Complex & Intelligent Systems
https://doi.org/10.1007/s40747-021-00505-8

ORIGINAL ARTICLE

Code-based encryption techniques with distributed cluster head and energy consumption routing protocol

M. Jalasri[1] · L. Lakshmanan[1]

Received: 3 June 2021 / Accepted: 12 August 2021

Abstract
Fog computing and the Internet of Things (IoT) played a crucial role in storing data in the third-party server. Fog computing provides various resources to collect data by managing data security. However, intermediate attacks and data sharing create enormous security challenges like data privacy, confidentiality, authentication, and integrity issues. Various researchers introduce several cryptographic techniques; security is still significant while sharing data in the distributed environment. Therefore, in this paper, Code-Based Encryption with the Energy Consumption Routing Protocol (CBE-ECR) has been proposed for managing data security and data transmission protocols using keyed-hash message authentication. Initially, the data have been analyzed, and the distributed cluster head is selected, and the stochastically distributed energy clustering protocol is utilized for making the data transmission. Code-driven cryptography relies on the severity of code theory issues such as disorder demodulation and vibration required to learn equivalence. These crypto-systems are based on error codes to build a single-way function. The encryption technique minimizes intermediate attacks, and the data have protected all means of transmission. In addition to data security management, the introduced CBE-ECR reduces unauthorized access and manages the network lifetime successfully, leading to the effective data management of 96.17% and less energy consumption of 21.11% than other popular methods.The effectiveness of the system is compared to the traditional clustering techniques.

Keywords Internet of Things (IoT) · Fog computing · Intermediate attacks · Data security · An encryption technique · Keyed-hash message authentication code-based encryption technique

Overview of managing data security using keyed-hash message authentication code-based encryption algorithm

Third-party data can be monitored and measured in real-time by IoT devices and technologies connected through the internet. The third-party information is data transmitted, stored, and it can still be recovered in the server [1]. IoT is a network of physical items integrated with electronics, software, sensors, and network networking to collect and transmit to third parties [2]. The fog computing-based third-party data transmission first layer contains network devices like routers and gateway for processing time-sensitive information to the layer of things [3]. The second former layer can be used for cable or wireless sensor communication. The third fog nodes layer measures the demands and forwards findings to other fog nodes or cloud nodes [4].

Third-party data is any information derived by a person not related directly to the person by which data is gathered. Primarily, the data is obtained from several websites and platforms by external providers, including a data management platform (DMP) [5, 6]. The fog computing method using sensors for monitoring the physical conditions of third-party data collection [7]. Third-party data is any information received by a company or other organization that has no direct connection to the visitor [8]. Third-party data are gathered, aggregated, and businesses sold to help them develop successful advertising and return campaigns [9, 10]. Its ordinary audience helps businesses expand in size to include potential prospects for which person buys related services from a direct competitor [11]. Sellers from third parties have legal access to vital infrastructure and confidential details of customers [12]. A third-party cyber-attack

✉ M. Jalasri
jalasrimani@gmail.com

L. Lakshmanan
lakshmanan.cse@sathyabama.ac.in

[1] Department of CSE, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu 600119, India

Published online: 30 August 2021

poses cyber protection, operational, conformity, and reputational threats for all the vendors' organizations [13, 14]. The third-party data transfer generally consists of irritating behavioral or demographic data aggregated from several sources [15]. The objective of the structure is to find basic analysis services at the edge of the network where they are necessary. This reduces the distance between data and the efficiency of the network throughout the network. Fog safety computing issues also offer users advantages.

Third parties' big data transfer problem is intermediate attacks and data protection, confidentiality, authentication, and credibility issues [16]. Data security in the distributed cluster head is significant when exchanging data [17]. A pre-image attack against cryptographic hash functions attempts to locate a message that has a particular hash value [18]. A cryptographic hash function can withstand preliminary attacks [19]. A birthday assault is a type of attack using the mathematics behind the birthday problem [20]. The birthday paradox principle considered that specific pairs in a randomly selected group of people are likely birthday-friendly [21]. Rainbow tables are extensive data collections that store various common and weak passwords and hashes generated using those passwords. Keyed Hash Message Authentication Code (HMAC) is a coding method that uses a key-connected algorithm [22]. The HMAC algorithm is a whole packet and complexity of the output key. The data collected from all the cluster nodes is carried out by each cluster head (CH) [23]. When data is obtained from all the participants, the CH sends the frame to the base station after implementing data aggregation. The CH should stay active while the nodes of the member function periodically [24].

