution.

Inspiration

The red fox is an animal and it forages the wild and domestic animals for producing the food for its survival. Red foxes are omnivorous type animals, and they have slim legs and lengthy tails. These red fox species are considered as seems like dog species due to their body parts. The red fox animal can be able to live in all lifestyles and it is flexible to all nature. The red fox animal is distributed all around the world. The red fox rapidly hunts its food without considering any risk factors. The red fox animals live in a group and in a couple of manners. After reaching the required growth, the adult red foxes left the group and searched for a suitable pair for survival.

The RFO algorithm is a meta-optimiser algorithm and it is developed by the foraging characteristics of the red fox. The red fox follows some trick to hunt its target food. During the hunting process, the red fox animal conceals in a small scrub and slowly moves towards its target food, and abruptly attacks the prey. Here also, the exploitation and exploration phases are also considered in this algorithm. The creation of arbitrary individuals in RFO is formulated in equation (8).

$$Y = [y_0, y_1, \dots, y_{n-1}] \quad (8)$$

Thus, the count of the population is represented as i , at the iteration s , the term y_0 is described the term $(Y_i^h)^s$ and here, the size of the issue at search space is signified as i .

Here, the conditional function of the term Q is indicated as e , and here, the value of the attribute is signified as n , and it lies in between $[x, y]^n$.

$$Y^h = [(y_0)^h, (y_1)^h, \dots, (y_{n-1})^h] \quad (9)$$

Here, are the terms x, y belonging to Q .

The optimal global solution is recommended by the optimal solution developed by the term $e(Y^h)$.

The red fox forms a group on a particular land area based on the availability of food. Sometimes it is left from the group if the deficiency of food occurs.

$$C((Y^h)^s, (Y_{bt})^s) = \sqrt{(Y^h)^s - (Y_{bt})^s} \quad (10)$$

The displacement of all red foxes present in the population is achieved by equation (11).

$$((Y^h)^s) = ((Y^h)^s) + \ell \circ \text{sgn}(((Y_{bt})^s) - ((Y^h)^s)) \quad (11)$$

Here, the random number is represented as ℓ .

Thus, the best solution is achieved by changing the position of red foxes. The fog tries to kill the target prey after the catching process. Here, the red fox tries to move toward the prey, causing an unexpected attack. The exploitation phase of this algorithm is determined by the random value q in $[0, 1]$, and it is signified by equation (12).

$$\begin{cases} \text{reaches near to prey} & \text{if } q > 3/4 \\ \text{hide position} & \text{if } q > 3/4 \end{cases} \quad (12)$$

The displacement of the individual red foxes is identified by cochlear expression.

The radius of the red fox team is used to identify the stipulations of the RFO algorithms. The radius of the team considers the random value x and variable for determining the stipulation of the RFO, and they are stuck in the middle of $[0, 0.2]$ and $[0, 2\pi]$ correspondingly.

$$q = \begin{cases} x \circ \frac{\sin(\Phi)}{\Phi} & \text{if } \Phi \neq 0 \\ H & \text{if } \Phi = 0 \end{cases} \quad (13)$$

Here, the random value is portrayed as H in $[0, 1]$. Thus, the whole population of the red fox team near the target food is arithmetically signified in equation (14).

$$\begin{cases} y_0^{new} = x \circ q \circ \cos(\Phi_1) + y_0^{act} \\ y_1^{new} = x \circ q \circ \sin(\Phi_1) + x \circ q \circ \cos(\Phi_2) + y_1^{act} \\ y_1^{new} = x \circ q \circ \sin(\Phi_1) + x \circ q \circ \sin(\Phi_2) \\ \quad + x \circ q \circ \cos(\Phi_3) + y_2^{act} \\ \quad \vdots \\ y_{n-1}^{new} = x \circ q \circ \sum_{j=1}^{n-2} \sin(\Phi_j) + x \circ q \circ \cos(\Phi_{n-1}) + y_{n-2}^{act} \\ y_{n-1}^{new} = x \circ q \circ \sin(\Phi_1) + x \circ q \circ \sin(\Phi_2) \\ \quad + \dots x \circ q \circ \sin(\Phi_{n-1}) + x \circ q \circ \sin(\Phi_{n-1}) + y_{n-x}^{act} \end{cases} \quad (14)$$

From the above population, new fox members are replaced instead of poor fox members. After the addition of new members to the above population, the optimal member is elected, and they are represented as $(Y(1))^s$, and $(Y(2))^s$ respectively. The centre of the field is calculated by equation (15).

$$G_b^s = \frac{1}{2} \left((Y(1))^s - (Y(2))^s \right) \quad (15)$$

The diameter of the field is determined by Euclidean distance, and it is evaluated by Eq. (16).

$$G_c^s = \sqrt{\left((Y(1))^s - (Y(2))^s \right)} \quad (16)$$

From this process, the random amount is elected, and it is represented as and it stuck in the middle of $[0, 1]$.

$$\begin{cases} \text{new member} & \text{if } \Omega > 0.45 \\ \text{mating in between the pairs} & \text{if } \Omega \leq 0.45 \end{cases} \quad (17)$$

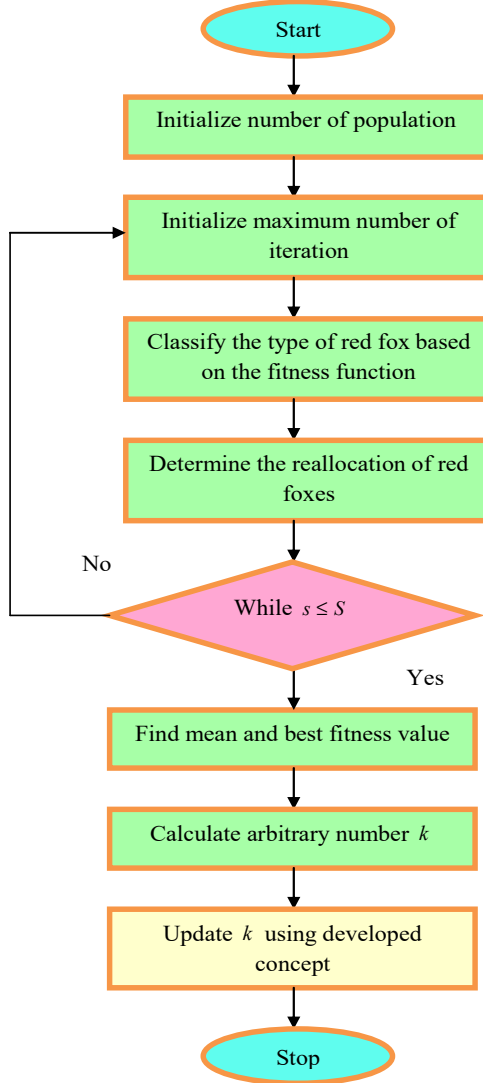
In the given search space, the random location is identified and further, the new pairs of red foxes are determined by equation (18).

$$(Y^{rep})^s = \frac{\Omega}{2}(Y(1))^s - (Y(2))^s \quad (18)$$

Thus, the value of x and Φ is adopted as 0.2 and 1, respectively.

