scientific reports

Check for updates

OPEN

Integrating meta-heuristic with named data networking for secure edge computing in IoT enabled healthcare monitoring system

Nalini Manogaran[1], Malarvizhi Nandagopal[2], Neeba Eralil Abi[3], Koteeswaran Seerangan[1], Balamurugan Balusamy[4] & Shitharth Selvarajan[5,6]✉

The advancement in technology, with the "Internet of Things (IoT) is continuing a crucial task to accomplish distance medical care observation, where the effective and secure healthcare information retrieval is complex. However, the IoT systems have restricted resources hence it is complex to attain effective and secure healthcare information acquisition. The idea of smart healthcare has developed in diverse regions, where small-scale implementations of medical facilities are evaluated. In the IoT-aided medical devices, the security of the IoT systems and related information is highly essential on the other hand, the edge computing is a significant framework that rectifies their processing and computational issues. The edge computing is inexpensive, and it is a powerful framework to offer low latency information assistance by enhancing the computation and the transmission speed of the IoT systems in the medical sectors. The main intention of this work is to design a secure framework for Edge computing in IoT-enabled healthcare systems using heuristic-based authentication and "Named Data Networking (NDN)". There are three layers in the proposed model. In the first layer, many IoT devices are connected together, and using the cluster head formation, the patients are transmitting their data to the edge cloud layer. The edge cloud layer is responsible for storage and computing resources for rapidly caching and providing medical data. Hence, the patient layer is a new heuristic-based sanitization algorithm called Revised Position of Cat Swarm Optimization (RPCSO) with NDN for hiding the sensitive data that should not be leaked to unauthorized users. This authentication procedure is adopted as a multi-objective function key generation procedure considering constraints like hiding failure rate, information preservation rate, and degree of modification. Further, the data from the edge cloud layer is transferred to the user layer, where the optimal key generation with NDN-based restoration is adopted, thus achieving efficient and secure medical data retrieval. The framework is evaluated quantitatively on diverse healthcare datasets from University of California (UCI) and Kaggle repository and experimental analysis shows the superior performance of the proposed model in terms of latency and cost when compared to existing solutions. The proposed model performs the comparative analysis of the existing algorithms such as Cat Swarm Optimization (CSO), Osprey Optimization Algorithm (OOA), Mexican Axolotl Optimization (MAO), Single candidate optimizer (SCO). Similarly, the cryptography tasks like "Rivest–Shamir–Adleman (RSA), Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), and Data sanitization and Restoration (DSR) are applied and compared with the RPCSO in the proposed work. The results of the proposed model is compared on the basis of the best, worst, mean, median and standard deviation.

[1]S.A. Engineering College (Autonomous), Chennai, Tamil Nadu 600077, India. [2]Department of CSE, School of Computing, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu 600062, India. [3]Department of Information Technology, Rajagiri School of Engineering & Technology, Kochi, Kerala 682039, India. [4]Shiv Nadar (Institution of Eminence Deemed to be University), Uttar Pradesh 201314, India. [5]Department of Computer Science, Kebri Dehar University, 250, Kebri Dehar, Ethiopia. [6]School of Built Environment, Engineering and Computing, Leeds Beckett University, LS6 3QS, Leeds, U.K. ✉email: ShitharthS@kdu.edu.et

The proposed RPCSO outperforms all other models with values of 0.018069361, 0.50564046, 0.112643119, 0.018069361, 0.156968355 and 0.283597992, 0.467442652, 0.32920734, 0.328581887, 0.063687386 for both dataset 1 and dataset 2 respectively.

Keywords Healthcare monitoring system, Edge computing, Internet of Things, Data sanitization and restoration, Optimal key generation, Revised position of cat swarm optimization

The IoT includes smart nodes, which can gather and sense the current time data for observing. This creates IoT continues an essential approach to understanding a distance medical observation, where the efficacy and the security of the healthcare information delivery are of high concern[1]. But, the IoT systems have limited sensing resources, computation, and caching, hence a basis for efficient and secure healthcare information retrieval is to win over the issue of asset restrains[2]. Contrasted with the IoT systems, the edge systems presented in the edge cloud have lots of caching and potential execution abilities, hence an edge cloud must be a primary answer for supporting resolving the computation and storage resource restrictions of IoT systems[3]. Conventional medical model experiments are concentrated highly on the data sharing and security approaches at the level of cloud servers[4]. Most importantly, the composition of cloud and edge server paradigms makes it very hard for the present-time medical model to offer efficient information execution and disorder estimation. This is a proof from the edge and cloud combined smart domain to enhance the living standard of people against the cyber-physical model. Because of the openness in the edge-cloud sector and restricted user access control, there may be several unavoidable causes that result in security problems such as the privacy of the users and the organization value of the providers[5], [6–12].

The "Software Defined Networking (SDN) intelligence satisfies the requirement of the edge computing concerning the load balancing and resource allocation, on the other hand, the security is offered by an approach of lightweight authentication. The controller of SDN is accountable for the orchestration of edge, time sensitivity, management of data, and offering rapid and very dependable transmission of information. These features are the primary demands of the medical device. The edge systems in an edge cloud may provide sufficient resources on the other hand the NDN may enhance the efficacy of the data retrieval[13]. The NDN[14] is a framework for an effective information delivery sector, where a candidate initiates a data transmission task by transmitting interest with a title. Any data router attaining interest sends interest in the direction of powerful providers by utilizing a "Forwarding Information Base (FIB)", and determines reverse ways by generating the "Pending Interest Table (PIT)". Any provider attaining interest offers information with final information to the candidates via the reverse ways, and any data router attaining information can cache information[15]. The upcoming merits of NDN can support improving the efficacy of IE-aided healthcare information retrieval by minimizing the latency of information delivery and reducing the redundancy of the information[16]. The NDN attains aggregation of requests hence various candidates can achieve information through one information delivery task[17]. The SDN searches for powerful providers by utilizing the titles hence the users can attain information from any best provider. The NDN permits the in-networking caching to minimize the distance among the information and users[18].

The medical sector presently employs "Information Technology (IT)" to offer smart devices that improve the diagnosis of health and offer effective and accurate treatment. The smart medical surveillance approaches and computerized healthcare diagnosis models offer services in multiple scenarios and environments that contain transportation, homes, workplaces, and hospitals helping to greatly reduce the doctor visit's cost and also to enhance the total standard of the sick person's care[19]. The smart medical applications and IoT sensors for the normal medical systems have highly modified the strategy of the medical sector as the amount of IoT systems in the medical sector utilized globally is validated to be higher than the 160 billion[20]. Embedded and wearable smart IoT sensors can gather the present time information, consisting of information related to the device's utility, mobility, and user habits[21]. This information is executed and garnered utilizing the deep learning and machine learning approaches to disclose the hidden patterns in the information and to discover the candidates to warn and diagnose about the complex situations[22]. The cloud-aware approaches that frequently utilize the mechanisms of big data evaluation can attain accurate and reliable outcomes for normal IoT developments that demand a quick response[23]. But, for severe healthcare IoT-aided developments that need a robust feature, present-time responses, and high accuracy, the cloud-aided frameworks can have a high impact on the bandwidth delay or network failure cases and this can lead to the healthcare emergencies or even the life loss[24].

The proposed work uses NDN based edge computing infrastructure that reduces cost and delay with decentralized data processing across the edge network. This work also integrates the efforts of the modified RPCSO for data sanitation, data restoration and optimized encryption with velocity and position based optimized encryption. The performance of the encryption is tested across various similar position based meta-heuristic bio-inspired algorithms such as OOA, SCO, MAO and CSO. The results shows the superiority of the proposed model in comparison to the existing models. The RPCSO-DSR outperforms the conventional schemes such as RSA, AES, DSR, ECC. These bio-inspired algorithms and encryption schemes are compared based on the computation time, restoration ratio, hidden ratio, block size and Mean Squared Error (MSE). They are also compared based on the correlation coefficient of Chosen Plaintext Attack (CPA) Known Plaintext Attack (KPA), key sensitivity analysis and restoration efficiency.

IoT-enabled healthcare systems by integrating the standard meta-heuristic approach with the NDN that offers a secured data sanitized and restored data.

- To perform a secure sanitization approach by employing the recommended RPCSO algorithm that supports an optimal key generation and provides authentication.

- To design an implemented RPCSO task by inheriting the features of conventional CSO that helps to optimize the multi-objective functions and also provides the secured functionality.
- To validate the functionality of the presented "NDN-based edge computing in IoT-enabled healthcare systems" adopted multiple conventional tasks with powerful performance attributes.

The recommended "NDN-based edge computing in IoT-enabled healthcare systems" includes the following modules. The state-of-art approaches are explained in Module II. The secure edge computing in IoT-enabled healthcare monitoring system: improved meta-heuristic algorithm for NDN is demonstrated in Module III. Further, the dataset details and novel meta-heuristic algorithm for developing the secured healthcare system are offered in Module IV. Then the optimal key generation and proposed architecture of sanitizing and restoring over the network layers is presented in Module V. Finally, the outcomes and the descriptions of the suggested "NDN-based edge computing in IoT-enabled healthcare systems" are given in Module VI. Finally, Module VII finalizes the recommended "NDN-based edge computing in IoT-enabled healthcare systems".

Existing works

Related works

In 2020, Li et al.[25] have presented a mechanism for SDN-aided edge computing in the IoT-aware medical model. In the implemented system, the IoT systems were verified by the servers of edge utilizing an approach called lightweight authentication. After performing the authentication, these systems have garnered information from the sick persons and transferred it to the servers of edge for evaluation, execution, and storage. The servers of edge were linked with the controller of SDN that processed the effective resource utilization, optimization of the network, and load balancing in the medical device. The presented task was estimated utilizing the computer-aided estimations. The solutions illustrated that the designed task offered better outcomes for the IoT-aided medical systems.

In 2020, Wang and Cai[26] have offered a secure medical management task combining NDN-aided IoT with the aid of edge cloud. This task utilized the NDN's merits to enhance the efficacy of the healthcare information retrieval and adopted the signature and ciphertext to help the security of the healthcare information delivery. The task was estimated and based on the outcomes the suggested task minimized the latency of healthcare information retrieval and the cost contrasted with the conventional solution.

In 2018, Rahman et al.[27] have constructed an "in-home therapy" maintenance approach that supported the nodes of IoT and the blockchain-aided sector to help always-available, anonymous, secure, and low latency data transmission within an "on-demand" information-sharing platform. This sector might offer an overall body joint limit of movement information for physically challenged people. The experiment outcomes from an overall execution of the approach displayed that it might help effectively a high amount of candidates.

In 2019, Alabdulatif et al.[28] have deployed an "Edge of Things (EoT)" task for smart and secure medical care surveillance devices. "Fully Homomorphic Encryption (FHE)" secured information privacy and was executed and secured within the method of EoT. It also illustrated the recommended task by estimating a study for the information of sick person's biosignal. This task highly improved the evaluation response period and functionality of the encrypted information executing while storing a high level of evaluation data privacy and accuracy.

In 2017, Elmisery et al.[29] have developed a task for the cloud medical care recommender system. The sick person's separate gateways were referred to as fog modes among the cloud medical care systems and IoHT systems. The recommended solution was combined into criteria concerning managing the patient's private medical information when employed by a cloud medical care recommended system to create medical perceptions. This task offered a better answer with precise outcomes that were advantageous to both service providers and patients.

In 2020, Jayaram and Prabakaran[30] have deployed the security task in the "patient-centric edge-cloud"-assisted medical care device. The network capacity and the response period utility were reduced in the recommended medical care device because of the efficient offloading and filtering tasks employed in the edge stage. The task enhances the estimation accuracy and prediction period of the disease while contrasting to the conventional classifier tasks. At last, the performance estimation and security of the implemented task were illustrated.

In 2018, Chen et al.[31] have implemented an "Edge-Cognitive-Computing-aided (ECC-aided) smart-medical care device. This task was capable to observe and estimate the user's physical information utilizing the cognitive evaluation. It tuned the resource allocation computing of the overall network. The research displayed that the ECC-aided medical care device offered a good candidate experience and tuned the resources of computing. Moreover, it enhances the patient's survival rates in emergency situations.

In 2020, Umar and Hossain[32] have addressed the classical and emerging edge frameworks and methods for the medical care systems and identified the challenges and requirements of diverse development situations. This experiment offered a comprehensive estimation of the utility of the cutting-edge-aided categorization and estimation mechanisms utilized for the edge intelligence. This work also provided a detailed overview of the common utility of the IoT answers in the edge sectors for the healthcare and medical treatment.

In 2022, Sashi Shreya et al.[33] describes the usage of biometric based authentication with login and password authentication with Burrows–Abadi–Needham algorithm to detect the well-known attacks on the medical network. It provides anonymity with personal identity.

In 2023, Christos Stergiou et al.[34] applied various technologies like, the Internet of Things (IoT), Wireless Sensor Networks (WSN), Cloud Computing (CC), and Machine Learning (ML), to hazardous viruses that infect people or animals causing threat to the normal sustainable human and animal life.

In 2023, Georgios Minopoulos et al.[35] integrated various applications like Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) that can accelerate drug discovery and detection process. Moreover, the integration of visualization techniques such as Virtual Reality (VR), Augmented Reality (AR), and Mixed

Reality (MR)) which are measured by the medical staff to provide the most accurate diagnosis and treatment for the patients.