Hence in this paper, a keyed-hash message authentication code-based encryption algorithm with distributed cluster head and energy consumption routing protocol has been used to improve the data management.HMAC is a cryptographic technique that can unpack public keys, private keys, and a hash into a combination. This paper uses HMAC to enter a method that can both encrypt data and verify data accuracy. Scalability restricting most connectivity within the various network clusters and routing the single hop from the sensor node towards the cluster's head aggregates the sensor nodes' data. The energy consumption routing protocol in the wireless body area network to secure the transfer of data. The protocol considers several network node parameters, such as residual capacity, propagation power, bandwidth availability, and hopping numbers. By normalizing node parameters, create the maximum gain function to pick the next-hop node and dynamically select the node with the highest function score. The proposed approach achieves effective multi-hop data routing and increases network data transfer efficiency. Authentication is an important matter for fog computing security, even though massive terminals are provided with services through front cloud servers. In addition to those inherited from cloud computing, fog computing faces new security and privacy challenges. Authentication assists and confirms the identity of a user. Fog is used throughout your network by deploying fog nodes. Touch screen, toggle, wireless connection, and directional microphones devices can act as fog nodes. When an IoT device generates data, it can be analyzed via one of the nodes without returning to the cloud.

The main contribution of the paper:

(i) Designing the CBE-ECR has been proposed to improve data security and enhance data collection to store third-party servers.
(ii) Encryption techniques to reduce the middle attacks like pre-image attacks, birthday attacks, rainbow tables.
(iii) The mathematical results have been analyzed, and the proposed CBE-ECR reduces unauthorized access and improves the network lifetime successfully.

The remaining of these paper structures has been followed: "Overview of managing data security using keyed-hash message authentication code-based encryption algorithm" overview of data management based on energy-efficient clustering protocol. "Literature review based on data security" literature review based on data security of exiting methods. "Code-based encryption with the energy consumption routing protocol", the proposed paper system, has been performed for third-party data security. "Keyed-hash message authentication" analyses the results and discussion, and "Results and discussion" explores the conclusion of the research.

Literature review based on data security

The encryption technique reduces advanced threats, and all data transfer methods have been protected. Concerning managing security and privacy, the introduced CBE-ECR reduces unregistered access and successfully manages the network life leading to effective transmission of knowledge.

Pedro Gonzalez-Gil et al. [25] suggested the DS4IoT for IoT based on lightweight data-security ontology. Current method estimates show steady IoT development, with many works depicting an even nascent security technology. In addition, new rules, including general data protection regulation (GDPR), include new approaches to data storage and personal data coverage. In this work, DS4IoT is a data security ontology for IoT that covers representing data protection principles with a modern approach from a data point of view and introducing classic concepts, including access control and authentication, certifications, and provenance.DS4IoT is an IoT cybersecurity metaphysics covering the data protection act 1998 with a modern data approach and conventional concepts including access control and encryption mechanics, accreditation, and origin.

Omar DIB et al. [26] explored the novel data exploitation framework (NDEF) based on blockchain technologies. These intelligent devices constantly produce vast quantities of data, which can be of use to many utilities. One major obstacle to the development of such services is that they often handle confidential and personal data. To accomplish this, they aim to introduce a new NDEF based on a blockchain platform to facilitate personal data in this article. Experimental research found that the approach presented is secure and efficient enough to be built into a real-world program. These electronic sensors constantly produce huge amounts of data that many utilities can make use of. The fact that confidential and personal information is often used is a major problem in developing such services.

Zhao Huang et al. [27] expressed the physical unclonable function (PUF)-based unified identity verification framework (PUF-UIVF) for secure authentication with hardware device for IoT. Millions of mobile devices were connected and communicated through networks during the era of the IoT. Silicon PUF has been introduced to complete system authentication and key storage to mitigate this threat effectively and is considered a reliable antipiracy solution. The proposed system is implemented and tested on the field-programmable gate array (FPGA) platforms. Experience findings show that the suggested architecture distinguishes embedded device hardware's robberies on low silicon overhead uniquely and reliably.

Data Management Framework (DMF) for pervasive IoT applications deliberated by saniyazahoor et al. [28]. The overall IoT's key objective is to make everyday devices available, responsive, and interconnected within the global framework of the internet in the future. The resources of IoT equipment (such as storage, processing, and energy) are restricted in many IoT applications; this document further suggests a DMF focused on parallelization for resource-controlled IoT applications. The findings show an increase in capacity, processing, and storage requirements about the sequential solution for IoT data processing within the proposed system.