The flow diagram and the pseudocode of the offered MUN-RFO algorithm are shown in Figure 3 and Algorithm 1.

Figure 3 Flow diagram of MUN-RFO algorithm (see online version for colours)



Algorithm 1 Developed MUN-RFO

```

Initialise the total number population  $a$  and iteration
for  $t = 1$  to  $mi$ 
    for  $i = 1$  to  $a$ 
        Classify the type of fox based on the fitness value
        Select the red fox from the generated population
        Evaluate the reallocation of all red foxes in the population
        While  $s \leq S$  then
            Determine the mean fitness value
            Determine the best fitness value

            Evaluate  $k = \frac{100 \circ \text{mean } fi}{\text{best } fi}$ 

            Update the  $k$  using improved concept by equation (7)
            Traditional update
        End
    End for
End for
Achieve the best solution
End

```

5 Level 2: elliptic curve cryptography with optimal key for encrypting insensitive data and data uploading in cloud

5.1 Procedure of ECC

In this work, the elliptic curve cryptography (ECC) is used to encipher the insensitive part of the EHR data. The ECC (Boudia et al., 2016) is one of the mostly adopted encryption systems because it encrypts the input data with a very small size key, and also the performance of the ECC is considerably better than the other encryption systems. The minimal power and the wireless communication system adopt the ECC technique for encrypting the data in a more efficient way. Here, the public keys are adopted to encipher the plain text into the form of cipher text. Additionally, the cost required for the encryption and the decryption process is dramatically low in the ECC system. In this process, the receiver has public and private keys for performing the encryption and decryption process. The process involved in the ECC encryption system is listed as follows:

- Generation of key pair: In this process, the private key is arbitrarily elected from the $[1, m - 1]$. This private key is adopted to determine the public key using equation (19).

$$P = cF \tag{19}$$

Here, the private key is represented as c .

- Generation of signature: Here, the signature value is determined by equation (20).

$$L = (q, r) \quad (20)$$

$$r = j^{-1} (G(L) + cq) | m | \quad (21)$$

$$q = w(jF) | m | \quad (22)$$

Here, the message is indicated as L , and the axis of jF is indicated as $w(jF)$.

- Verification of signature: The condition followed in the system is depicted in equation (23).

$$\text{if } w(Q) = q | m | \quad (23)$$

$$Q = tF + uP \quad (24)$$

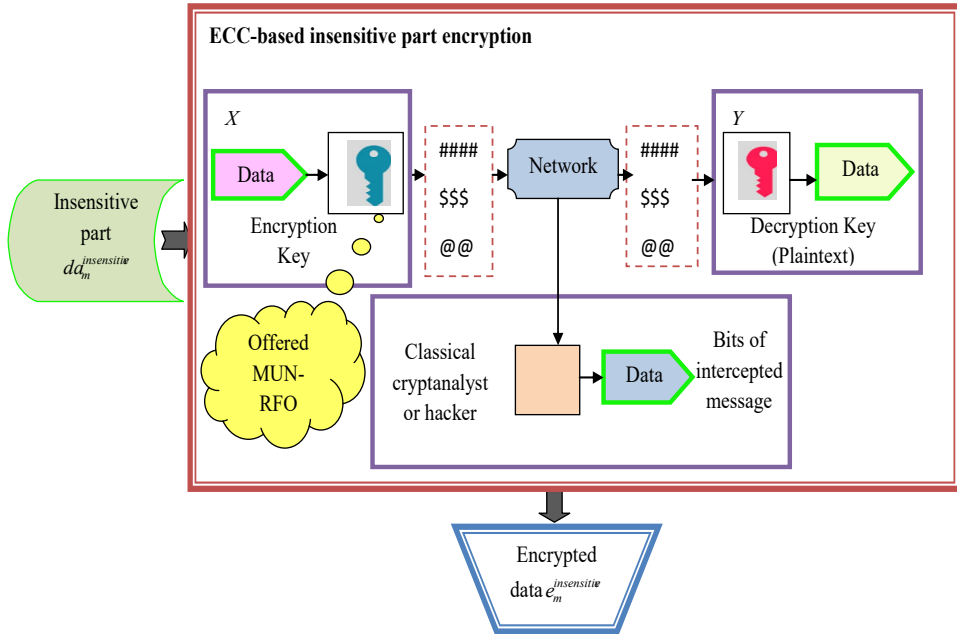
$$t = G(L)v | m | \quad (25)$$

$$u = qv | m | \quad (26)$$

$$v = r^{-1} | m | \quad (27)$$

Here, the signature is verified if the condition in equation (23) is fulfilled.

Figure 4 Insensitive part encryption using ECC with optimal key (see online version for colours)



5.2 Non sensitive part encryption using ECC with optimal key

In this process, the separated insensitive data $da_m^{insensitive}$ is encrypted with the help of the ECC. The insensitive part is composed of minor details of the patient, like their contact information etc. Here, the encryption is performed with the help of the optimal key generated by the developed MUN-RFO algorithm. The proposed MUN-RFO algorithm is also adopted to optimise the generated key, and this key is available in binary format. This optimisation lowers the time and memory required to complete the encryption process. Due to the optimal key generation process, the encryption process is rapidly completed. The encrypted data from this process is depicted as $e_m^{insensitive}$. The pictorial illustration of the insensitive part encryption using ECC is signified in Figure 4.