Research gaps and challenges

The technique of smart healthcare has evolved in distinct countries, in which the healthcare facilities related to the pilot projects are investigated. In the case of IoT-enabled healthcare systems, the IoT device security and the related data are very significant and the Edge computing handles their processing as well as the computational problems. SDN-oriented Edge computing is useful in the effective usage of lessened resources of IoT devices. Yet, the related data as well as the less powered devices are vulnerable to several security threats. Table 1 lists the features as well as the challenges of the state-of-the-art SDN-based edge computing in IoT-enabled healthcare system methods. AI[25] offers better intelligent decisions and it also results in low latency, packet delivery ratio, and average response time. But, the privacy of patients is protected along with their data. NDN[26] helps the security of medical data delivery and also returns less complexity. Still, the cluster head reelection mechanism is not used. Blockchain[27] permits the leveraging of immutabilities of metadata and the limitations of the high bandwidth are also avoided. Yet, the off-chain storage time is not minimized. FHE[28] preserves a high level of data privacy as well as analysis accuracy and the data is analyzed and stored in an encrypted format. But, it cannot be used for the advanced data mining models. Fog-based middleware[29] minimizes the mean absolute error and also enhances the privacy. Still, it does not perform the experiments on several real datasets from the UCI repository. SECHS[30] reduces the network capacity as well as the response time and also reduces the cost of resource provisioning at the cloud layer. Yet, it does not deal with the transmission protocol and edge-to-edge secure object tracking. ECC[31] reasonably optimizes the computing resources and also provides a better user QoE. But, an emotional recognition system is not constructed. AI[32] identifies the challenges and demands of distinct application scenarios and also enhances the edge computing services for the healthcare. Still, the information processing management as well as the local storage is not addressed. Hence, these challenges have drawn the attention to developing a novel method in the field of SDN-based edge computing in IoT-enabled healthcare systems.

Research gaps that are addressed in the proposed system when compared with the existing systems is given in the below discussion in detail.

- The proposed work performs preprocessing of data with data sanitation and data restoration which were not used in the existing systems. This preprocessing increases the performance of the encryption. The data sanitation process is a unique feature of the proposed work, which hides the sensitive patient data from the unauthorized users. The data restoration process with key generation and exchange of the RPCSO ensures that the intended users are only allowed to access the sensitive information related to the patient data. Thus, the proposed work not only ensures the optimization but also provides data privacy and security.
- The edge computing ensures that low latency on the data storage and processing. This low latency is due to the presence of the position optimization of RPCSO and NDN edge interface. The best position identification is done based on the ratio of the best position with the product of average and worst positions. This enhances the performance and reduces the time. The proposed model has reduced the hidden and preservation ratio when compared with the existing models.

Author [citation]	Methodology	Features	Challenges
Li et al.[25]	AI	It results in low latency, packet delivery ratio, and average response time	It protects the privacy of patients along with their data
		It offers better intelligent decisions	
Wang and Cai[26]	NDN	It returns less complexity	It does not use the cluster head reelection mechanism
		It helps the security of medical data delivery	
Rahman et al.[27]	Blockchain	It avoids the limitations of the high bandwidth	It does not minimize the off-chain storage time
		The leveraging of immutabilities of metadata is permitted	
Alabdulatif et al.[28]	FHE	It analyses and stores the data in an encrypted format	It cannot be used for the advanced data mining models
		It preserves a high level of data privacy as well as analysis accuracy	
Elmisery et al.[29]	Fog-based middleware	It enhances the privacy	The experiments are not performed on several real datasets from the UCI repository
		It minimizes the mean absolute error	
Jayaram and Prabakaran[30]	SECHS	The cost of resource provisioning is reduced at the cloud layer	It does not deal with the transmission protocol and edge-to-edge secure object tracking
		It reduces the network capacity as well as the response time	
Chen et al.[31]	ECC	It provides a better user QoE	It does not construct an emotional recognition system
		It reasonably optimizes the computing resources	
Umar and Hossain[32]	AI	The edge computing services are enhanced for the healthcare	It does not address the information processing management as well as the local storage
		It identifies the challenges and demands of distinct application scenarios	

Table 1. Features and challenges of state-of-the-art Sdn-based edge computing in Iot-enabled healthcare system.

- Meta heuristic algorithms assure the optimization of the encryption process which is essential for a system working on human body sensors. The performance of the models is compared based on the computation time, restoration ratio, hidden ratio, block size and Mean Squared Error (MSE). They are also compared based on the correlation coefficient of Chosen Plaintext Attack (CPA) Known Plaintext Attack (KPA), key sensitivity analysis and restoration efficiency. The proposed work outshines the rest of the existing models in comparison based on all of the above mentioned parameters.
- RPCSO algorithm is used for node optimization, that ensures the minimization of delay in selection of the data node, which is the novel contribution of the work. This is because the fitness evaluation is done based on the ratio of the best position with the product of average and worst positions. The conventional CSO algorithm used seeking and tracing mode to find the best position, which is based on NP-Hard problem, therefore complex to develop and apply in practically large input data.
- Integrating all the aspects, the proposed work is efficient, cost-effective, secured, reliable and low-latency system, which has all the essential requirements for an effective health-care management system.

Materials and methods

This section includes various aspects of the proposed work such as IoT based security systems, Edge computing and NDN-based IoT Connected Healthcare System , which is the overall system architecture including the data acquisition system, data processing system and the data analysis system used in the proposed work. The overall process description is also provided in this section including the data restoration, encryption, and performance analysis of the encryption process with the decypted data.

IoT and its security

IoT[26] Millions of systems are linked to the Internet. These systems are enhancing simultaneously. This count enhanced by 2.5 times in the upcoming years because of the concept of IoT that is the basic mechanism of the upcoming linked globe. The IoT is the modern technology in the data transmission that is the interconnection of the conventional systems with the extra intelligence. These systems are performing the detected information and transmit it to other systems via the Internet. At first, the IoT systems are performed in the unlicensed band utilizing the ZigBee and Bluetooth technologies. Presently, the 4G mobile frameworks are employed for the deployment of the IoT. But, these frameworks do not satisfy the demands of IoT, and modern mechanisms are required to enhance the capabilities of the conventional strategies. Other than the restrictions of short-range communication of these systems, the IoT systems have densely populated in the unlicensed spectrum. Hence, it has resulted in multiple experimental problems and opportunities for the experimental society. For instance, the IoT systems can utilize the licensed spectrum effectively utilizing the idea of the "Cognitive Radio". A CR can able to utilize the licensed spectrum when it is available and this creates IoT systems applicable to a wide range of developments. Likewise, the "Licensed Spectrum Access (LSA)" notion in the 5G that has a development of the CR idea is another experimental region. Thus, the IoT developments are enlarging into multiple platforms that create various difficulties such as privacy and security of IoT networks and the systems.

Security in IoT The IoT systems which are resource-constrained are susceptible to multiple attacks that highly affect their functionality. To safeguard the IoT-aware frameworks, the traditional cryptographic mechanisms not performing well and leading to critical security attacks. These attacks can be passive or active and may be deployed from the outside or inside of the network. There are multiple security threats on IoT that may stop the transmission of the network like eavesdropping, sniffing, replay, and so on. But the "Denial of Service (DoS)" and Sybil threats are highly threatening as they exhaust the bandwidth of the network and the system resources.

Edge computing

Edge computing is an efficient and economical platform that enlarges the cloud computing. It offers minimal delay information services by offering the computing assets near to the IoT-aware network's edge. The goal is to decrease the traffic load and execution from the resource-constrained IoT systems to capable edge servers. Hence, the load balancing is attained that leads to mobility assistance and low latency. The edge computing is a powerful technology for the developments of IoT that has multiple merits; for instance the energy-efficient transmission among the IoT developments, IoT nodes in the vehicular frameworks, actuator, and sensor networks. Moreover, it is best employed in the developments such as the medical sector that need context-aided execution to delay-sensitive information. The experts have employed the clustering idea for the decentralized edge computing to enhance the execution abilities of the entire device. Experts have utilized the multi-channel to diminish the latency and enhance the stability of the model in the real-world developments. Moreover, some of the research scholars have employed the edge computing in a safe brain-to-brain transmission. The scholars have employed a "wireless electroencephalogram headset" utilizing which the receiver attains the sender's thoughts. For instance, if the sender considers a number of words, then attains it.

NDN-based IoT connected healthcare system

The NDN[36] has developed as a potential mechanism to win over the issues and provide answers to the data-sensitive Internet developments. The NDN attains better data delivery according to the consumer and produces. One of the important demands for the medical care observation device is to process real-time execution and communication of the medical care information created from the IoT wearable and systems. The execution abilities of the hardware systems have offered a high enhancement, but the transmission devices still depend on the protocol legacy and are not entirely enable to offer the needed scalability in their developments. To rectify this issue the NDN has become an effective task because of its effective data delivery task as contrasted to the conventional transmission tasks. The NDN-IoT-aided medical care architecture is a successful answer for effective

information. This framework gathers information from multiple installed sensors on the human body, utilizes the lightweight operations and captures the producer place, and attains the delivery of on-demand information for the consumers. The NDN has multiple factors such as forwarding, routing, security, catching, and naming. This NDN provides various merits such as content caching to minimize the network congestion and enhance the delivery speed of the data, effortless configuration of the network systems, and constructing the building security into the framework at the information level. The "NDN-based IoT-connected healthcare system" is diagrammatically shown in Fig. 1. The overall process representation as a flow chart is represented as Fig. 2

Figure 1 has two sections such as the producer layer and the consumer layer. The producer layer is basically the layer that acquires the data from human body sensors through SDN-IoT integrated framework. The resource constrained framework is connected to the edge infrastructure, which provides parallel data distribution with decentralization. This entire producer layer supports the data processing with data sanitation, data restoration which enhances the performance of the encryption. Then the data is analyzed in the consumer layer once the encryption is applied with RPCSO optimization. This algorithm is applied for enhancing the performance of encryption. The arrival of the best position, velocity of the solution, with respect to the number of iterations is measured for best, worst, mean, median and standard deviation during the data analysis in the consumer layer. The performance of the models is compared based on the computation time, restoration ratio, hidden ratio, block

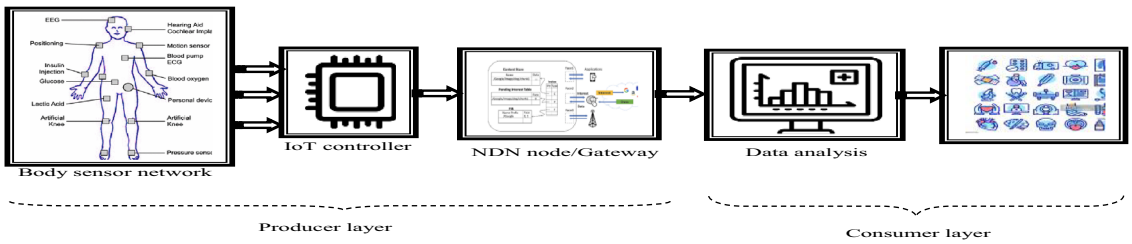

Fig. 1. Diagrammatic representation of the NDN-aided IoT-connected healthcare system.

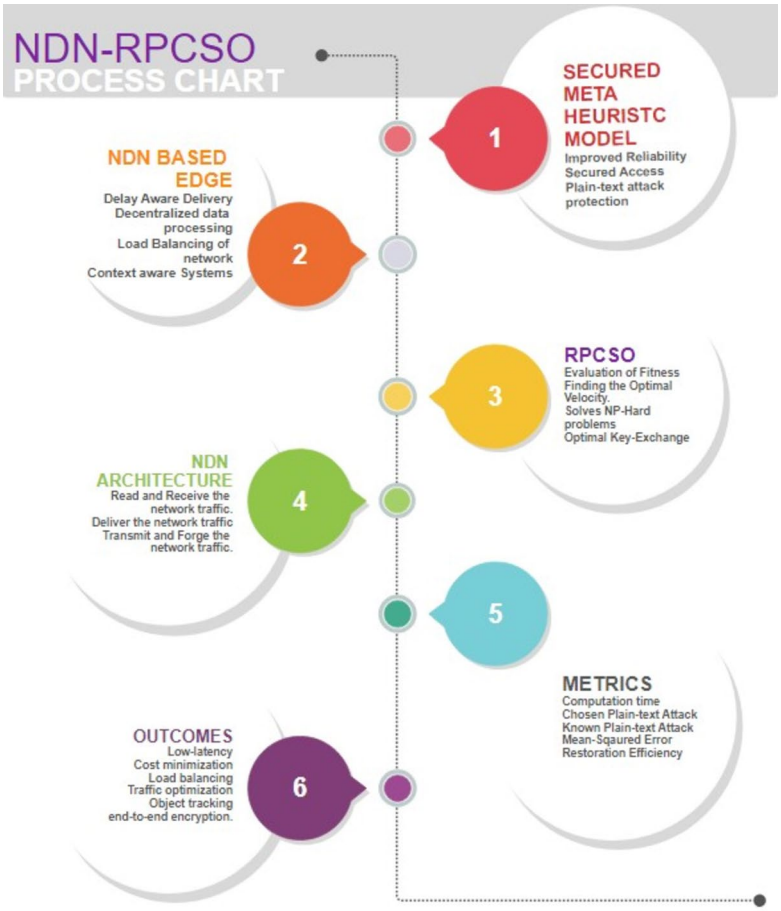

Fig. 2. Overall process description with flow chart with various aspects of the proposed work.

size and Mean Squared Error (MSE). They are also compared based on the correlation coefficient of Chosen Plaintext Attack (CPA) Known Plaintext Attack (KPA), key sensitivity analysis and restoration efficiency.

Dataset details and novel meta-heuristic algorithm for developing the secured healthcare system

Healthcare data details

The details of the healthcare data utilized for the suggested secured healthcare system are provided here.