Novel Data Flow and Distributed Deep Neural Network (DF-DDNN) based IoT-Edge model for less latency in Big Data edge computation described by Veeramanikandan et al. [29]. Deep learning provides nearly half the time accurate knowledge relative to other learning algorithms. The edge/fog computing environment supports the IoT problem, such as latency, bandwidth utilization, and the network's eternal connectivity. In this regard, the IoT-edge model based on DF-DDNN is proposed for large data sets. Compared to the conventional IoT-Cloud model, our proposed approach reduced the latency by up to 33%.

Low-rank-matrix-completion problem (LRMC) and topological interference management (TIM) for clustering for D2D networks discussed by Salam Doumiati et al. [30].In this document, they are developing a popular clustering and TIM architecture for a D2D network. To this end, they are TIM model as an LRMC problem and solve it using a new system based on semi-definite programming (SDP) with low complexity. Our scheme reduces the LRMC-based TIM approach's computation time.

For latency-sensitive IoT services, such as sensor monitoring, Fog Computing offers moving computing, communication, and store systems between the clouds to the edge of the network. Safety in fog-enabled services, such as healthcare monitoring, is, however, a fundamental problem. In contrast, here received decentralized, efficient clouds security protocols (RDECS), including continued data monitoring given by Viejo et al. [31].

IoT plays a major role in the diagnostic and detection process in Healthcare (H-IoT). Various medical sensors based on IoT are used for biometric measurement and transmission to the cloud for additional analysis by Sarrab et al. [32]. Therefore, this work proposes an IoT-fog framework to categorize streamed data critically and detect anomalies in the fog with low latency and high response times.

Based on the existing PUF-UIVF, DMF, DF-DDNN, and LRMC-TIMF analyses, some issues are computation time, latency, and accuracy. Hence in this paper, CBE-ECR has been proposed to have less computation time, less latency, accurately predict the attack based on the keyed-hash message authentication technique.

Code-based encryption with the energy consumption routing protocol

CBE-ECRis used for controlling data protection and data transfer protocols using key-hash authentication services. At first, the data is analyzed, and the cluster head is chosen, then the energy clustering protocol that is stochastically distributed is utilized for transmission. Encryption minimizes transitional assaults and the attack by unknown users. The developed CBE-ECReliminates unauthorized access and effectively manages network life as well as data protection management.

Three devices, namely IoT device (N), regulator device (CRN), and fog computing device, are used in the CBE-ECR. IoT system involves both the IoT device and the regulator device. IoT device is resource devices that are restricted while regulator device is not restricted either within or outside the IoT system. IoT devices sometimes communicate directly with the regulator device, but it is granted for interaction among points. The architecture of CBE-ECR is shown in Fig. 1. The architecture includes data protection with the