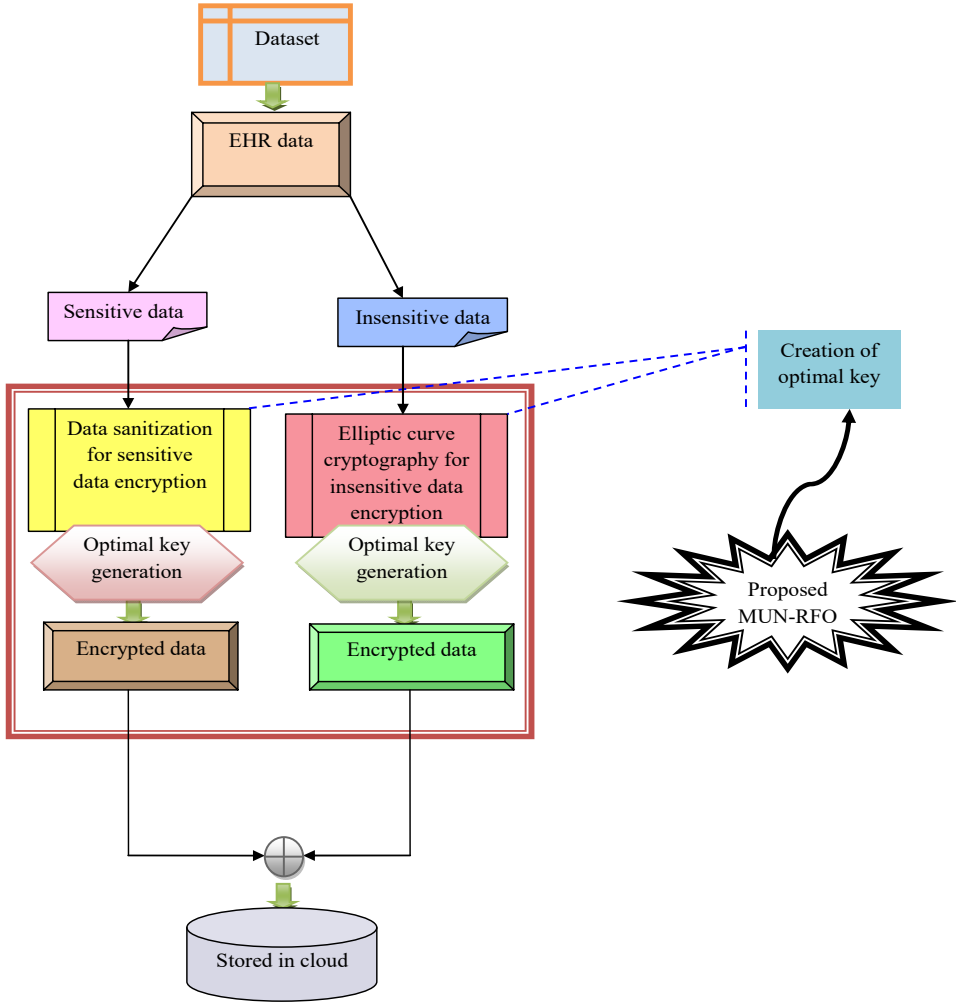
5.3 Data uploading in cloud

In recent days, clinicians have adopted cloud platforms for storing a huge amount of EHR. This platform can ease the maintenance of EHR for healthcare providers. Here, the encrypted data from the data sanitisation e_m^{sanit} and ECC $e_m^{insensitive}$ are combined together, and they are stored in the cloud platform. The user can access the needed information from the cloud structure by decrypting the enciphered data using the key generated in the data sanitisation and ECC process. A huge amount of encrypted data is stored in the cloud platform for easy access and maintenance. Furthermore, the encrypted data can be stored in the cloud platform for a long period without any leakage.

5.4 Overall processing steps of secure healthcare cloud data platform

The developed MUN-RFO-OKDES-based two-level EHR security system is developed to secure the sensitive and insensitive part of the EHR data, and it prevents the hacking of data from unauthorised users. Additionally, the developed MUN-RFO-OKDES-based two-level EHR security system is used for easy access to EHR data without any security issues. At first, the gathered EHR data from the reference link was split into two parts like, sensitive and insensitive parts. The sensitive part of the EHR data is encrypted using a data sanitisation process, and here, the optimal key required to start up the encryption process is created by the developed MUN-RFO algorithm. This algorithm is also used to achieve lowered computation time, memory size, and increased preservation and hiding ratio by optimising the binary format key generated in the data sanitisation process. Further, the insensitive part of the EHR data is encrypted with the assistance of ECC. Here also, the optimal key is generated by the developed MUN-RFO algorithm to do the encryption process. The developed algorithm is utilised to optimise the binary format key in ECC to lower the time and memory size in the encryption process. Lastly, the encrypted data from both encryption processes are merged together and safely stored in the cloud architecture for easy access. This can prevent data duplication and other illegal activities. The pictorial representation of the developed MUN-RFO-OKDES-based two-level EHR security system is given in Figure 5.

Figure 5 Pictorial representation of the developed MUN-RFO-OKDES-based two levels EHR security system (see online version for colours)



6 Results and discussion

6.1 Stimulation setup

The explored MUN-RFO-OKDES-based two levels EHR security system was functioned by the Python software. Here, the developed MUN-RFO-OKDES-based two-level EHR security system has a population number of 10, the highest iteration rate of 50, and a chromosome length was taken as 16. Several traditional algorithms, such as honey badger algorithm (HBA) (Hashim et al., 2022), deer hunting optimisation algorithm (DHOA) (Brammya et al., 2019), electromagnetic field optimisation (EFO) (Yurtkuran, 2019), and RFO (Khorami et al., 2021), were taken to discover the effectiveness of the developed

MUN-RFO-OKDES-based two levels EHR security system. The simulation parameters of the developed two levels EHR security system are shown in Table 2.