Dataset 1 ("Diabetes Dataset ") this data source is collected from the source named Kaggle via the link: "https://www.kaggle.com/datasets/saurabh00007/diabetescsv" "access date: 2023-09-27". This is in the format of csv. It includes 9 columns.

Dataset 2 ("Heart Disease Dataset") this data source is also acquired from the Kaggle platform through the hyperlink: "https://www.kaggle.com/datasets/yasserh/heart-disease-dataset" "access date: 2023-09-27".This includes 76 attributes. It is integer integer-valued source when the values start from 0 to 4.

Dataset 3 ("Maternal Risk Dataset") this data source is also acquired from the Kaggle platform through the hyperlink: https://archive.ics.uci.edu/dataset/863/maternal+health+risk "access date: 2023-08-14".Data has been collected from different hospitals, community clinics, maternal health cares from the rural areas of Bangladesh through the IoT based risk monitoring system. This dataset contains 1013 instances and 6 columns of the real-time IoT measured patient data.

From the above-mentioned data sources the attained data is specified as S_d, *here* $d = 1, 2, 3, ...D$, and the total amount of data is indicated as D.

The datasets contain data related to the human body sensors, which can provide the realistic experience of how these data could be acquired in the real-time environment from the human body. The third dataset contains real-time maternity data acquired through IoT sensors from various hospitals and health centers in Bangladesh. Moreso these datasets have numerical values and don't have any bias or unrealistic data, which can disturb the performance of the proposed algorithm. With simple and essential features, these datasets can be really useful to significantly examine the superiority of the proposed algorithm.

Traditional CSO

CSO[37] In order to ensure the efficacy of the employed computationally intelligence-aided functionality of the cats the conventional CSO is developed. This CSO rectifies one of the NP-hard issues called the "open shop scheduling" issue that is faced by various manufacturing and industrial developments. The traditional CSO is partitioned into two modes such as "Seeking Mode (SM)" and the "Tracing Mode (TM)" mode. The cat's rest time is normally referred to as SM mode where it utilizes most of its lifespan. On the other hand, the TM mode refers to the hunting or preying time of the cat. Each cat is featured by its own velocity, flag, and position to detect whether the cat is presented in the TM or SM mode. In this CSO task, the suggested two modes are integrated by the "Mixture Ratio (MR)".

SM This mode considers the resting phase of the cat and also as being aware of its neighborhood for its next activity. With the support of the schedule vector, the position is offered. In this SM, there are four attributes. The fundamental stages of the SM are explained here.

- Assign a a replica of the current cat's c place with $a = SMP$. The specific cat is taken as one of the candidates when if the SPC's value is true or $a = SMP - 1$.
- Create a new SRD's arbitrary value.
- If the value of fitness is unequal, then estimate the likelihood of every member with the aid of Eq. (1), and the value of default likelihood for every member is set as 1.
- Process the mutation and change the present place.

$$Q_b = \frac{|fs_b - fs_{\min}|}{fs_{\max} - fs_{\min}}, \ where \ \ 0 < b < a \tag{1}$$

From the above steps, the SMP is considered as the SM's replica count of the cats. Then the SPC is referred to as a Boolean value and the SRD is the initial range in the chosen answer vector. In addition, the cat's fitness is denoted as fs_b and the swarm's maximum fitness is specified as $fs_{\max}$. Also, the swarm's minimum fitness is pointed as $fs_{\min}$.

TM This mode considers the rapid motion of the cat based on its own velocity when hunting a prey or any other object which is in movement. The TM's processes are given as follows.

- Based on Eq. (2), the velocity of every cat c is updated.
- Examine if the velocities are in the highest phase.

$$v_c' = w * v_c + z * g * (Q_{bst} - Q_c) \tag{2}$$

- Upgrade the cat's c position based on Eq. (3).

$$Q_c' = Q_c + v_c \tag{3}$$

Here, the factor v_c refers to the cat's velocity, and also the cat's c best place is denoted as Q_{bst} that has the best fitness measure. The cat's c updated velocity is specified as v_c' and the weighted attribute's inertia is pointed as w. In addition, the constant factor is indicated as g. The conventional CSO utilizes the random integer that selects the variable arbitrarily. This leads to the inaccurate results and poor functionality. In order to resolve this issue in the modern RPCSO task, a new random variable z is estimated based on the fitness values. This is formulated in Eq. (4). Moreover, the cat's c actual place is denoted as Q_c, and the cat's new place is pointed as Q_c'. The conventional CSO scheme's pseudo-code is given in Algorithm 1.

```
Consider the population factors and the initialization attributes
Find out the objective function
For u = 1 to U_max
        Process the seeking mode
        Perform the mutation and change the place of an individual utilizing Eq. (1).
        Perform the tracing mode
        Validate the highest place velocity employing Eq. (2)
        Upgrade the best position
End
```

Algorithm 1. Classical CSO

Novel RPCSO

The conventional CSO is a computational intelligent approach motivated by the cat's behavior. It supports solving the NP-hard issues and offers effective computational solutions. It also produced the outcomes in the less amount of time. However, when the input amount increases, it gives poor performance and also because of the random variable utilization, the results are prone to error. Hence, a new RPCSO scheme is presented. Instead of selecting the integer randomly, this RPCSO algorithm utilizes fitness values to select the integer. The estimation of the new random integer z is shown in Eq. (4).

$$z = \frac{bfit}{(wfit * mfit)} \tag{4}$$

Here, the worst fitness value is specified as $wfit$, and the best fitness value is pointed as $bfit$. In addition, the mean fitness value is denoted as $mfit$. This new random variable is replaced in the conventional CSO algorithm's velocity estimation which is formulated in Eq. (2).

The newly implemented RPCSO's pseudo-code is presented in Algorithm 2. In addition, the flow chart for the designed RPCSO is given in Fig. 3.

```
Consider the population factors and the initialization attributes
Find out the objective function
For u = 1 to U_max
    For j = 1 to m_ppn
        Validate the random variable z by employing Eq. (4)
        Process the seeking mode
        Perform the mutation and change the place of an individual utilizing Eq. (1).
        Perform the tracing mode
        Validate the highest place velocity employing Eq. (2)
        Upgrade the best position
    End
End
        Do the iterative process
        Attain the optimum solutions
```

Algorithm 2. RPCSO

Optimal key generation and proposed architecture of sanitizing and restoring over the network layers

Optimal key generation

In the recommended architecture, the extraction of keys offers a high part in the both restoration and the sanitization operation. Here, the optimization is performed with the support of the designed RPCSO algorithm. The transformation of the answer is the initial phase of the development of the key. In this, the key ky is changes as another form with the help of the "Kronecker" approach. After that, the key is changed into ky_1 by employing Eq. (5) in that the size is taken to be $\sqrt{no''} \times Q_{\max}$. For instance, the key matrix is created and given in Eq. (5) for the key = {9, 8, 3}.

$$ky_1 = \begin{bmatrix} 9 & 9 & 9 \\ 8 & 8 & 8 \\ 3 & 3 & 3 \end{bmatrix}_{\left[\sqrt{no''} \times q_{\max}\right]} \tag{5}$$

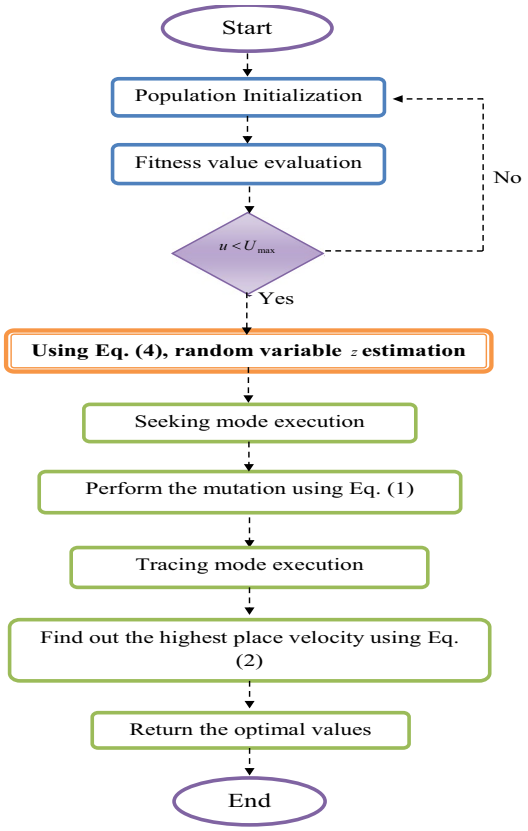

Fig. 3. The suggested RPCSO algorithm's flow chart.

The variable *no* is indicated as the transaction number and the factor no'' is denoted as the "number's nearest highest perfect square". Further, the variable Q_{max} specified as the highest transaction length. According to Eq. (6), the recreated key matrix ky_1 is generated by processing the duplication of row-wise. Besides, the key matrix ky_2 is created with the support of the "Knonecker" approach and it is formulated in Eq. (6).

$$ky_2 = ky_1 \otimes ky_1 \tag{6}$$

The "Kronecker's" product is denoted as $\otimes$ and the size of ky_2 is also denoted as $\sqrt{no''} \times Q_{max}$. In this, the primary goal of the suggested task is the key optimization denoted as utilizing the recommended RPCSO algorithm. The optimal key construction task utilizing suggested RPCSO is depicted in Fig. 4.

Proposed architecture process with different layers in NDN

In the recommended framework, the systems are classified into IoT systems, user systems, and edge systems. The IoT systems[26] are partitioned into cluster candidates that are accountable for monitoring and taking the healthcare information and the cluster heads that are responsible for gathering the healthcare information from the members of the cluster. Every sick person is assigned with a various cluster candidates and a cluster head that can be constructed into a fabric belt. Based on the category of the system, the framework includes the user layer, edge cloud layer, and patient layer. The patient layer includes the cluster candidates and the cluster heads periodically gather the healthcare data detected by the cluster candidates. After that the transfer the gathered information to an edge cloud for the purpose of catching. After that, the edge cloud layer is integrated with the edge systems that provide computation and storage systems for quickly catching and offering the healthcare information. Furthermore, the user layer includes user systems like computers that utilize the merits of NDN to attain secure and effective healthcare information acquisition. According to the hierarchical layers, the framework for the hierarchical medical care monitoring is recommended. In this task, a work contains the prefix that indicates a healthcare sector like a hospital, the patient is referred by the patient IOD, and the category of the healthcare data like blood pressure is detected by the medical data ID. The prefix is supported to explain each system. The edge system's downstream interface connects with a user system or cluster head and then the edge systems are linked by the upstream interfaces. For the IoT-assisted devices, an adversary must consider several capabilities.

1. Read and receive the overall network traffic.
2. Deliver the network traffic.
3. Transmit and Forge the network traffic.

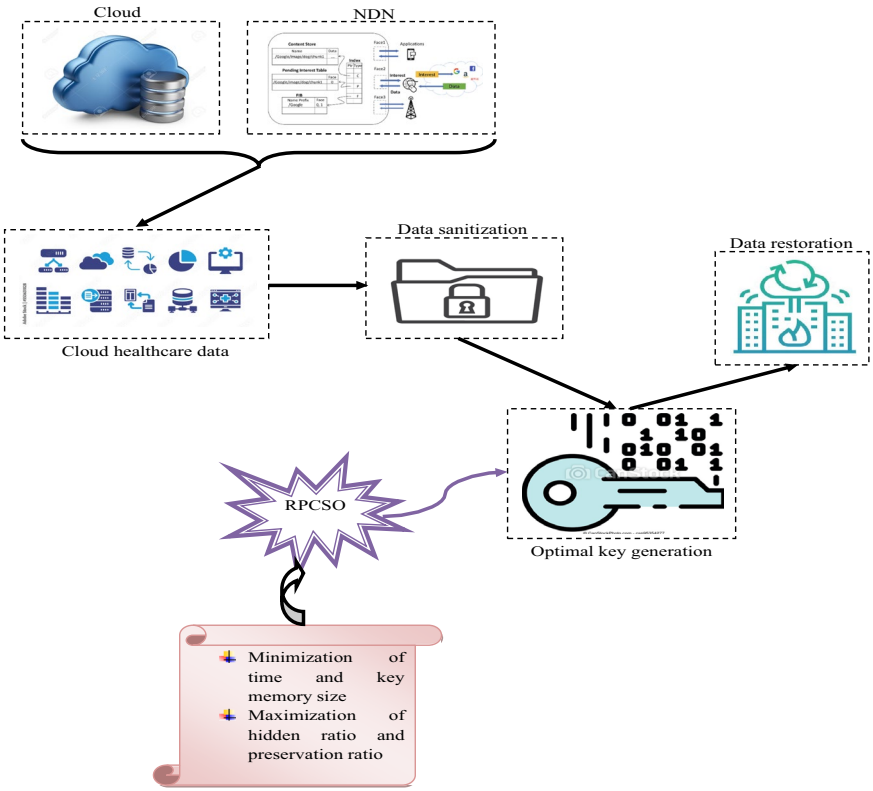

Fig. 4. The RPCSO-based optimal key generation task.