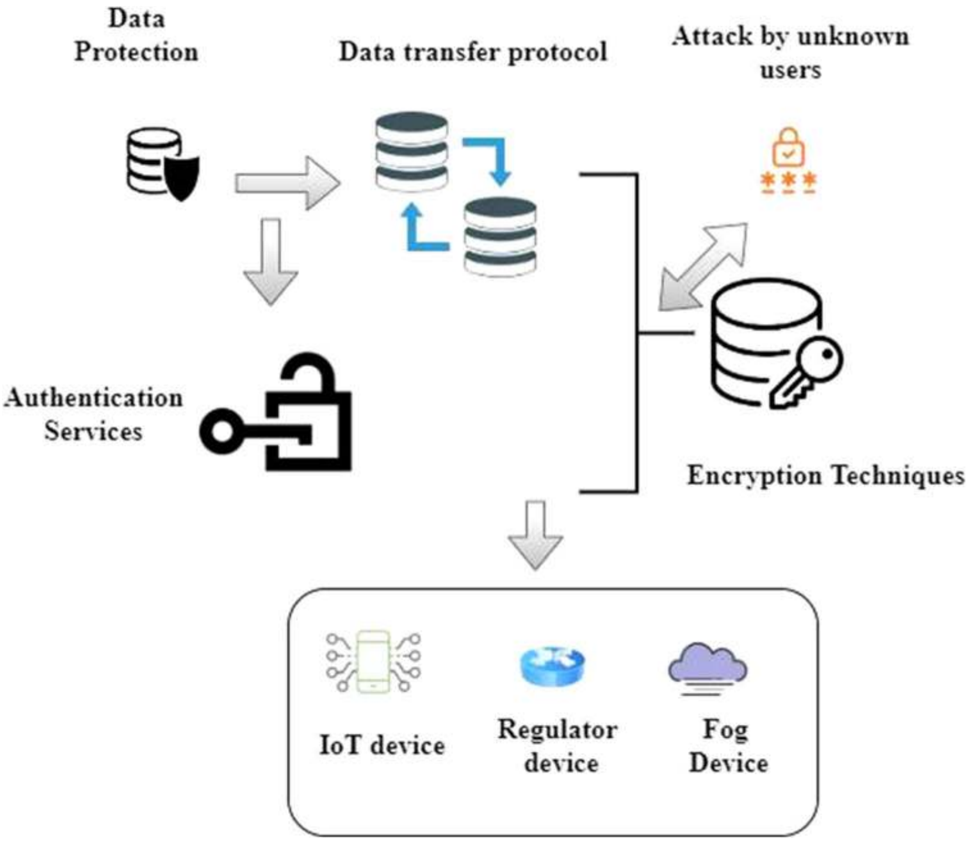

Fig. 1 The architecture of CBE-ECR

data transfer protocol. The attack by unknown users can be avoided by the Encryption techniques that utilize the authentication services.

Fog computing equipment, IoT devices, and the expert decryption algorithm are generally assumed to remain securely stored in the data store. When an instant post correlation verifies IoT, it creates evidence of connection attack by unknown users with the variable at the beginning of encryption. Fog Computing devices, IoT device provisions, and the master secret key are presumed to remain in safe storage in the device's database. When an IoT device authenticates with the immediate post connection, unknown at the outset of encryption, it generates a Proof of Association with the variable. Data protection is encrypted by all public key data transfer protocols that rely on the hardness of decoding in a linear error corrective code, partially or totally with authentication services, for their security, if selected with some techniques.CBE-ECR encourages the confirmation of the IoT device by the regulator device and notifies for computing devices' practical domestic practice.

Data security management effectively supervises and manages an organization's data to ensure that unauthorized users do not access or corrupt the data. A data security management plan includes planning, implementing, verifying, and updating the scheme's components. In the CBE-ECR framework, it is believed that different regulator nodes use a specific server. Therefore, after IoT devices are authorized and licensed, all fog devices get notified by specific personal regulators. Such expectation allows information from one device in a clever manner in which the IoT domain remains safely and securely. The secured data transmission between the regulator device, fog computing device, IoT device with the authenticated users flow is illustrated n Fig. 2.

Furthermore, specific nodes in virtual environment fields have to interact with various devices within the contexts. The data transfer between all the devices or nodes within the protocols is controlled by keyed-hash message authentication. The management of data security is shown in Fig. 2.

Keyed-hash message authentication

A problem based on authentication method must always be regarded in addition to provide complete mutual encryption. The IoT node is then sent to the regulator with the data it wishes to transmit and generates a hash data represented as L_1. The prior stage of authentication is described below

$$h_r = l\left(h_1, MH_k, r_{gh_v}\right) * L_1 \tag{1}$$

The prior stage of authentication h_r is obtained from Eq. (1), Mutual hidden Key (MH_k), r_{gh_v} represent the

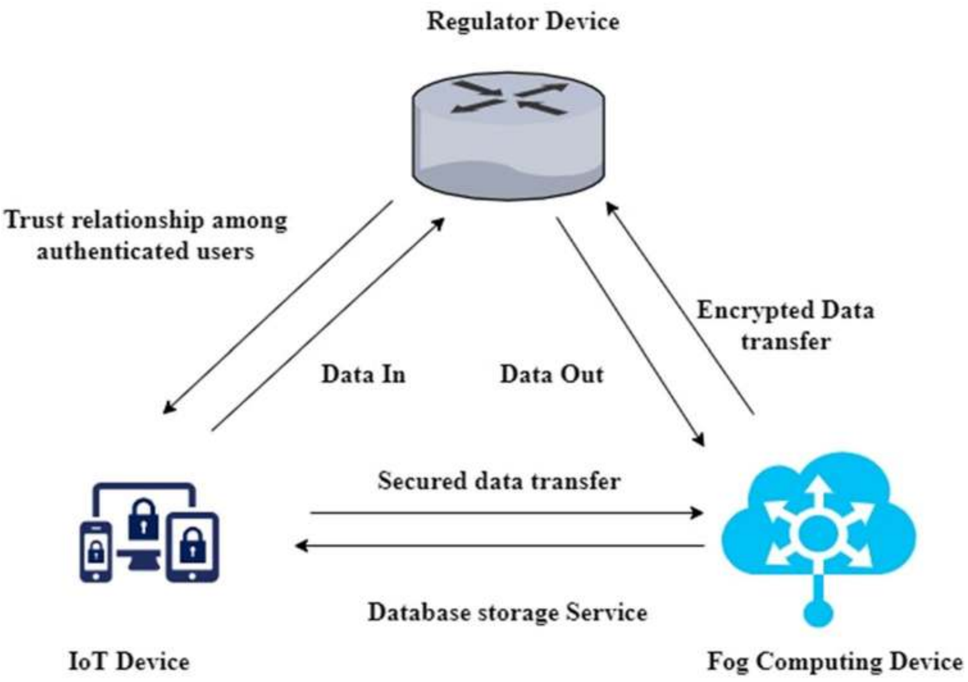

Fig. 2 The management of data security

Keyed-hash series server, L_1 represent the hash data, l represents the resulting quality.