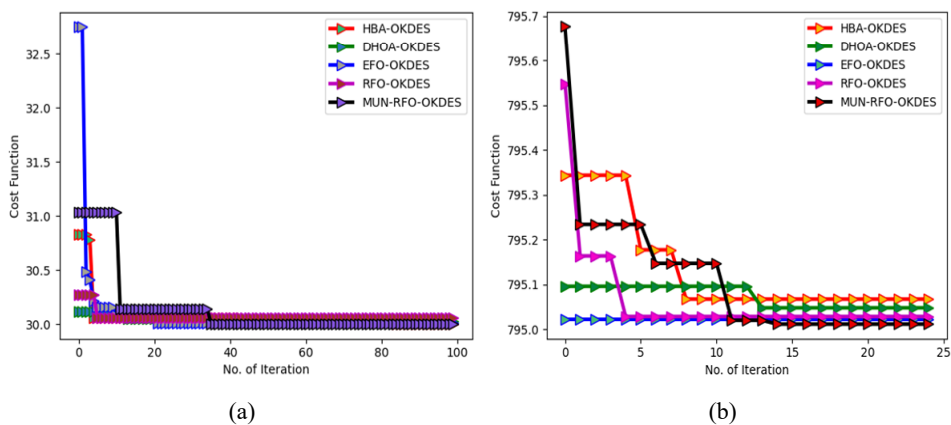
Table 2 Simulation parameters of the developed two levels of the EHR security system

Parameters	Values
<i>EHR security system</i>	
FirstBlockArrivalTime	0 second
Simulator System Configuration	Intel core i3 and 8GB RAM
InterBlockArrivalTime	10, 20, 30, 40, 50, 60 seconds
<i>MUN-RFO algorithm</i>	
Alpha	0.5
Gamma	0.8
Exploration probability (p)	0.1
Exploitation probability (q)	0.1

6.2 Cost function assessment

The cost function examination of the developed MUN-RFO-OKDES-based two-level EHR security system is given in Figure 6. Here, the iteration is adopted in x-coordinate to carry out this comparison. The cost function of the MUN-RFO-OKDES-based two levels EHR security system is lower by 0.022% of HBA-OKDES, 0.011% of DHOA-OKDES, 0.0025% of EFO-OKDES and 0.001% of RFO-OKDES at 5th iteration for dataset 2. So the experimental finding proved that the cost requirement of the developed MUN-RFO-OKDES-based two levels EHR security system is less than the old algorithms.

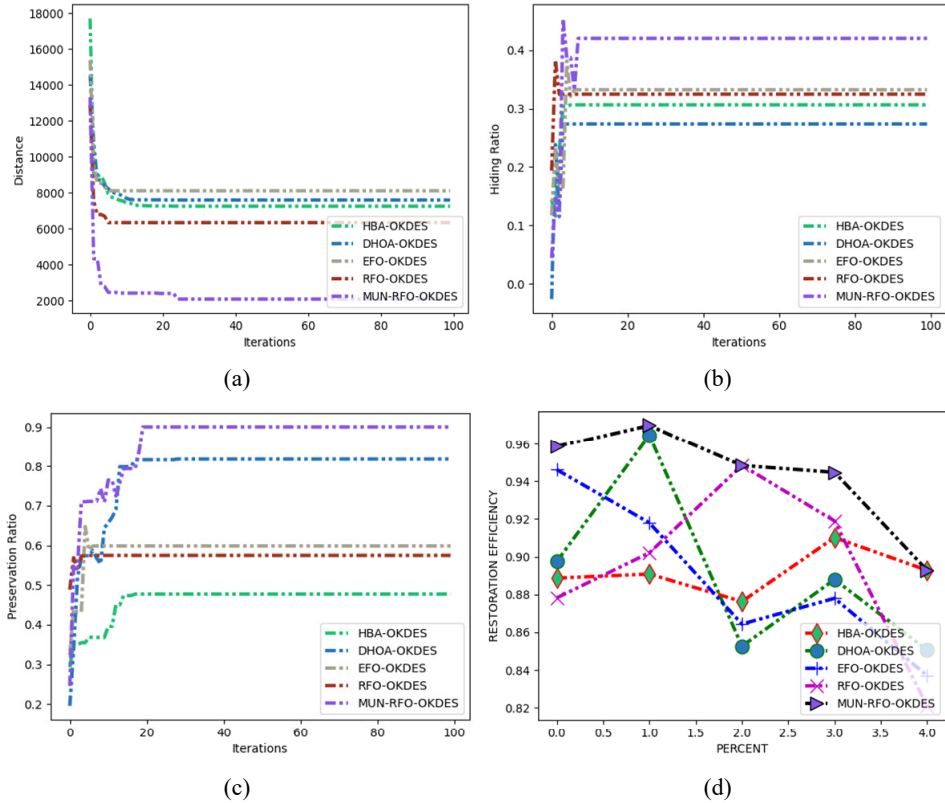
Figure 6 Cost function assessment of the developed cloud-based two-level EHR security system in terms of (a) sensitive data, (b) insensitive data (see online version for colours)



6.3 Efficiency assessment using various attributes

Figure 7 illustrates the efficiency assessment of the developed MUN-RFO-OKDES-based two levels EHR security system using the various constraints. At iteration 60, the hiding ratio of the developed MUN-RFO-OKDES-based two levels EHR security system is improved than the HBA-OKDES, DHOA-OKDES, EFO-OKDES, and RFO-OKDES with 45.16%, 66.66%, 32.35% and 36.36%. Hence, the experimental finding revealed that the hiding ratio of the developed MUN-RFO-OKDES-based two levels EHR security system is superior to the classical algorithms.