According to the abilities, an attacker can deploy multiple threats including the spoofing and eavesdropping. Since the encryption and hash approaches can change the plain text to cipher text, experts utilized the suggested architecture to attain the security of the data delivery in the healthcare sector. If there exist Y prefixes, for the y^{th} prefix Px_y $\left(1 \le y \le Y\right)$ then the "Trusted Authority (TA)" creates a shared key K_y and offers a one-way hash function H_y. This is derived in Eq. (7).

$$K_y = KG\left(Px_y, MasterKey\right) \tag{7}$$

The term's Px_y hash prefix HPx_y is formulated in Eq. (8).

$$HPx_y = H_y\left(Px_y, K_y\right) \tag{8}$$

If the edge system Es_y is estimated by the variable Px_y then it is offered with the factor HPx_y. If the register of patients Z with the healthcare institute HI_{yz} considered by the variable Px_y, then for the z^{th} sick person Pa_{yz} $(1 \le z \le Z)$ the general TA in creates the shared key K_{yz} and offers a one-way hash function H_{yz}. This is expressed in Eq. (9).

$$K_{yz} = KG\left(Pa_{yz}, MasterKey\right) \tag{9}$$

For any healthcare data MD_{yza} of the variable Pa_{yz}, if the factor MD_{yza} is considered by the name Na_{yza} where the variable Px_y is denoted as a prefix. Then if the sick person's ID is denoted as SID_y and the healthcare information ID is specified as HID_z, then the variable is pointed as $HPID_{yz}$ the hash patient ID of the variable SID_y. This is shown in Eq. (10). Moreover, the ID of hash medical data is indicated as $HMID_{yza}$ for the variable HID_a and this is derived in Eq. (11).

$$HPID_{yz} = H_{yz}\left(SID_z, K_{zy}\right) \tag{10}$$

$$HMID_{yza} = H_{yz}\left(MID_z, K_{zy}\right) \tag{11}$$

The hash name HNa_{yza} of the variable Na_{yza} is denoted as $HPx_y/HSID_{yz}/HMID_{yza}$ and the factor's MD_{yza} encryption healthcare information EMD_{yza} is formulated in Eq. (12). If an authorized candidate like the doctor is legalized to access MD_{yza} then, he is offered with K_{yz} *and* HNa_{yza}. In addition, every legal edge system or IoT system is constructed with the private and public keys.

$$EMD_{yza} = Encrypt\left(MD_{yza}, K_{yz}\right) \tag{12}$$

The data sanitization is the operation of concealing the sensitive information or data that helps to avoid the data from revealing on to the illegal users. In addition, the restoration is the inverse operation of the data sanitization task that is performed to estimate the sanitization task's efficacy. During the task of data sanitization, the binary conversion is performed for both the creation of the key matrix and data. The recommended RPCSO algorithm is utilized to create the optimal key. The suggested "NDN-based edge computing in IoT-enabled healthcare system" architecture is provided in Fig. 5.

The primary goal of this task is to implement a safe architecture for edge computing in the IoT-aided medical care model utilizing the heuristic-aided authentication and NDN. There are three layers in the recommended task such as patient layer, the edge cloud layer, and the user layer. In the initial layer, various IoT systems are linked together, and utilizing the cluster head data, the sick persons transfer their information to the layer of the edge cloud. The layer of edge cloud is accountable for computing and storage assets for quickly offering and caching the health care information. Thus, the patient layer is an advanced heuristic-aided sanitization approach named RPCSO with NDN to cover up the sensitive information that must not be revealed to the unauthorized candidate. The approach of authentication utilizes a multi-objective function key development task concerning the factors such as modification degree, preservation rate, and hiding failure rate. In addition, the information from the edge cloud layer is sent to the user layer, where the generation of the optimal key with NDN-aided restoration is processed, hence attaining secure and effective healthcare data retrieval. The task is estimated quantitatively on multiple healthcare data sources from the Kaggle and UCI repositories and the research evaluation displays the superior functionality of the recommended system considering cost and latency when contrasted over classical solutions.

Objective function and its constraint specification

The suggested "NDN-based edge computing in IoT-enabled healthcare systems" helps to sanitize and restore the data. The sanitization supports hiding the data and the restore operation is the reverse operation of the data sanitization. The data sanitization operation secures the sensitive information and reduces the assets disposal. Moreover, the data restoration approach is cost-effective and provides the simplified management. However, the data sanitization operation does not provide the location of the hidden data and is also very time-consuming.

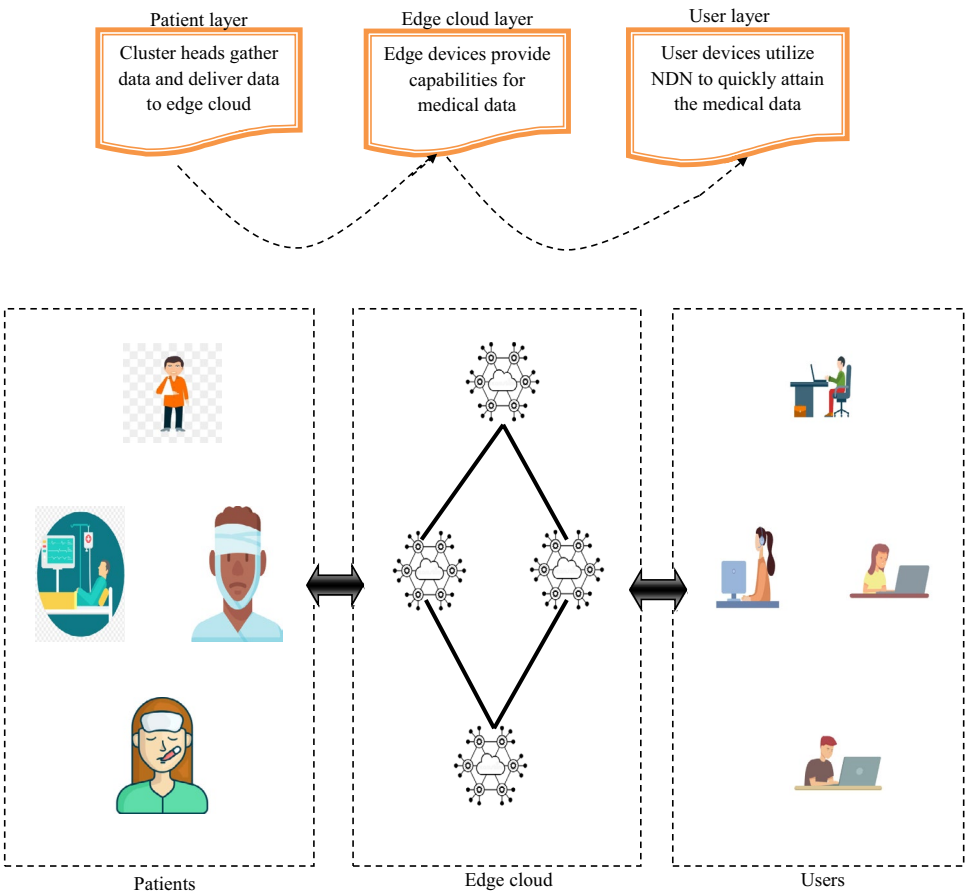

Fig. 5. The architecture of the recommended NDN-based edge computing in IoT-enabled healthcare system.

Similarly, the data restoration task is very complex, and overall data restoration demands more safety control, storage space, and time. Hence, the suggested "NDN-based edge computing in IoT-enabled healthcare systems" assists in providing more effective data sanitization and data restoration tasks. In this task, a binary format key is utilized to perform the tasks. This key is optimally tuned by the recommended RPCSO algorithm. At first, the raw data S_d is given as an input. After that, the data is sanitized S_d^{san} with the support of the edge cloud layer. Next, the sanitized data S_d^{san} is restored S_d^{res} by the user layer with the support of the optimal key. The objective function for the key optimization is shown in Eq. (13).

$$ob = \arg \min_{\{Ke_g\}} \left[T + Ms + \frac{1}{\Pr} + \frac{1}{Hr} \right] \tag{13}$$

Here, the optimized key is denoted as Ke_g which is in the binary format i.e., 0 or 1. Moreover, the factor T denotes the time and the factor Ms specifies the memory size of the key. The preservation and the hidden ratios are represented as $\Pr \quad and \quad Hr$ correspondingly. These constraints are explained as follows.

Time T "It is the factor which is estimated to complete the overall process".

Memory size of key Ms "It is the validation of how much memory is utilized for the optimal key".

Preservation ratio Pr "It is the reciprocal of the data loss and it is formulated in Eq. (14).

$$\Pr = \frac{I_2}{TI} \tag{14}$$

Here, the variable I_2 points to the amount of zero indices, and then the term TI denoted as the overall amount of data indices which are preserved.

Hiding Ratio Hr "It is the rate of sensitive data that are effectively hidden". It is given in Eq. (15).

$$Hr = \frac{I_1}{TP} \tag{15}$$

In this, the factor I_1 specifies the amount of data indices which have to be hidden, and the length of the non-zero indices is referred to TP.

Results and discussions

Simulation setup

The implemented "NDN-based edge computing in IoT-enabled healthcare system" was executed with the support of Pycharm and research experiments were conducted. The length of the chromosome was 16 for the offered work and the utmost iteration of the designed "NDN-based edge computing in IoT-enabled healthcare system" was 50. In addition, the involved population was 10 for the suggested "NDN-based edge computing in IoT-enabled healthcare systems. The simulations are executed based on several conditions such as best, worst, mean, median and standard deviation for various iterations. The position and velocity optimization with respect to the Computation time, Hidden Ratio, Preservation Ratio, Memory size and the Mean Squared Error are compared for the algorithms OOA, SCO, CSO, RPCSO, MAO. The encryption metrics such as RSA, ECC, DSA, RPCSO-DSA and AES are also compared for the Computation time, Hidden Ratio, Preservation Ratio, Memory, Mean Squared Error, correlation coefficient of KPA, CPA, key sensitive analysis and the restoration efficiency.

Performance metrics

Some of the performance attributes are employed in the recommended "NDN-based edge computing in IoT-enabled healthcare system's" experimental analysis. They are described below.

Computation time "The amount of time utilized to do the computation". The complexity of the instructions in an algorithm and number of the conditional statements executed by the algorithm decides the time complexity. The proposed method applies the RPCSO algorithm with edge NDN architecture that reduces the computational complexity with the decentralized data distribution. This reduces the cost and latency of the algorithm. The performance is tuned by modified RPCSO algorithm.

Chosen Plaintext Attack (CPA) "It is the cryptanalysis threat that considers the attacker can attain the cipher texts for random plain texts". The goal of the attack is to reduce the message security by gaining the most common cipher text. The victim receives the text with the complete random text injected by the attackers.

Known Plaintext Attack (KPA) "It is the cryptanalysis threat that has access to both the plain text and its encrypted format". The attackers gain access to the codebook that contains both the plaintext and the modified ciphertext. This allows the attacker to modify the message according to his wish. The proposed method uses data sanitation, data restoration and then encryption using the RPCSO optimization algorithm. Thus, these attacks are eliminated and the message are protected from the attackers.

Mean Squared Error (MSE) "It estimates the number of errors in statistical approaches".

$$MSE = \frac{1}{n} \sum_{h=1}^{n} \left(Z_h - \hat{Z}_h \right) \tag{16}$$

In this, the data point count is denoted as n and the observed values are specified as Z_h. Moreover, the predicted values are indicated as $\hat{Z}_h$. A larger MSE indicates that the data points are dispersed widely around its central moment (mean), whereas a smaller MSE suggests the opposite.

Restoration efficiency "It is the efficacy of restoring the data that have been damaged by the threats". This is the measure of the data loss and data recovery, after the data is recovered from a cyber-attack. The ability to rebuild the original data is measured by the Restoration efficiency.

The implemented RPCSO algorithm's convergence validation over multiple traditional algorithms

The presented RPCSO algorithm's convergence is verified with the aid of the iteration number over multiple heuristic algorithms which is shown in Fig. 6. The suggested RPCSO task's convergence is raised by 96.6% of OOA-DSR, 88% of MAO-DSR, 96.6% of SCO-DSR, and 93.3% of CSO-DSR correspondingly for the first data source in Fig. 6a when the execution number is 15. Hence, it is proved that the designed RPCSO has higher convergence values than the other conventional tasks.

The presented RPCSO task's statistical examination over diverse heuristic algorithms

The offered RPCSO scheme's statistical research is illustrated in Table 2 against diverse traditional algorithms for the two suggested data sources. For the second data source, the median of the offered RPCSO is enriched by 21% of OOA, 71% of MAO, 15.3% of SCO, and 27.5% of CSO appropriately. Therefore, it is portrayed that the implemented RPCSO has better functionality rates than the other normal tasks. Table 2 describes the performance

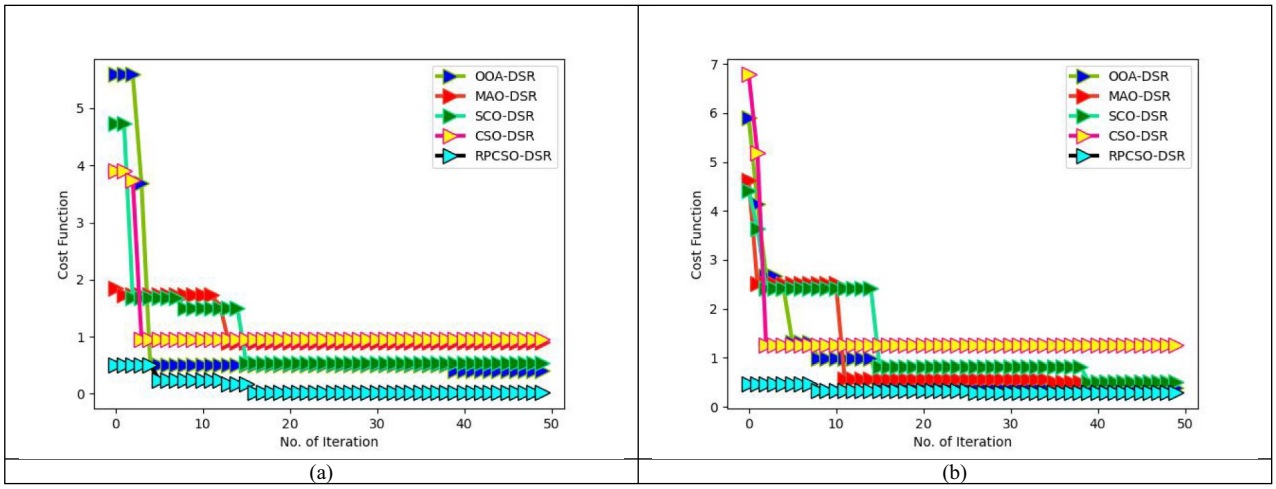

Fig. 6. The presented RPCSO algorithm's convergence verification over multiple optimization algorithms concerning " (**a**) Dataset 1, and (**b**) Dataset 2".