Besides, the hash and strings L_1 has two more values, and the Mutual hidden Key (MH_k) have the Keyed-hash series server, and where r is the series or quality structure of the principles in which the full hash function is obtained. Thus it connects the resulting quality to the remote system of the prior stage of the authentication communication.

The keyed-hash message authentication flow with the prior stage of authentication h_r, the Keyed-hash series server r_{gh_v}, hash function h_1, Mutual hidden Key MH_k is shown in Fig. 3. Eventually, the resulting hash function quality is hacked and stored in the Keyed-Hash server as a correct

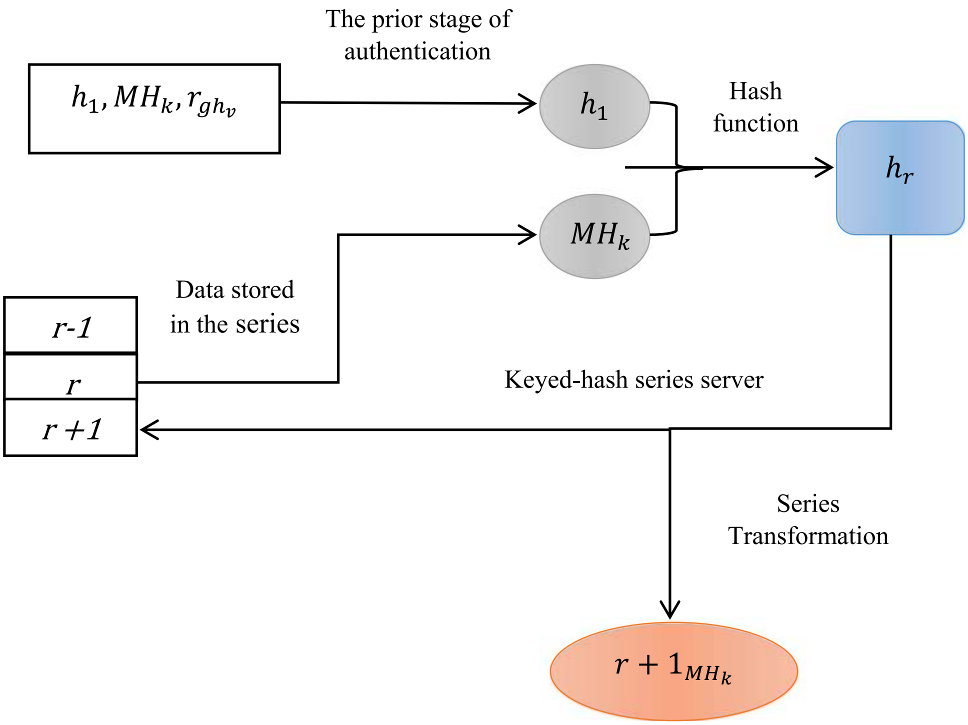

Fig. 3 The keyed-hash message authentication

value with the mutual hidden key. Hash-based Message authentication code is a decryption code with a hash feature that uses a digital signature. The hash transport layer security (HMAC) creates a decentralized key to the server and client known to that particular source and destination. The new data stored in the series is shown below

$$r+1_{\mathrm{MH}_k} = l\left(h_1, \mathrm{MH}_k\right) * r_{gh_v} \tag{2}$$

The new information stored in the series is described from Eq. (2), Mutual hidden Key (MH_k), h_g represent the hash function quality, r_{gh_v} represent the Keyed-hash series server, l represents the resulting quality. $r+1$ represents the series transformation. Encryption involves taking plain text, such as a text message or e-mail, in an unreadable format—called the clipboard text. This ensures that digital data is kept confidential either on computer systems or transmitted over networks.

The regulator device applies a particular methodology to guarantee that the provided hit rate is accurate after gathering information. First, all data is obtained from M, and the hash function is represented as h_1. In the Second stage, hash and function for h_1 with the specific keys, Mutual hidden Key (MH_k), regulator device contained in the hash link key server. The resulting value is then compared to the received data, as shown below

$$*_{h_g} = g(h_1^{'}, MH_k, y_{h_g}) \tag{3}$$

The comparison between the received data $*_{h_g}$ is obtained from Eq. (3), Mutual hidden Key (MH_k), y_{h_g} Represent the accurate data information.