Figure 7 Performance assessment of the developed cloud-based two level EHR security system for (a) distance, (b) hiding ratio, (c) preservation ratio, (d) restoration efficiency (see online version for colours)

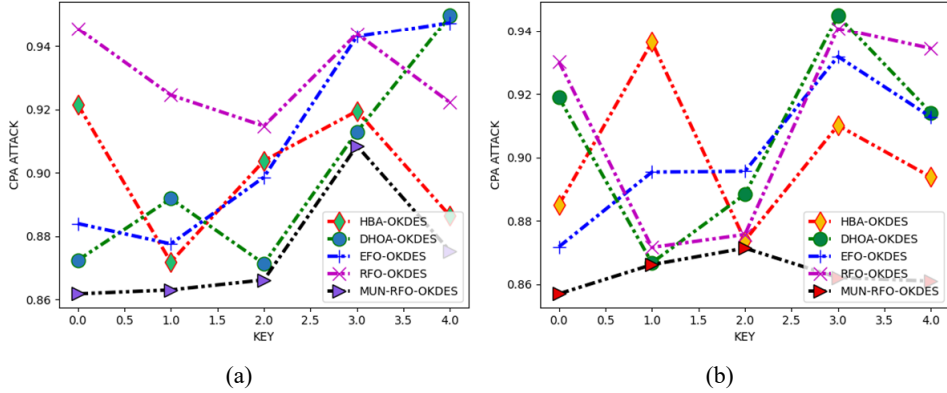


6.4 CPA attack assessment

The CPA attack assessment of the proposed MUN-RFO-OKDES-based two levels EHR security system is demonstrated in Figure 8. For dataset 1, the CPA attack of the implemented MUN-RFO-OKDES-based two levels EHR security system is 1.14% lower than HBA-OKDES, 1.49% lower than DHOA-OKDES, 1.83% lower than EFO-OKDES, and 0.11% lower than RFO-OKDES at the key value of 2. Therefore, the comparative

outcome proved that the CPA attack of the developed MUN-RFO-OKDES-based two levels EHR security system is much lower than the ancient algorithms.

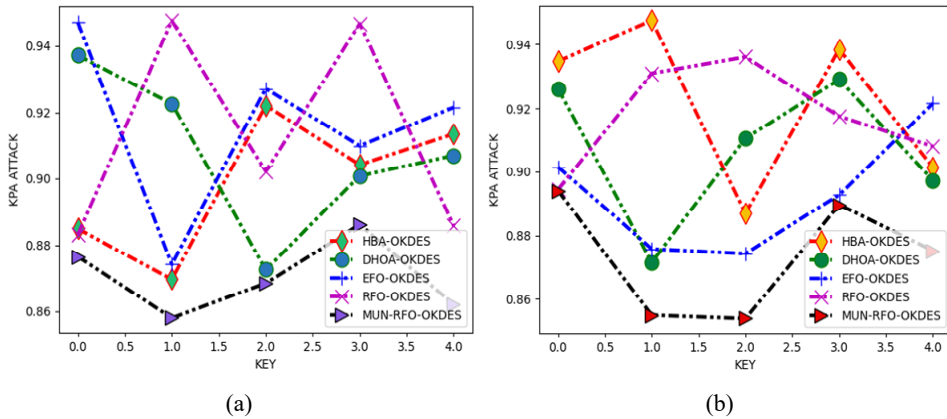
Figure 8 CPA attack assessment of the developed cloud-based two-level EHR security system for (a) sensitive data, (b) insensitive data (see online version for colours)



6.5 KPA attack assessment

Figure 9 represents the KPA attack examination of the implemented MUN-RFO-OKDES-based two levels EHR security system. At the key value of 1, the KPA attack of the developed MUN-RFO-OKDES-based two levels EHR security system is reduced than HBA-OKDES, DHOA-OKDES, EFO-OKDES, and RFO-OKDES by 1.2%, 7.4%, 2.09% and 10.94% for dataset 1. So the comparative outcome depicted that the KPA attack of the MUN-RFO-OKDES-based two levels EHR security system is reduced than the current algorithms.

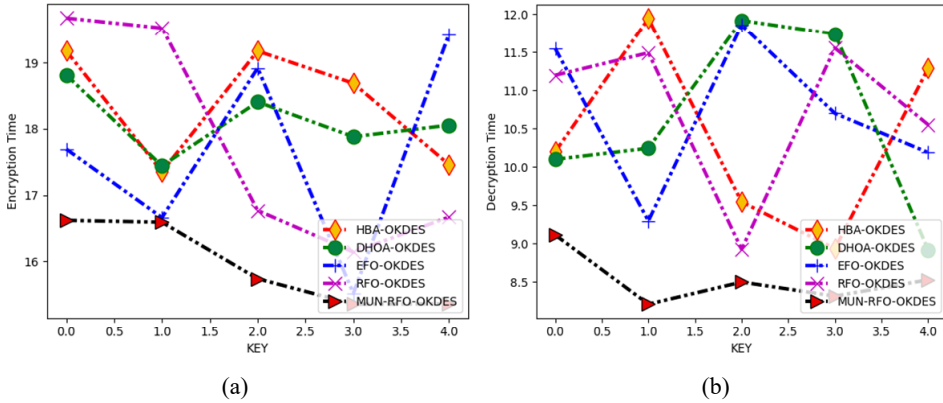
Figure 9 KPA attack assessment of the developed cloud-based two-level EHR security system for (a) sensitive data, (b) insensitive data (see online version for colours)



6.6 Encryption and decryption time analysis

The enciphering and the deciphering time analysis of the suggested MUN-RFO-OKDES-based two levels EHR security system are indicated in Figure 10 and Figure 11. The encryption time of the developed MUN-RFO-OKDES-based two levels EHR security system is 24.51%, 19.35%, 14.83% and 7.74% lower than HBA-OKDES, DHOA-OKDES, EFO-OKDES and RFO-OKDES at a key value of 2.5. Hence, the correlated outcome signifies that the encryption time for the proposed system is much less than the traditional algorithms.

Figure 10 Encryption and decryption time assessment of the developed cloud-based two-level EHR security system among various algorithms for (a) encryption time, (b) decryption time (see online version for colours)



6.7 Insensitive data-based analysis among various classifiers

The insensitive data analysis among various techniques is depicted in Figure 11. At the key value of 30, the decryption time of the MUN-RFO-OKDES-based two levels EHR security system is reduced than the DES, AES, SHA-1, and MUN with 55.43%, 73.91%, 41.30% and 80.43%. So, it is proved that the time required to decrypt the data in the proposed system is lower than the traditional classifiers.

6.8 Statistical assessment

The statistical assessment of the offered MUN-RFO-OKDES-based two levels EHR security system for the sensitive and insensitive data is given in Table 3. For sensitive data, the mean value of the developed MUN-RFO-OKDES-based two levels EHR security system is 0.23% higher than HBA-OKDES, 0.299% higher than DHOA-OKDES, 0.166% higher than EFO-OKDES and 0.266% higher than RFO-OKDES. Therefore it is confirmed that the mean value of the developed MUN-RFO-OKDES-based two levels EHR security system is improved than the ancient algorithms.