Terms	OOA[6]	MAO[7]	SCO[8]	CSO[37]	RPCSO
"Dataset 1"					
"Best"	0.410454063	0.910353282	0.540082612	0.95338818	0.018069361
"Worst"	5.590398129	1.854675877	4.732999093	3.911659805	0.50564046
"Mean"	0.858517903	1.121954178	0.979063144	1.127535332	0.112643119
"Median"	0.512931198	0.910353282	0.540082612	0.95338818	0.018069361
"Std"	1.277195814	0.358400811	0.891855501	0.689565445	0.156968355
"Dataset 2"					
"Best"	0.393224171	0.513451788	0.499691011	1.253183911	0.283597992
"Worst"	5.903362433	4.626162077	4.414968986	6.781762824	0.467442652
"Mean"	0.849215097	1.016578404	1.293196278	1.442212249	0.32920734
"Median"	0.393224171	0.559887285	0.816502108	1.253183911	0.328581887
"Std"	1.035067652	0.93836552	0.940730313	0.93986443	0.063687386
"Dataset3"					
"Best"	0.437125662	0.934212309	0.572310456	0.962341234	0.02134224
"Worst"	5.621305692	1.873402142	4.765423472	3.934201234	0.52342276
"Mean"	0.872134569	1.145601235	0.987321452	1.142533023	0.13421178
"Median"	0.532456709	0.930124212	0.560023451	0.972290342	0.030311272
"Std"	1.294768142	0.373324521	0.912307832	0.703324567	0.173422378

Table 2. The offered RPCSO algorithm's statistical examination over diverse traditional heuristic approaches.

of the various algorithms in different scenarios such as Best, Worst, Mean, Median and Average performance measurements with respect to the attainment of the best solution for the position. In comparison with the predecessors the RPCSO outperformed the rest of the models with the best results in all the cases for both the datasets used for the measurements. RPCSO also reduces the key memory size and the maximization of the hidden and preservation size. Figure 6 shows how various evolutionary algorithms reduce the cost function in-terms of the computational complexity, as per the progression of the iteration of these algorithms in attaining the best solution of the position and the velocity. As per the Fif.5 the RPCSO shows lowest cost function, compared with all other similar existing algorithms and reaches the ideal solution in lesser iterations compared with the other evolutionary algorithms.

The performance estimation of the implemented NDN-based edge computing in IoT-enabled healthcare systems over various algorithms and cryptography mechanisms

The offered "NDN-based edge computing in IoT-enabled healthcare" system's functionality is examined over diverse classical algorithms and cryptography approaches for the two benchmark data sources. This functionality verification is presented in Figs. 7, 8, 9, and 10. For the first data source in Fig. 7a, the implemented "NDN-based edge computing in IoT-enabled healthcare" system's computation time is minimized by 4.6% of OOA-DSR, 8% of MAO-DSR, 1.8% of SCO-DSR, and 1.2% of CSO-DSR accordingly when the size of the block is 15. Hence, the designed "NDN-based edge computing in IoT-enabled healthcare systems" has attained superior functionality than the other conventional works.

The suggested NDN-based edge computing in IoT-enabled healthcare system's correlation coefficient for attack analysis over multiple optimization algorithms and cryptography tasks

Figures 11 and 12 depict the correlation coefficient for CPA attack analysis to the recommended "NDN-based edge computing in IoT-enabled healthcare systems" over multiple traditional algorithms and cryptography tasks. Likewise, Figs. 13 and 14 offer the correlation coefficient for KPA attack estimation of the presented "NDN-based edge computing in IoT-enabled healthcare systems" over diverse heuristic approaches and the cryptography tasks. From Fig. 14b, the correlation coefficient for KPA attack estimation is reduced by 86.3% of RSA, 79% of AES, 82.3% of ECC, and 86.6% of DSR appropriately for the second dataset when the case value is 3. Hence, it is ensured that the presented "NDN-based edge computing in IoT-enabled healthcare systems" has a more powerful attack analysis capacity than the other normal solutions.

The presented NDN-based edge computing in IoT-enabled healthcare system's correlation coefficient for key sensitive analysis over distinct algorithms and methods

The correlation coefficient for key sensitive analysis to the implemented "NDN-aided edge computing in IoT-enabled healthcare system" over diverse traditional algorithms and cryptography approaches are illustrated in Figs. 15 and 16 for the two standard data sources. When the key percent value is 30 for the first dataset in Fig. 15a, the correlation coefficient for key sensitive analysis to the developed "NDN-aided edge computing in IoT-enabled healthcare system" is diminished by 96.8% of OOA-DSR, 97.6% of MAO-DSR, 96.9% of SCO-DSR, and 97.8% of CSO-DSR correspondingly. Therefore, the constructed "NDN-aided edge computing in IoT-enabled healthcare system" has better security than other mechanisms.

The restoration efficiency examination of the offered NDN-based edge computing in IoT-enabled healthcare system over multiple conventional algorithms and approaches

The restoration efficiency of the implemented "NDN-based edge computing in IoT-enabled healthcare system" is examined over diverse classical algorithms and cryptography approaches for the two data sources and shown in Figs. 17 and 18. When the percent value is 25 for the second data source in Fig. 18b, the restoration efficiency for the implemented work is enhanced by 96.8% of RSA, 96.2% of AES, 96.6% of ECC, 96.7% of DSR accordingly. Hence, it is confirmed that the presented "NDN-based edge computing in IoT-enabled healthcare system" has higher efficacy rates than the other tasks.

Discussion

The simulation results are presented in Figs. 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, and 18. The Fig. 7 shows the performance comparison of the conventional evolutionary algorithms such as OOA, SCO, CSO, MAO with the proposed RPCSO for various aspects such as computation time, preservation ratio, hiding ratio, and block size, MSE. The RPCSO has lower computation time, block size, and MSE with higher hiding ratio and preservation ratio, which are the desired levels of performance. Figure 8 shows the comparative analysis of the cryptoraphic functions such as RSA, AES, ECC, DSR with RPCSO-DSR. The RPCSO-DSR has lower computation time, block size, and MSE with higher hiding ratio and preservation ratio, which are the desired levels of performance. Figures 9 and 10 shows the performance comparison of the conventional algorithms and encryption schemes with RPCSO for the second data source.

Figure 11 shows comparison of the correlation coefficient of CPA attacks for OOA, SCO, CSO, MAO with RPCSO. The RPCSO measure the lowest correlation of CPA attacks. Figure 12 shows comparison of the correlation coefficient of CPA attacks for various encryption schems such as RSA, AES, ECC, DSR with RPCSO-DSR. This figure also shows that the RPCSO has the lowest correlation coefficient of the CPA attacks. Figures 13 and 14 shows the comparison of the correlation coefficient of KPA attacks for conventional evolutionary algorithms

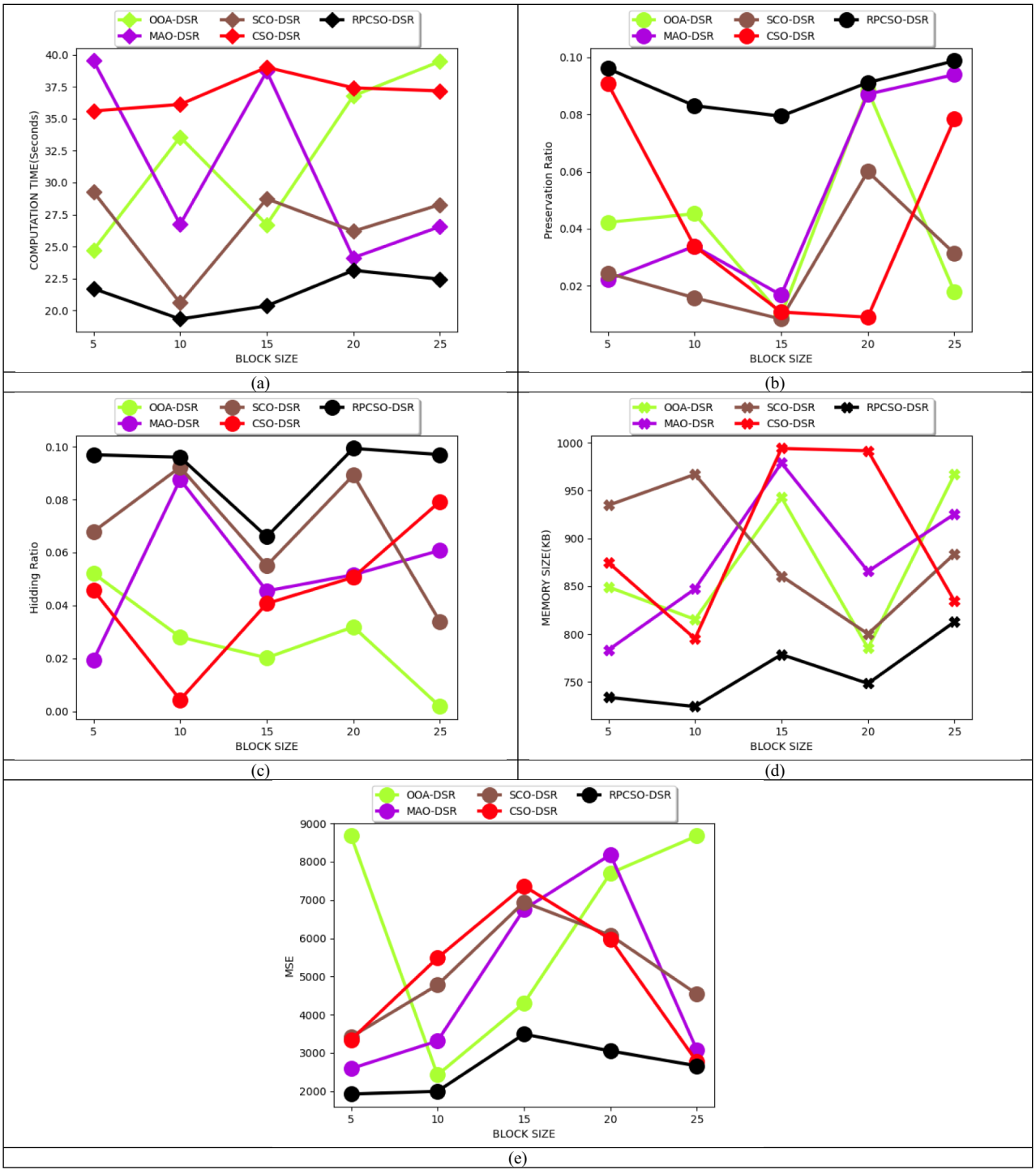

Fig. 7. The suggested NDN-based edge computing in IoT-enabled healthcare system's performance examination for the first data source over diverse conventional algorithms in terms of " (**a**) Computation time, (**b**) Preservation ratio, (**c**) Hiding ratio, (**d**) Memory size, and (**e**) MSE".

and encryption schemes. These figures also shows that the RPCSO has the lowest correlation coefficient of the KPA attacks.

Similarly Fig. 15 shows the comparison of the key sensitive analysis between the RPCSO with the other conventional evolutionary algorithms, such as OOA, MAO, SCO, CSO. Figure 16 shows the the comparison of the key sensitive analysis between the RPCSO with the other encryption schemes such as AES, RSA, DSR, ECC with RPCSO-DSR. The RPCSO shows the low key sensitivitiy analysis compared with the rest of the methods. Figures. 17 and 18 shows the comparison of the restoration efficiency of RPCSO with other conventional evolutionary algorithms and RPCSO-DSR with other encryption schemes. This measure is higher the better and RPCSO and RPCSO-DSR outperforms the rest of the schemes and models.