It should be mentioned that specific frameworks bind the stages to pass around and haze the group's latest hash function with different components like the transient encryption key and the accumulated hash value. Therefore, the CBE-ECR seems at first glance to manage data security. A hacker may claim that the key-hash chain entries can corrupt or discover the hidden key to break that stage in the system. Even then, it's not simple to locate the encryption data because it varies in each session. If the opponent knows the hidden key or initial hash, the pointless information becomes a fleeting data packet.

The CBE-ECR is developed to maintain secrecy, although becoming theoretically quicker than diagonal encryption techniques. It can have consistency since it is focused on the development of data fingerprints. The Significance of CBE-ECR is focused on assuming that a hacker can recover the actual credential data from a hash-value utilizing broad immediate post lists of hazards beyond an adorable assault. As hazing implementations can be open to all, the implementation should produce the respective codes if everyone knows such an application. The Keyed-Hash Message Encryption Application method is used to create fingerprints to settle the Privacy of data.

CBE-ECR can be used as part of the report by creating a hash function and a pre-shared secret key to verify the validity and source. It would indeed be impossible for a hacker to produce plate interfaces despite understanding the closed key. It requires hashes to be created for all potential quality combinations transmitted using each valid secret key.

A hatching mechanism must meet specific safety criteria such as plaintext resistance, subsequent plaintext opposition, and impact opposition for managing data security. During the tolerance based on a feature's nature, there is an information stream to create particular digestion of a particular component that is impossible to locate the secured data. The Privacy and security of data can be maintained and managed by certain conditions. The suggested CBE-ECR is thus intended to be autonomous for managing data security and privacy.

Code-based encryption

Contrary to the code-based encryption technique, the CBE-ECR suggested approach encrypts a significant part of the encoding that defines the retrieval mechanism and is identical to the data stream begin key. The actual data are collected from the database server. The encryption technique can be integrated into a data generation key that must be checked during and after encoding. Rather than using the default data encryption method, the suggested code-based encryption technique encrypts the data by scratching the headers' first byte keys. Therefore, standard encryption techniques add mathematical uncertainty concerning the number of term measures since they encode the data via various systems using unique components. The code-based encryption technique improves the authentication speed since the regular secret key does not apply.

The security service provider has the components, namely database, server, encryption, to maintain data privacy. The user maintains the authentication and privacy server to lock the security model for all data streams, as illustrated in Fig. 4.

A few data choices can be the initial computation of the code-based template, except allocated and unconfirmed data security-privacy must be managed. The data can include up to few connectors, but it is not allowed to overlap. The majority of instances necessary to rebuild the actual data stream in the lowest possible situation would thus be maximized. The absolute majority of instances must be implemented in the code-based encryption technique. In particular, it is possible to verify if each case is retrievable just after data are decrypted in each phase.

The initial code-based template calculation can be a few data choices unless the data security data confidentiality is