Figure 11 Insensitive data analysis of the developed cloud-based two-level EHR security system among various algorithms for (a) CPA attack, (b) KPA attack, (c) encryption time, (d) decryption time (see online version for colours)

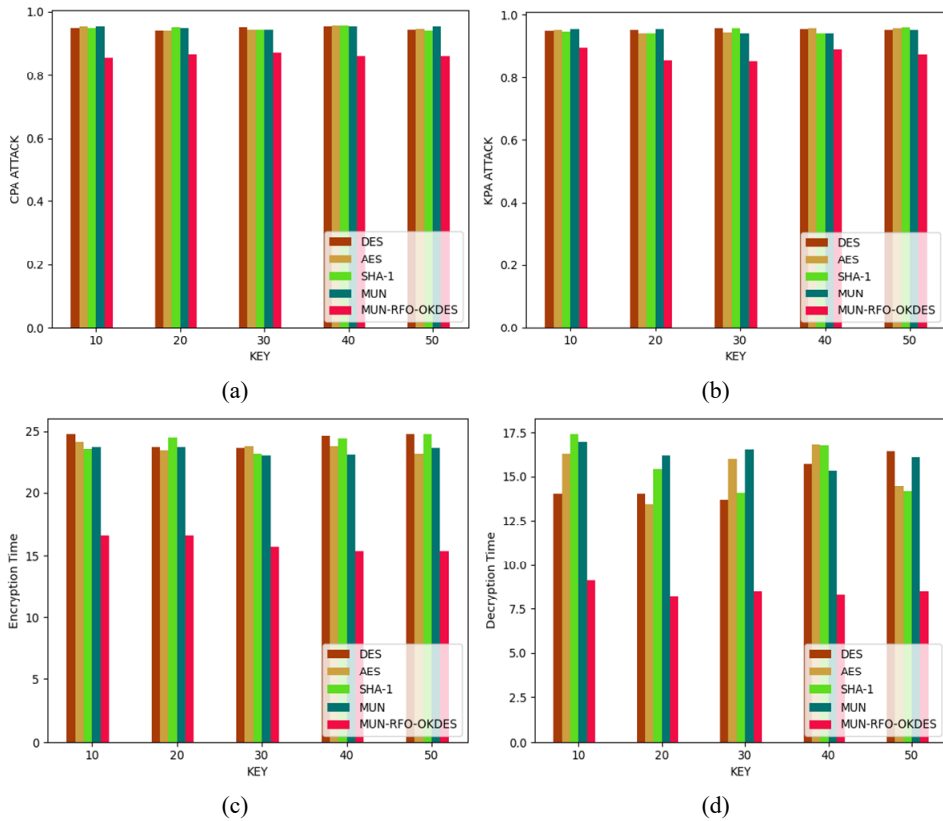


Table 3 Statistical assessment of the implemented cloud-based two-level EHR security system

<i>Sensitive data</i>					
<i>Terms</i>	<i>HBA-OKDES</i> (Hashim et al., 2022)	<i>DHOA-OKDES</i> (Brammya et al., 2019)	<i>EFO-OKDES</i> (Yurtkuran, 2019)	<i>RFO-OKDES</i> (Khorami et al., 2021)	<i>MUN-RFO-OKDES</i>
Best	30.00608	30.03067	30.01276	30.05792	30.00005
Worst	30.82782	30.11634	32.75161	30.27401	31.03895
Mean	30.07613	30.05137	30.09391	30.06872	30.14921
Median	30.04324	30.0506	30.01276	30.05792	30.00005
Std.	0.152512	0.026762	0.386511	0.047096	0.318663
<i>Insensitive data</i>					
Best	795.0674	795.048	795.0218	795.0287	795.0117
Worst	795.3437	795.096	795.0218	795.5478	795.6767
Mean	795.1359	795.073	795.0218	795.0657	795.1109
Median	795.0674	795.096	795.0218	795.0287	795.0202
Std.	0.109662	0.023989	1.14x10 ⁻¹³	0.10769	0.146353

6.9 Evaluation of statistical analysis using recent approaches

Evaluation of statistical analysis for the offered MUN-RFO-OKDES-based two levels EHR security system using recent approaches is given in Table 4. Thus, it is revealed that the offered approach attains better results than the other baseline approaches.

Table 4 Statistical evaluation of the implemented cloud-based two-level EHR security system

<i>Terms</i>	<i>OECC (Malik et al., 2020)</i>	<i>RSA-MABC (Aggarwal et al., 2022)</i>	<i>PSO-CS (Adhikari et al., 2023)</i>	<i>MUN-RFO-OKDES</i>
<i>Encryption statistical report</i>				
Best	19.57596	21.8877	17.6548	16.61971
Worst	18.57596	18.8877	15.6548	15.35433
Mean	18.97596	20.0877	17.2548	15.9326
Median	18.57596	19.8877	17.6548	15.73869
Std.	0.489898	1.16619	0.8	0.567056
<i>Decryption statistical report</i>				
Best	15.6974	14.6974	11.36448	9.11607
Worst	11.6974	10.6974	8.36448	8.212111
Mean	13.6974	12.4974	10.36448	8.535338
Median	13.6974	12.6974	11.36448	8.500758
Std.	1.414214	1.6	1.264911	0.313177

6.10 Investigation of computation time and computation complexity of the developed model

The validation of computation time and the complexity of the recommended model are shown in Tables 5 and 6. From Table 5, it is revealed that the computation time of the offered approach is better than the other conventional approach which is utilised to reduce the overfitting issues. Accordingly, from Table 6, the term is defined as the number of maximum iterations, and the variable is denoted as the number of populations.