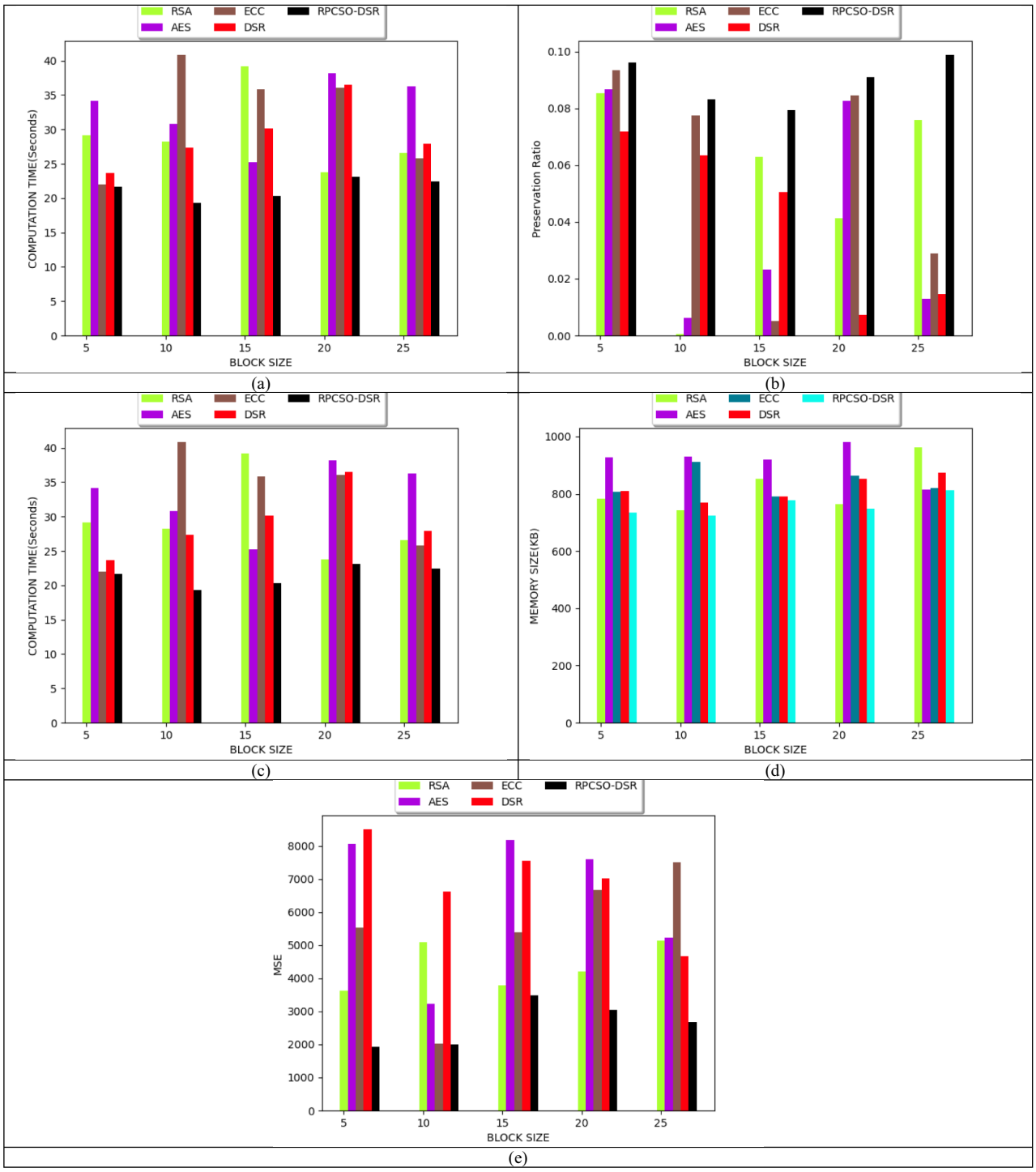

Fig. 8. The suggested NDN-based edge computing in IoT-enabled healthcare system's performance examination for the first data source over diverse conventional cryptographic approaches in terms of "(**a**) Computation time, (**b**) Preservation ratio, (**c**) Hiding ratio, (**d**) Memory size, and (**e**) MSE".

Potential research outcomes of the novel RPCSO-NDN algorithm

The RPCSO algorithm redcues the complexity of finding the fittest position of the CSO, by taking the avearge of the best fit position with the product of the mean and worst fit position to look for the prey. This reduces the complexity of time spent in SM and TM for the fitness evaluation of the conventional CSO optimization algorithm. Thus this RPCSO part is useful in reducing the time and complexity of the conventiona CSO and thus makes this suitable for larger input data

The NDN architecture helps the user to access the sanitized and restored data with ease. This layer reads the network traffic, delivers the trafffic, transmits and forges the network traffic. The main purpose of this layer is

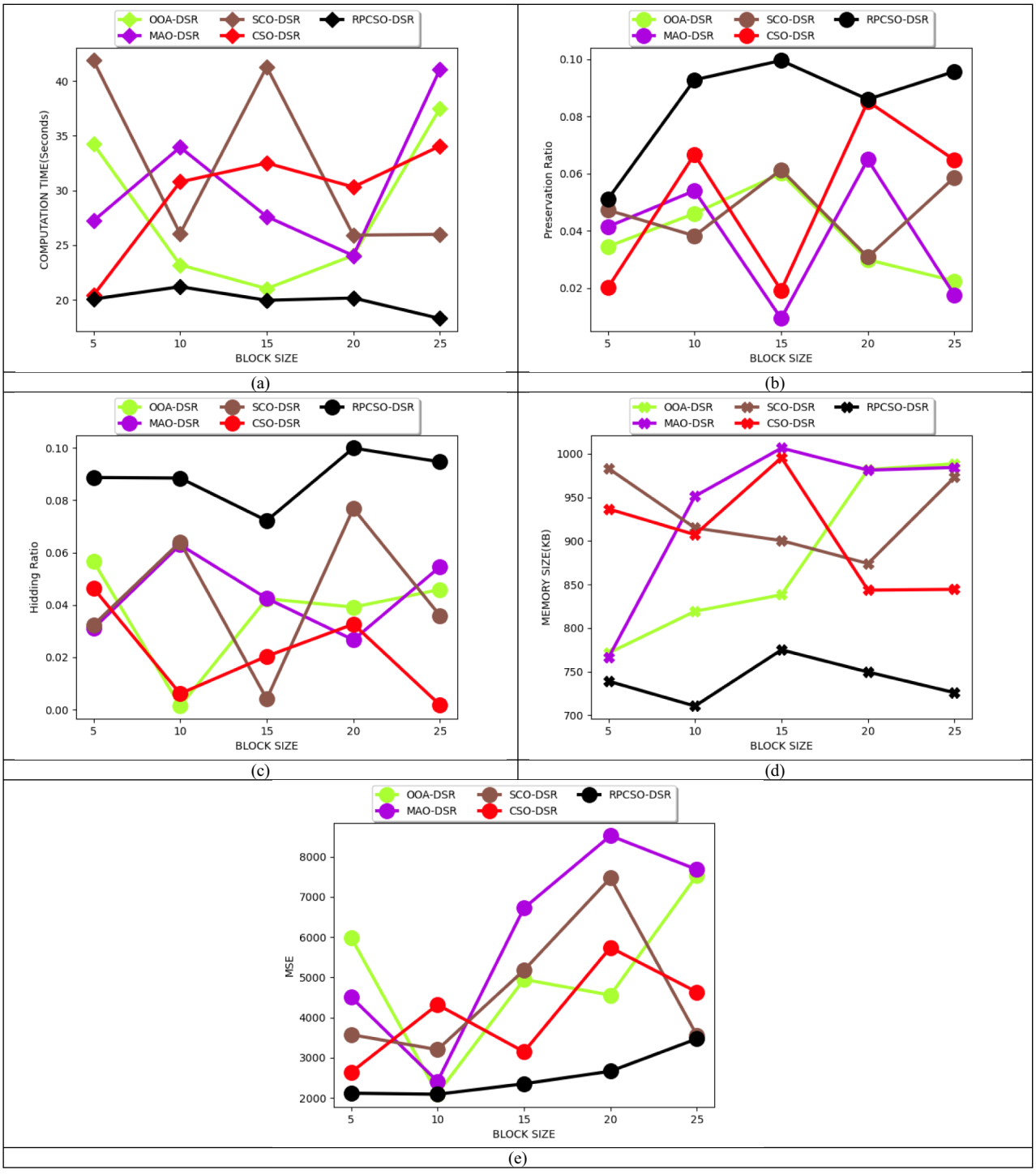

Fig. 9. The suggested NDN-based edge computing in IoT-enabled healthcare system's performance examination for the second data source over diverse conventional algorithms in terms of "(**a**) Computation time, (**b**) Preservation ratio, (**c**) Hiding ratio, (**d**) Memory size, and (**e**) MSE".

to provide ease of access between the user and the edge infrastructure to easily access, acquire and monitor the patient data.

RPCSO-NDN reduces the key size, helps faster random number generation for key exchange between the edge and user infrastructure, which provides secured interoperability between the patient data source and the receving user interface. The data sanitation process for NDN hides the private and sensitive data and restoration allows the data to be restored only to the authorized users. Hence the Key generation process of RPCSO and data sanitation of the NDN increases the security and privacy of the proposed work. The scalability of the proposed work is assured with restoration and NDN edge-user interface, which is a cloud-based infrastructure that can support many users, who are authorized to access the medical data of the patients in real-time environements.

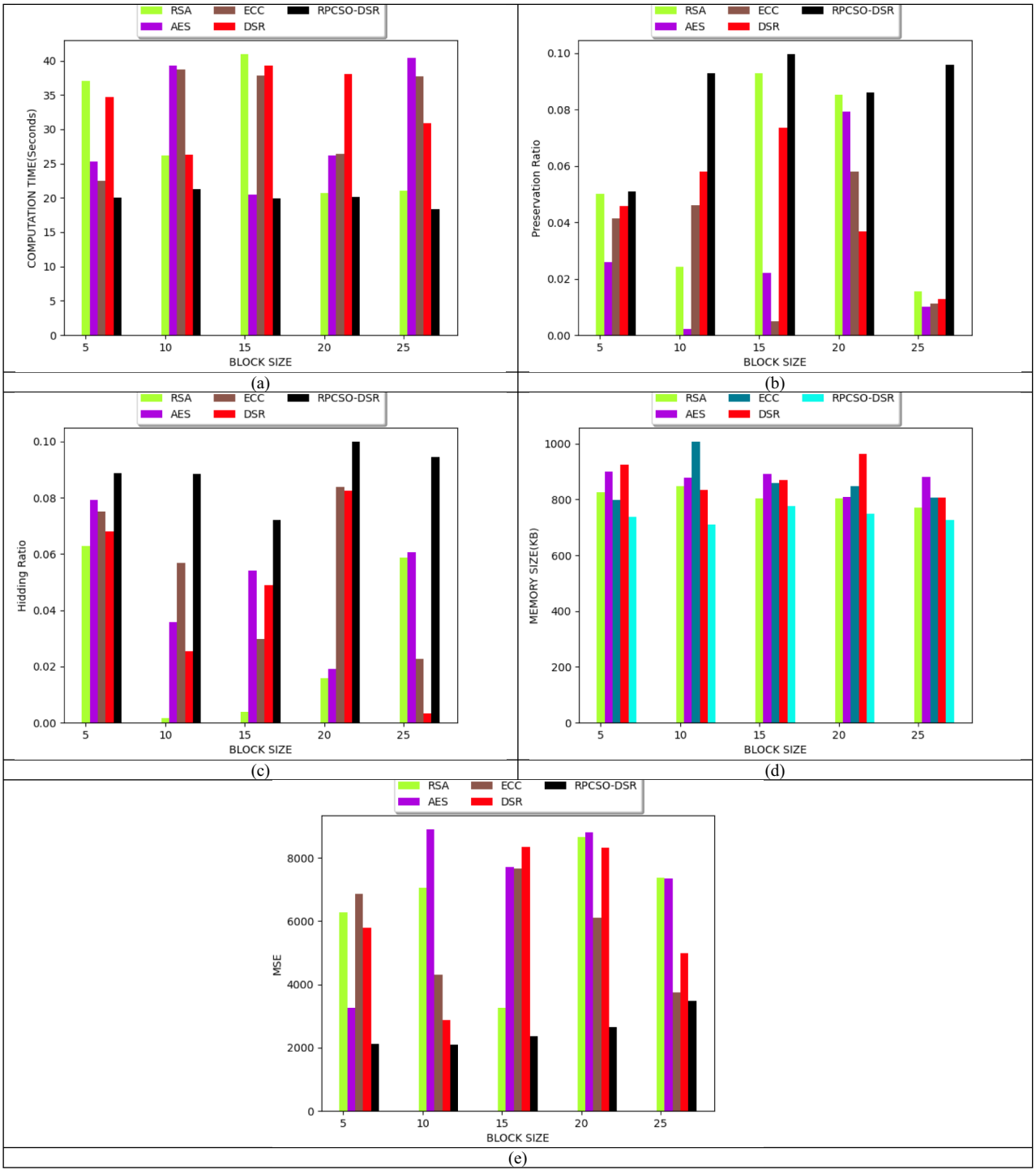

Fig. 10. The suggested NDN-based edge computing in IoT-enabled healthcare system's performance examination for the second data source over diverse conventional cryptography approaches in terms of "(**a**) Computation time, (**b**) Preservation ratio, (**c**) Hiding ratio, (**d**) Memory size, and (**e**) MSE".

The proposed work also has reduced hidden and restoration ration because of the faster convergence due to the integration of the RPCSO-NDN infrastructure, where RPCSO increases the performance of the exploration and NDN provides ease of access to the authorized users, who are connected to the edge infrastructure.