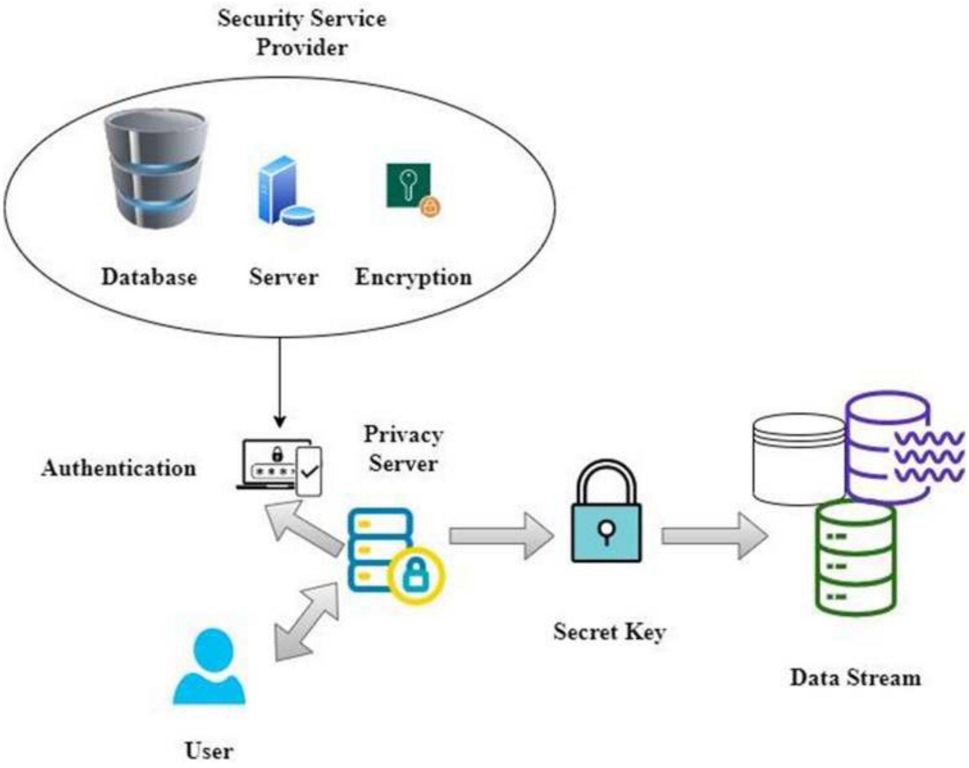

Fig. 4 The stages of code-based encryption technique

provided as allocated and not confirmed. There may be up to a small number of connectors; however, no overlap is allowed. This would maximize the large percentage of the necessary instances to rebuild the actual data stream at the minimum possible cost.

Essentially, the CBE-ECRreduces unauthorized access and manages the network lifetime successfully. The difficulty of computing the network lifetime is expressed as follows in the suggested encryption method, and the difficulty in computing is described below

$$S_{Q-B} = D_U Q_U + D_V Q_V + D_W Q_W + D_Y Q_Y \tag{4}$$

The difficulty in computing is obtained from Eq. (4), the completeness function is represented as D_U, D_V, D_W, D_Y that ends precisely at functions U, V, W, Y and returns to cycle start. Furthermore, Q_U, Q_V, Q_W, Q_Y are the possibilities leading to D_U, D_V, D_W, D_Y. The total of Q_U, Q_V, Q_W, Q_Y is 1.This would maximize the sufficient circumstances to reconstruct the overall network traffic at the lowest possible level. In code-based data encryption, the absolute majority of cases must be carried out.

If the procedure is represented as S_U, T_V, T_W in each step, the above Eq. (4) can be modified and shown below

$$S_{Q-B} = S_U Q_U + \left(S_U + S_V\right) Q_U + \left(S_U + S_V + S_W\right) + D_Y Q_Y \tag{5}$$

Each stage of procedure representation is obtained from Eq. (5), $S_U + S_V + S_W$ represent the contrast function parameters.Q_U, Q_Y represent the scaling parameter. In contrast to the code-based cryptosystem, a significant portion of encoding that defines the recovery mechanism is proposed for encoding by the CBE-ECR and is identical with the starting key of the data stream. The approximation stage and the contrast function is described below

$$\begin{cases} S_{\text{con}} = S_U = S_V = S_W \\ S_{Q-B} \sim S_{\text{con}} Q_U \end{cases} \tag{6}$$

The approximation stage S_{Q-B} and the contrast function S_{con} is obtained from Eq. (6), $S_U + S_V + S_W$ represent the contrast function parameters. The encryption process suggested is about the same for the authentication of data $S_{\text{ES}-B}$. The difficulty of the authentication is described as follows. Data collected by a third party are any information derived by a person not directly related to the person through whom data are collected. Data are generated by external providers, including a data management platform, from several websites and platforms.

$$S_{\text{ES}-B} = (S_U + S_V + S_W) * S_{\text{con}} Q_U \tag{7}$$

Authentication of data is obtained from Eq. (7), here $S_U + S_V + S_W$ represent the contrast function parameters, S_{con} represent the contrast function, Q_U represent the scaling parameters. Protected information is collected, aggregated, and sold to companies to help them develop successful campaigns for advertising and returns. Its ordinary audience helps companies expand to include potential opportunities to buy the related services from a competing product.

In specific, when the execution time is a few bits shortest, the computation time and the encryption stage of detailed data is described as follows:

$$\mathrm{Et}_{sf-bt} = S_a + S_b + S_c \tag{8}$$

The computation time and the encryption stage Et of particular data is obtained from Eq. (8), $S_a + S_b + S_c$ represent the significance *sf* of each data byte *bt*.

The hash message authentication manages the data security and the transmission protocols. The data obtained is distributed to overall cluster heads, then the energy in the clustering protocol is utilized to make the data transmission. The cluster head is typically chosen, and it is centered on the least number of hops in the standard protocol for the fog computing device. Nevertheless, the data type leftover energy and route data usage are ignored. The chosen path can be made with the minimal hop amount; nevertheless, the length is far, or the energy usage is heavy.