Table 5 Validation of computation time of the recommended model

<i>Methods</i>	<i>HBA (Hashim et al., 2022)</i>	<i>DHOA (Brammya et al., 2019)</i>	<i>EFO (Yurtkuran, 2019)</i>	<i>RFO (Khorami et al., 2021)</i>	<i>MUN-RFO-OKDES</i>
Time (sec)	30.25	28.22	25.43	22.06	20.44

Table 6 Computational complexity of the designed approach

<i>Proposed model</i>	<i>MUN-RFO-OKDES</i>
Complexity	$O(\text{MaxIter} * (N_{\text{pop}}))$

7 Conclusions

The suggested cloud-based two levels EHR security system was developed to secure the sensitive and insensitive parts of the EHR data to prevent the hacking of data from the unethical person. The developed MUN-RFO-OKDES-based two levels EHR security system was also used to prevent the duplication and leakage of patient information. Here, the gathered EHR data was divided into two parts, such as sensitive and insensitive data. The sensitive data was encrypted with the aid of a data sanitisation technique, and here, the optimal key required to do the encryption process was developed by the MUN-RFO algorithm. Moreover, the insensitive part of the EHR data was enciphered with the assistance of the ECC system, and here also, the optimal key was created with the assistance of the developed MUN-RFO algorithm. Furthermore, the developed MUN-RFO algorithm was also used to optimise the key generated in the data sanitisation and ECC process to lower the computation time, memory size, and time and to enhance the hiding and preservation ratio during the encryption process. The obtained encrypted data from the two techniques were merged together, and they were stored in the cloud platform for easy access and maintenance. At iteration 60, the hiding ratio of the developed MUN-RFO-OKDES-based two levels EHR security system was improved than the HBA-OKDES, DHOA-OKDES, EFO-OKDES, and RFO-OKDES with 45.16%, 66.66%, 32.35% and 36.36%. So, the developed MUN-RFO-OKDES-based two levels EHR security system has lowered memory size, time and enhanced preservation ratio, and hiding ratio than the ancient security providing system. In the future, we will mainly focus on more encryption functions. It will help the cloud providers to effectively ignore expensive encryption methods and also to protect data privacy. Especially, we will try to use a large number of cloud applications which will help to provide undeniably and data security.

References

- Abirami, P. and Bhanu, S.V. (2020) 'Enhancing cloud security using crypto-deep neural network for privacy preservation in trusted environment', *Soft Computing*, Vol. 24, pp.18927–18936.
- Adhikari, S., Brayich, M., Akila, D., Sakar, B., Devika, S. and Revathi, S. (2023) 'Hybrid optimization using CC and PSO in cryptography encryption for medical images', *ICMMCS 2023: Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science*, Vol. 1450, pp.79–93.
- Aggarwal, M., Malik, A. and Madhukar, M. (2022) 'Effective cryptographic renewal method with Rivest-Shamir-Adleman, modified artificial bee colony optimization to achieve secure cloud storage and computation in cloud computing', *Journal of Computational and Theoretical Nanoscience*, Vol. 17, No. 6, pp.2702–2708.
- Ahamad, D., Hameed, S.A. and Akhtar, M. (2020) 'A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization', *Journal of King Saud University – Computer and Information Sciences*, Vol. 34, No. 6, pp.2309–3110.
- Ahmad, W., Wang, S., Sheharyar and Mahmood, Z. (2018a) 'Outsourced ciphertext-policy based privacy preservation for mobile cloud computing', *Procedia Computer Science*, Vol. 129, pp.128–134.
- Ahmad, W., Wang, S., Ullah, A., Sheharyar and Mahmood, Z. (2018b) 'Reputation-aware trust and privacy-preservation for mobile cloud computing', *IEEE Access*, Vol. 6, pp.46363–46381.

- Almadhor, A., Khan, A.A., Wechtaisong, C., Yousaf, I., Kryvinska, N., Tariq, U. and Ben Chikha, H. (2023) 'Chest radiographs-based pneumothorax detection using federated learning', *Computer Systems Science and Engineering*, Vol. 47, No. 2, pp.1775–1791.
- Alphonsa, M.M.A. and Amudhavalli, P. (2018) 'Genetically modified glowworm swarm optimization based privacy preservation in cloud computing for healthcare sector', *Evolutionary Intelligence*, Vol. 11, pp.101–116.
- Anandkumar, R., Dinesh, K., Obaid, A.J., Malik, P., Sharma, R., Dumka, A., Singh, R. and Khatak, S. (2022) 'Securing e-health application of cloud computing using hyperchaotic image encryption framework', *Computers and Electrical Engineering*, May, Vol. 100, p.107860.
- Boava, A. and Iano, Y. (2016) 'Secure inter-cloud architecture for virtual cloud computing based on hybrid IP and MPLS infrastructure solution', *IEEE Latin America Transactions*, July, Vol. 14, No. 7, pp.3490–3495.
- Boudia, O.R.M., Senouci, S.M. and Feham, M. (2016) *Elliptic Curve Based Secure Multidimensional Aggregation for Smart Grid Communications*, 2017, Vol. 17, No. 23, pp.7750–7757, IEEE.
- Brammya, G., Praveena, S., Preetha, N.S.N., Ramya, R., Rajakumar, B.R. and Binu, D. (2019) 'Deer hunting optimization algorithm: a new nature-inspired meta-heuristic paradigm', *The Computer Journal*, 24 May.
- Dai, H., Ji, Y., Yang, G., Huang, H. and Yi, X. (2020) 'A privacy-preserving multi-keyword ranked search over encrypted data in hybrid clouds', *IEEE Access*, Vol. 8, pp.4895–4907.
- de Oliveira, M.T., Bakas, A., Frimpong, E., Groot, A.E.D., Marquering, H.A., Michalas, A. and Olabarriaga, S.D. (2020) 'A break-glass protocol based on ciphertext-policy attribute-based encryption to access medical records in the cloud', *Annals of Telecommunications*, Vol. 75, pp.103–119.
- Denis, R. and Madhubala, P. (2021) 'Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems', *Multimedia Tools and Applications*, Vol. 80, pp.21165–21202.
- Grover, B. and Kushwaha, D.K. (2022) 'Authorization and privacy preservation in cloud-based distributed ehr system using blockchain technology and anonymous digital ring signature', *Health Services and Outcomes Research Methodology*, Vol. 23, pp.227–240.
- Hashim, F.A., Houssein, E.H., Hussain, K., Mabrouk, M.S. and Al-Atabany, W. (2022) 'Honey badger algorithm: new metaheuristic algorithm for solving optimization problems', *Mathematics and Computers in Simulation*, February, Vol. 192, pp.84–110.
- Hindistan, Y.S. and Yetkin, E.F. (2023) 'A hybrid approach with GAN and DP for privacy preservation of IIoT data', *IEEE Access*, Vol. 11, pp.5837–5849.
- Kanwal, T., Anjum, A., Malik, S.U.R., Khan, A. and Khan, M.A. (2021) 'Privacy preservation of electronic health records with adversarial attacks identification in hybrid cloud', *Computer Standards & Interfaces*, October, Vol. 78, p.103522.
- Khan, A.A., Alsubai, S., Wechtaisong, C., Almadhor, A., Kryvinska, N., Al Hejaili, A. and Ghulam, U. (2023a) 'Cd.fl: cataract images-based disease detection using federated learning', *Computer Systems Science and Engineering*, Vol. 47, No. 2, pp.1733–1750.
- Khan, A.A., Driss, M., Boulila, W., Sampedro, G.A. and Abbas, S. (2023b) 'Privacy preserved and decentralized smartphone recommendation system', in *IEEE Transactions on Consumer Electronics*, Vol. 70, No. 1, pp.1–11.
- Khorami, E., Babaei, F.M. and Azadeh, A. (2021) 'Optimal diagnosis of COVID-19 based on convolutional neural network and red fox optimization algorithm', *Computational Intelligence and Neuroscience*, Vol. 2021, No. 1, p.11.
- Kumar, N.P.H. and Prabhudeva, S. (2021) 'Layers based optimal privacy preservation of the on-premise data supported by the dual authentication and lightweight on fly encryption in cloud ecosystem', *Wireless Personal Communications*, Vol. 121, pp.1489–1508.