Conclusion

A secure architecture for the "edge computing in IoT-aided medical care" model utilizing heuristic-aided authentication and NDN has been presented in this work. The suggested task included three layers such as patient layer, the edge cloud layer, and the user layer. In the initial layer, various IoT systems were linked together, and

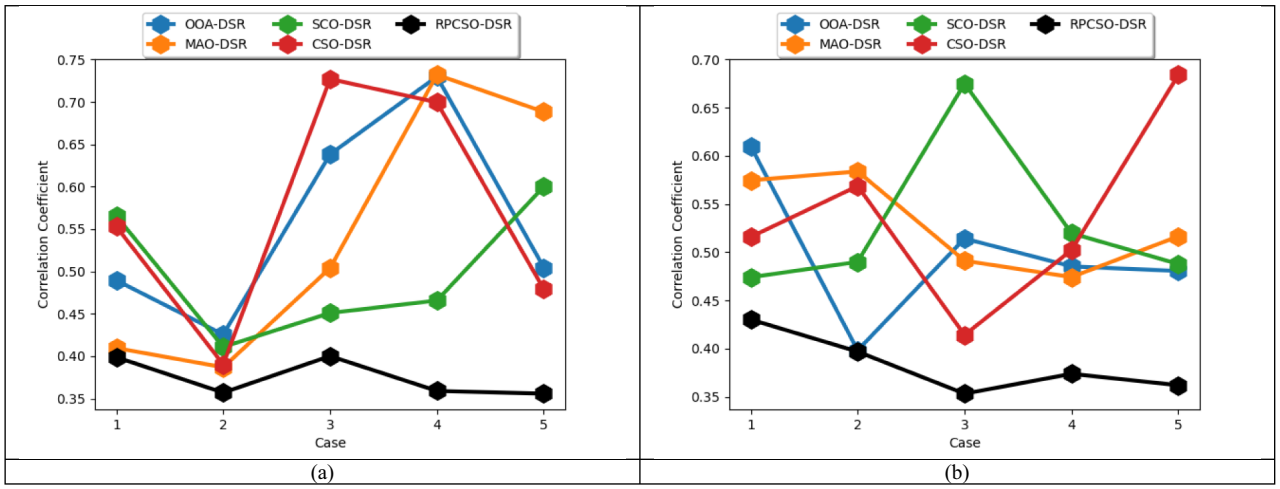

Fig. 11. The presented NDN-based edge computing in IoT-enabled healthcare system's correlation coefficient for CPA attack estimation over diverse conventional algorithms concerning " (**a**) Dataset 1, and (**b**) Dataset 2".

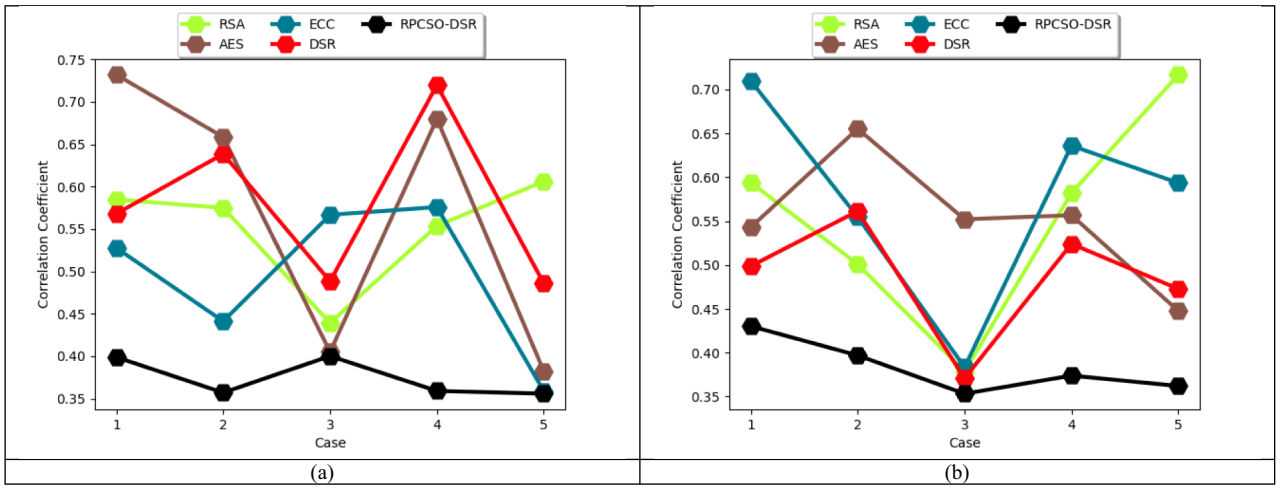

Fig. 12. The presented NDN-based edge computing in IoT-enabled healthcare system's correlation coefficient for CPA attack estimation for the diverse traditional cryptography approaches concerning " (**a**) Dataset 1, and (**b**) Dataset 2".

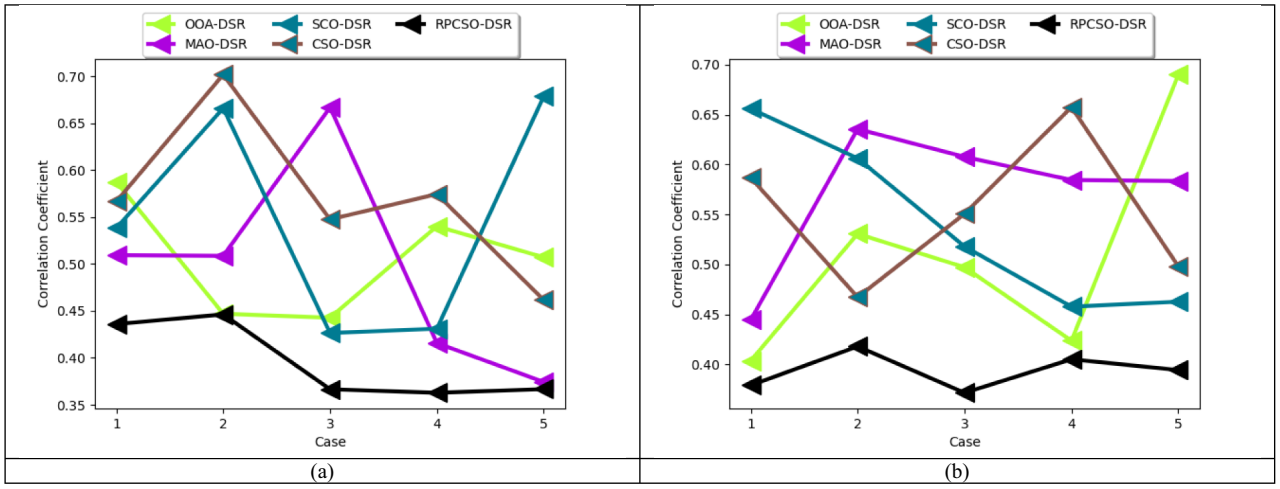

Fig. 13. The presented NDN-based edge computing in IoT-enabled healthcare system's correlation coefficient for KPA attack estimation over multiple conventional algorithms concerning " (**a**) Dataset 1, and (**b**) Dataset 2".

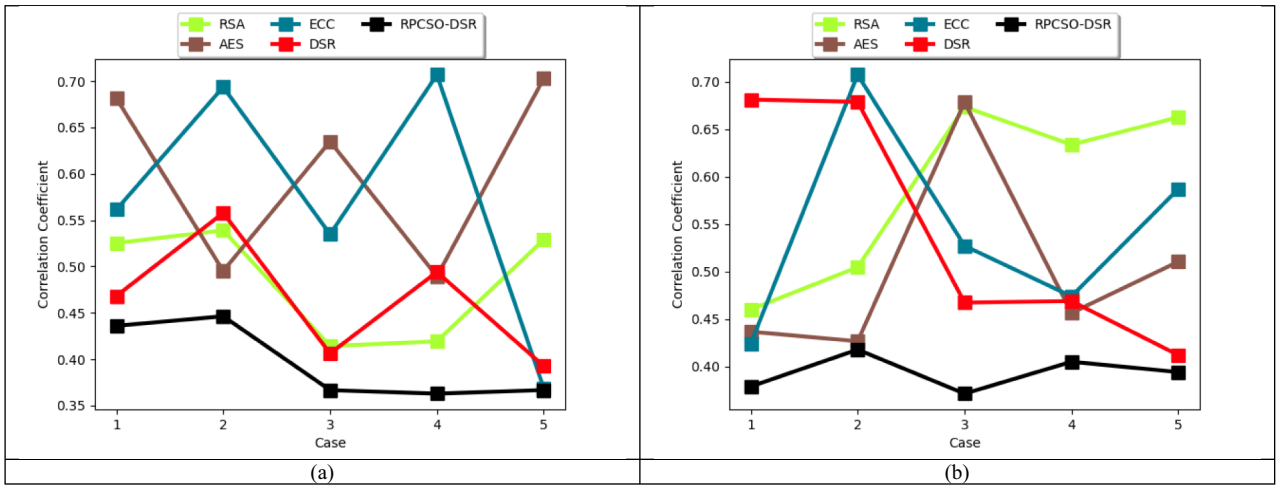

Fig. 14. The presented NDN-based edge computing in IoT-enabled healthcare system's correlation coefficient for KPA attack estimation over multiple conventional cryptography tasks concerning " (**a**) Dataset 1, and (**b**) Dataset 2".

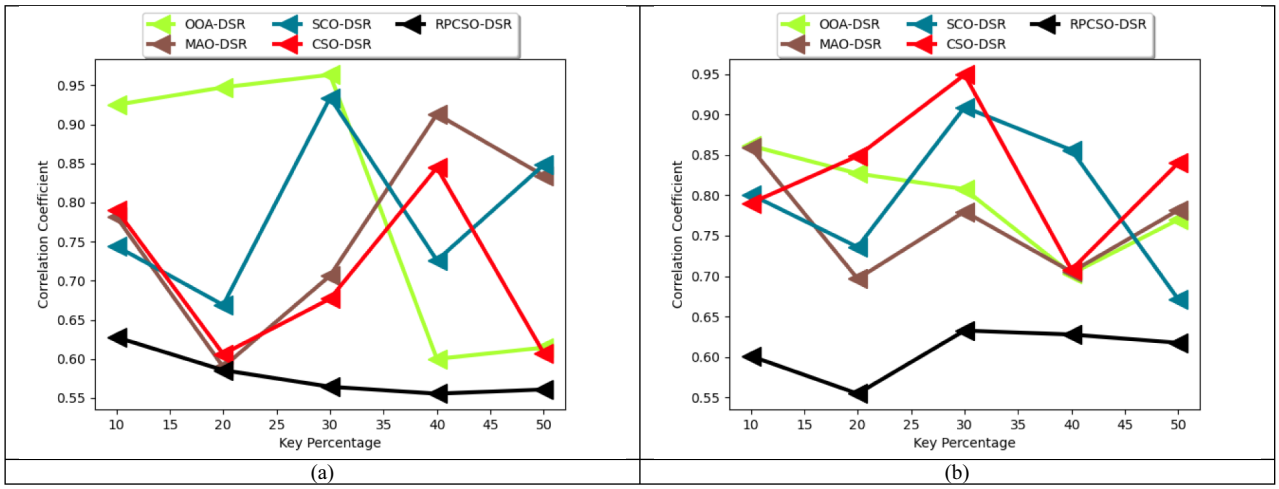

Fig. 15. The designed NDN-based edge computing in IoT-enabled healthcare system's correlation coefficient for key sensitive analysis over multiple conventional algorithms in terms of " (**a**) Dataset 1, and (**b**) Dataset 2".

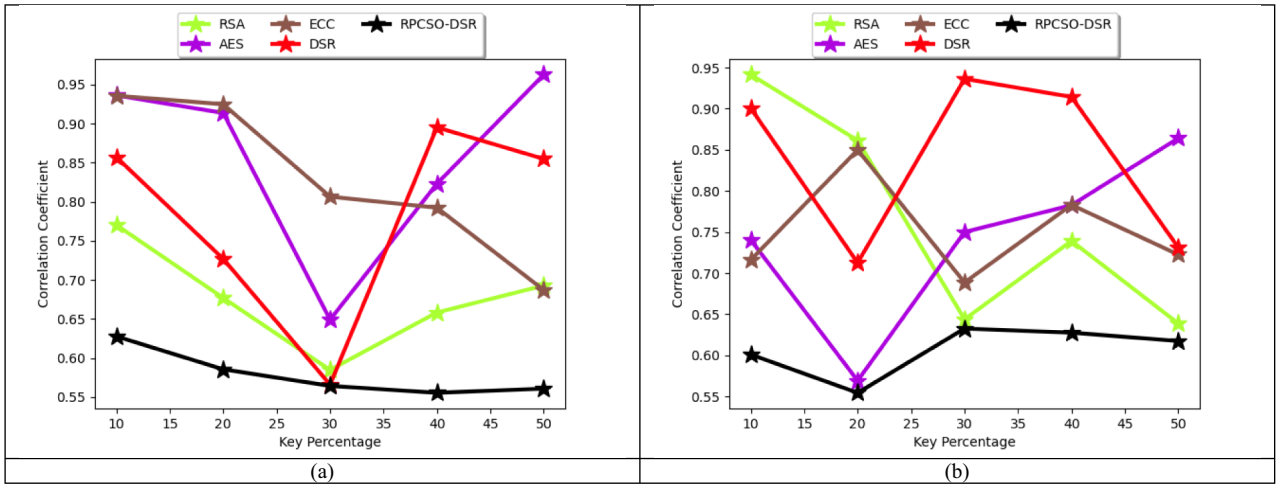

Fig. 16. The designed NDN-based edge computing in IoT-enabled healthcare system's correlation coefficient for key sensitive analysis over multiple conventional cryptography approaches in terms of " (**a**) Dataset 1, and (**b**) Dataset 2".

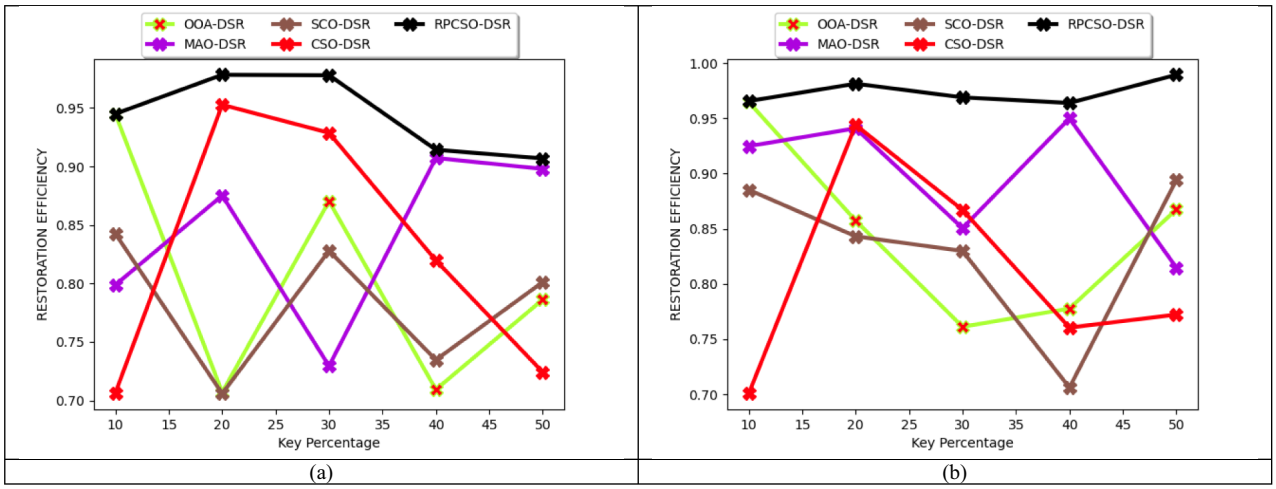

Fig. 17. The implemented NDN-based edge computing in IoT-enabled healthcare system's restoration efficiency investigation over distinct conventional algorithms regarding " (**a**) Dataset 1, and (**b**) Dataset 2".

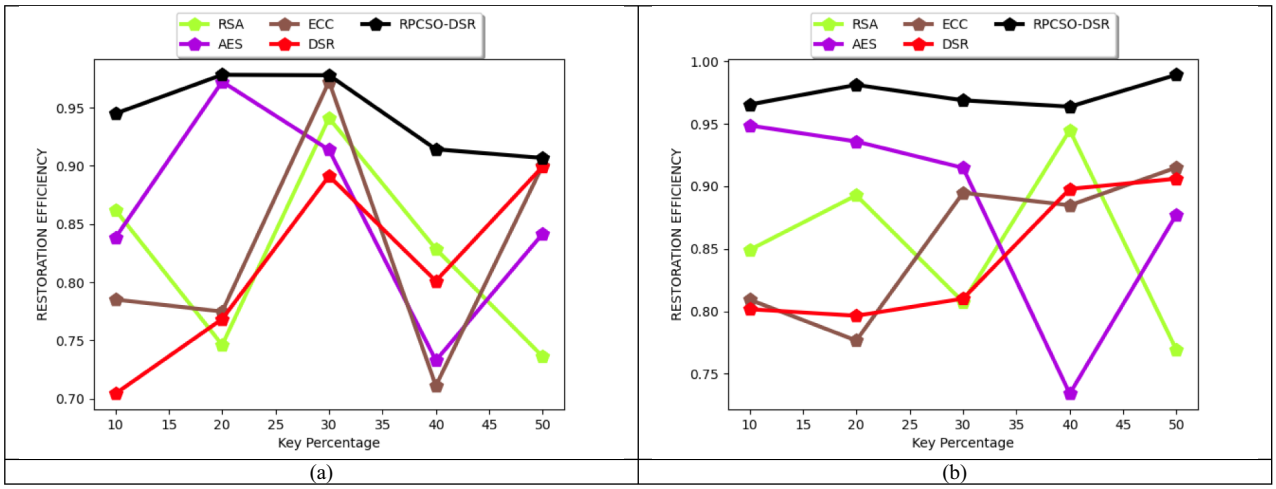

Fig. 18. The implemented NDN-based edge computing in IoT-enabled healthcare system's restoration efficiency investigation over distinct conventional cryptography approaches regarding " (**a**) Dataset 1, and (**b**) Dataset 2".

utilizing the data of the cluster head, the sick persons were transferring their information to the layer called the edge cloud. The edge cloud layer was accountable for computing and storage resources for quickly offering and caching healthcare information. Therefore, the patient layer was a modern heuristic-aided sanitization scheme named RPCSO with NDN to cover up the sensitive information that must not be revealed to the unauthorized members. This authentication task employed a multi-objective function key implementation approach taking the attributes such as modification degree, rate of information preservation, and hiding failure rate. In addition, the edge cloud layer's data was subjected to the user layer, where the development of optimal key with NDN-aided restoration was performed. Thus, the secure and effective data retrieval was attained. The suggested work was examined quantitatively on numerous medical data sources from Kaggle and repository and the research estimation given the superior functionality outcomes of the recommended task concerning the cost and latency when contrasted against traditional solutions. The suggested "NDN-based edge computing in IoT-enabled healthcare system's" preservation ratio was enriched by99.61% of OOA-DSR, 99.93% of MAO-DSR, 99.6% of SCO-DSR, and 99.8% of CSO-DSR correspondingly for the second data source when the block size is 15. Finally, hence it was ensured that the implemented "NDN-based edge computing in IoT-enabled healthcare systems" has supremacy over the other classical healthcare systems. The proposed work is aided with the merits of the

- Data sanitization and data restoration before the encryption process of RPCSO algorithm.
- RPCSO reduces the key memory size, computation time and MSE.
- Velocity based fitness evaluation of RPCSO which optimizes the key exchange process and determines various plain text attacks.
- RPCSO increases the hidden ratio, preservation ratio, and restoration efficiency.

- Reduction of the cost, resource limitations and latency through NDN based edge networks.
- Enhanced privacy and security for the sensitive networks like body sensor networks.

Data availability

Dataset 1: The data underlying this article are available in diabetes.csv, at "https://www.kaggle.com/datasets/saurabh00007/diabetescsv" "access date: 2023-09-27". Dataset 2: The data underlying this article are available in Heart Disease Dataset, at "https://www.kaggle.com/datasets/yasserh/heart-disease-dataset" "access date: 2023-09-27". Dataset 3: The data underlying this article are available in Maternal Risk Dataset, at "https://archive.ics.uci.edu/dataset/863/maternal+health+risk" "access date: 2023-08-14".

Received: 21 February 2024; Accepted: 28 August 2024
Published online: 15 September 2024

References

1. Liao, H. *et al.* Learning-based context-aware resource allocation for edge-computing-empowered industrial IoT. *IEEE Internet Things J.* **7**(5), 4260–4277 (2020).
2. Mutlag, A. A., Abd Ghani, M. K., Arunkumar, N., Mohammed, M. A. & Mohd, O. Enabling technologies for fog computing in healthcare IoT systems. *Futur. Gener. Comput. Syst.* **90**, 62–78 (2019).
3. Fang, H., Qi, A. & Wang, X. Fast authentication and progressive authorization in large-scale IoT: How to leverage AI for security enhancement. *IEEE Netw.* **34**(3), 24–29 (2020).
4. Li, H., Ota, K. & Dong, M. LS-SDV: Virtual network management in large-scale software-dened IoT. *IEEE J. Sel. Areas Commun.* **37**(8), 1783–1793 (2019).
5. Zhou, Z., Liao, H., Gu, B., Mumtaz, S. & Rodriguez, J. Resource sharing and task ofoading in IoT fog computing: A contract-learning approach. *IEEE Trans. Emerg. Topics Comput. Intell.* **4**(3), 227–240 (2020).
6. Dehghani, M. & Trojovský, P. Osprey optimization algorithm: A new bio-inspired metaheuristic algorithm for solving engineering optimization problems. *Front. Mech. Eng.* **8**, 1126450 (2023).
7. Villuendas-Rey, Y., Velázquez-Rodríguez, J. L., Alanis-Tamez, M. D., Moreno-Ibarra, M. A. & Yáñez-Márquez, C. Mexican axolotl optimization: A novel bioinspired heuristic. *Mathematics* **9**(7), 781 (2021).
8. Shami, T. M., Grace, D., Burr, A. & Mitchell, P. D. Single candidate optimizer: A novel optimization algorithm. *Evol. Intell.* **17**, 1–25 (2022).
9. Khan, M. A., Quasim, M. T., Alghamdi, N. S. & Khan, M. Y. A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. *IEEE Access* **8**, 52018–52027 (2020).
10 Kh-Madhloom, J., Ghani, M. K. A. & Baharon, M. R. ECG encryption enhancement technique with multiple layers of AES and DNA computing. *Intell. Autom. Soft Comput.* **28**(2), 494 (2021).
11 Kumari, S. *et al.* A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. *J. Supercomput.* **74**, 6428–6453 (2018).
12. Ahamad, D., Hameed, S. A. & Akhtar, M. A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization. *J. King Saud Univ. Comput. Inf. Sci.* **34**(6), 2343–2358 (2022).
13. Verma, P. & Sood, S. K. Fog assisted-IoT enabled patient health monitoring in smart homes. *IEEE Internet Things J.* **5**(3), 1789–1796 (2018).
14 Rahman, M. A. & Hossain, M. S. A cloud-based virtual caregiver for elderly people in cyber physical IoT systems. *Cluster Comput.* **22**, 2317 (2017).
15. He, W., Yan, G. & Xu, L. D. Developing vehicular data cloud services in the IoTenvironment. *IEEE Trans. Ind. Inform.* **10**(2), 1587–1595 (2014).
16. Azimi, I. *et al.* HiCH: Hierarchical fog-assisted computing architecture for healthcare IoT. *ACM Trans. Embed. Comput. Syst.* **16**(5s), 1–20 (2017).
17. Chiang, M. & Zhang, T. Fog and IoT: An overview of research opportunities. *IEEE Internet Things J.* **3**(6), 854–864 (2016).
18. Hao, Y. *et al.* Smart-edge-CoCaCo: AI-enabled smart edge with joint computation, caching, and communication in heterogeneous IoT. *IEEE Netw.* **33**(2), 58–64 (2019).
19. Alam, M. M. *et al.* A survey on the roles of communication technologies in IoT-based personalized healthcare applications. *IEEE Access* **6**, 36611–36631 (2018).
20. Mutlag, A. A., Ghani, M. K. A., Arunkumar, N., Mohammed, M. A. & Mohd, O. Enabling technologies for fog computing in healthcare IoT systems. *Futur. Gener. Comput. Syst.* **90**, 62–78 (2019).
21. Greco, L., Percannella, G., Ritrovato, P., Tortorella, F. & Vento, M. Trends in IoT based solutions for health care: Moving AI to the edge. *Pattern Recognit. Lett.* **135**, 346–353 (2020).
22. Hossain, M. S. & Muhammad, G. Cloud-assisted industrial Internet of Things (IIoT)-Enabled framework for health monitoring. *Comput. Netw.* **101**(2016), 192–202 (2016).
23 Habibzadeh, H. *et al.* A survey of healthcare Internet of Things (HIoT): A clinical perspective. *IEEE Internet Things J.* **7**(1), 53–71 (2020).
24. Satija, U., Ramkumar, B. & Manikandan, M. S. Realtime signal quality-aware ECG telemetry system for IoT-based health care monitoring. *IEEE Internet Things J.* **4**(3), 815–823 (2017).
25. Li, J. *et al.* A secured framework for SDN-based edge computing in IoT-enabled healthcare system. *IEEE Access* **8**, 135479–135490 (2020).
26. Wang, X. & Cai, S. Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud. *Futur. Gener. Comput. Syst.* **112**, 320–329 (2020).
27. Rahman, M. D. A. *et al.* Blockchain-based mobile edge computing framework for secure therapy applications. *IEEE Access* **6**, 72469–72478 (2018).
28. Alabdulatif, A., Khalil, I., Yi, X. & Guizani, M. Secure edge of things for smart healthcare surveillance framework. *IEEE Access* **99**, 1–1 (2019).
29. Elmisery, A. M., Rho, S. & Aborizka, M. A new computing environment for collective privacy protection from constrained health-care devices to IoT cloud services. *Cluster Comput.* **22**, 1611–1638 (2017).
30 Jayaram, R. & Prabakaran, S. Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system. *Egypt. Inform. J.* **22**, 404 (2021).
31. Chen, M., Li, W., Hao, Y., Qian, Y. & Humar, I. Edge cognitive computing based smart healthcare system. *Futur. Gener. Comput. Syst.* **86**, 403–411 (2018).
32 Amin, S. U. & Hossain, M. S. Edge intelligence and Internet of Things in healthcare: A survey. *IEEE Access* **9**, 45–59 (2020).

33. Shreya, S., Chatterjee, K. & Singh, A. A smart secure healthcare monitoring system with Internet of Medical Things. *Comput. Electr. Eng.* **101**, 107969. https://doi.org/10.1016/j.compeleceng.2022.107969 (2022).
34. Stergiou, C. L., Plageras, A. P., Memos, V. A., Koidou, M. P. & Psannis, K. E. Secure monitoring system for IoT healthcare data in the cloud. *Appl. Sci.* **14**(1), 120. https://doi.org/10.3390/app14010120 (2024).
35. Minopoulos, G. M. *et al.* Exploitation of emerging technologies and advanced networks for a smart healthcare system. *Appl. Sci.* **12**(12), 5859. https://doi.org/10.3390/app12125859 (2022).
36. Dudeja, R. K., Bali, R. S. & Aujla, G. S. Secure and pervasive communication framework using named data networking for connected healthcare. *Comput. Electr. Eng.* **100**, 107806 (2022).
37. Bouzidi, A., Riffi, M. E. & Barkatou, M. Cat swarm optimization for solving the open shop scheduling problem. *J. Ind. Eng. Int.* **15**, 367–378 (2019).

Author contributions
All authors have equally contributed to the paper. All authors have read and agreed to the published version of the manuscript.

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to S.S.

Reprints and permissions information is available at www.nature.com/reprints.

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