- Kundalwal, M.K., Chatterjee, K. and Singh, A. (2019) 'An improved privacy preservation technique in health-cloud', *ICT Express*, September, Vol. 5, No. 3, pp.167–172.
- Li, S., Zhou, Y., Jiao, L., Yan, X., Wang, X. and Lyu, M.R-T. (2015) 'Towards operational cost minimization in hybrid clouds for dynamic resource provisioning with delay-aware optimization', *IEEE Transactions on Services Computing*, June, Vol. 8, No. 3, pp.398–409.
- Liu, H., Yao, X., Yang, T. and Ning, H. (2019) 'Cooperative privacy preservation for wearable devices in hybrid computing-based smart health', *IEEE Internet of Things Journal*, April, Vol. 6, No. 2, pp.1352–1362.
- Liu, Z., Liu, Y. and Fan, Y. (2018) 'Searchable attribute-based signcryption scheme for electronic personal health record', *IEEE Access*, Vol. 6, pp.76381–76394.
- Malik, A., Aggarwal, M., Sharma, B., Singh, A. and Singh, K.K. (2020) 'Optimal elliptic effective approach for secure data storage in clouds', *International Journal of Knowledge and Systems Science*, Vol. 11, No. 4.
- Marwaha, H. and Singh, R. (2019) 'The secure migration of data to cloud using data sanitization and MAC address based AES', *International Journal of Recent Technology and Engineering (IJRTE)*, March, Vol. 7, No. 6, ISSN: 2277-3878.
- Marwan, M., Kartit, A. and Ouahmane, H. (2018) 'Security enhancement in healthcare cloud using machine learning', *Procedia Computer Science*, Vol. 127, pp.388–397.
- Menon, S.P., Shukla, P.K., Sethi, P., Alasiry, A., Marzougui, M., Alouane, M.T-H. and Khan, A.A. (2023) 'An intelligent diabetic patient tracking system based on machine learning for e-health applications', *Sensors*, Vol. 23, No. 6, p.3004.
- Pachala, S., Rupa, Ch. and Sumalatha, L. (2021) 'An improved security and privacy management system for data in multi-cloud environments using a hybrid approach', *Evolutionary Intelligence*, Vol. 14, pp.1117–1133.
- Shin, Y., Yang, W., Kim, S. and Chung, J-M. (2022) 'Multiple adaptive-resource-allocation real-time supervisor (MARS) for elastic IIoT hybrid cloud services', *IEEE Transactions on Network Science and Engineering*, May, Vol. 9, No. 3, pp.1462–1476.
- Tao, Y., Qiu, J. and Lai, S. (2022) 'A hybrid cloud and edge control strategy for demand responses using deep reinforcement learning and transfer learning', *IEEE Transactions on Cloud Computing*, March, Vol. 10, No. 1, pp.56–71.
- Xu, X., Fu, S., Qi, L., Zhang, X., Liu, Q., He, Q. and Li, S. (2018) 'An IoT-oriented data placement method with privacy preservation in the cloud environment', *Journal of Network and Computer Applications*, 15 December, Vol. 124, pp.148–157.
- Yang, Y., Li, X., Qamar, N., Liu, P., Ke, W., Shen, B. and Liu, Z. (2018) 'Medshare: a novel hybrid cloud for medical resource sharing among autonomous healthcare providers', *IEEE Access*, Vol. 6, pp.46949–46961.
- Yuan, X., Weng, J., Wang, C. and Ren, K. (2018) 'Secure integrated circuit design via hybrid cloud', *IEEE Transactions on Parallel and Distributed Systems*, 1 August, Vol. 29, No. 8, pp.1851–1864.
- Yurtkuran, A. (2019) 'An improved electromagnetic field optimization for the global optimization problems', *Computational Intelligence and Neuroscience*, Vol. 2019, No. 1.
- Zhang, H., Zhou, Z., Ye, L. and Du, X. (2018) 'Towards privacy preserving publishing of set-valued data on hybrid cloud', *IEEE Transactions on Cloud Computing*, June, Vol. 6, No. 2, pp.316–329.

Acronyms

<i>Abbreviation</i>	<i>Description</i>
EHR	Electronic health records
MUN-RFO	Modified uniform number-based red fox optimisation
OKDES	Optimal key-based data encryption scheme
PKI	Public key infrastructure
XACML	Extensible access control markup language
PPX-AC	Privacy-preserving extensible access control
HLPN	High-level petri nets
CDNNCS	Crypto-deep neural network cloud security
OS-ABE	Outsourced encryption policy based on cipher text attributed policy
HBA	Honey badger algorithm
DHOA	Deer hunting optimisation algorithm
EFO	Electromagnetic field optimisation