Consequently, in this section, data is analyzed, and the cluster is selected. Finally, the clustering protocol is used for data transmission with the distributed energy. The complete energy usage in the x direction and the latency is described below

$$\mathrm{Com}_{\mathrm{ene}(x)} = \sum\nolimits_{y=0}^{y=M_x-1} \cos S_y, y+1 \tag{9}$$

The complete energy usage and the latency $\mathrm{Com}_{\mathrm{ene}(x)}$ is obtained from Eq. (9), $\cos S_y, y+1$ refers to the energy absorbed to send and receive data from y devices in the following direction, where M_x Specifies an average of x route points and can be demonstrated via an energy usage wireless communication device.y represent the number of device.

Whenever the cluster energy is depleted, the relation breaks in fog computing. The lifespan of the connection thus has a clear connection with the node energies. Besides, to consider the node energy usage, the connectivity route must be chosen.

The data collection and the stages of encryption, in the form of energy absorbed by the sender and the receiver for data calculation per bit, are shown in Fig. 5. The connectivity between the devices and the energy utilized are explained below

$$\cos S_y, y+1 = A_T\left(l, b_{y,y+1}\right) + A_R\left(l, b_{y,y+1}\right) \tag{10}$$

The connectivity between the devices and the energy utilized $cosS_y, y+1$ is obtained from Eq. (10), $A_T\left(l, b_{y,y+1}\right)$ represent the energy absorbed by the sender, $A_R\left(l, b_{y,y+1}\right)$ represent the energy absorbed by the receiver.

If a device distributes the data to a neighboring device, the sender and receiver attain an equal amount of energy. The energy usage of the device as per bit of data is calculated as follows

$$A_T = A_{T-e}(l, c) + A_{T-a}(l, c) \tag{11}$$

The energy usage of the device as per bit of data is obtained from Eq. (11), l represents the distributed message of data in the form of byte, c represents the range among the devices.A_{T-e} represent the devices on space free type, A_{T-a} represent the communication stage of devices.

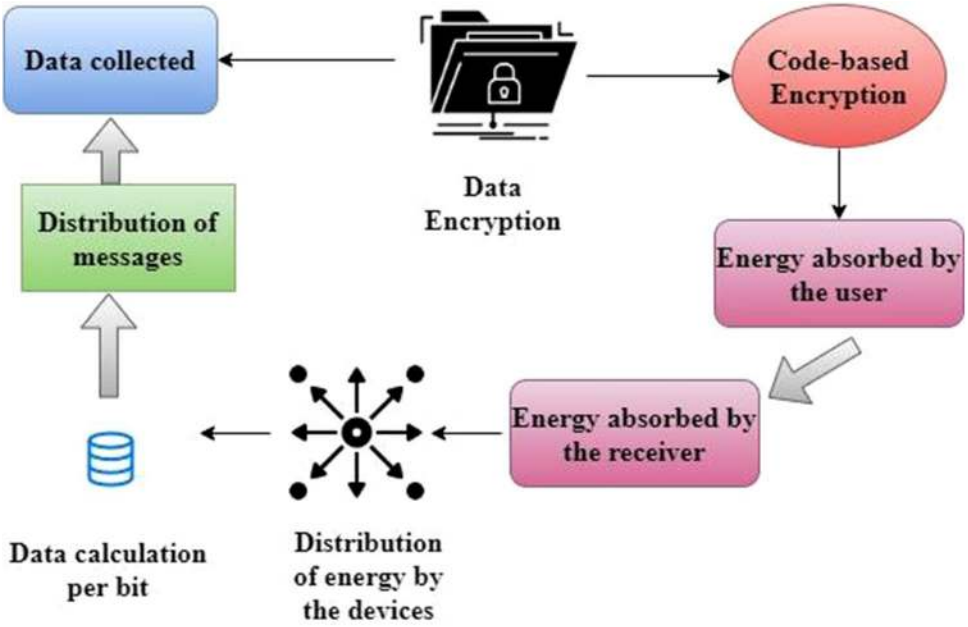

Fig. 5 The data collection and the energy distribution

The device amplifier's energy diffusion parameters in the free-range phase to calculate the accuracy and clustering protocol is shown below

$$\begin{cases} C_0 = \sqrt{\frac{A_g}{A_m}} \\ C_0 = \begin{cases} lA_e + lA_g * b^2, l \le C_o \\ lA_e + lA_m * b^4, l \ge C_o \end{cases} \end{cases} \tag{12}$$

The energy distribution between the free-range phase A_g and the clustering protocol A_m is obtained from Eq. (12), the node uses a propagation descent feature b^2 if b is higher than the specified limit C_o. Electrical storage is the energy usage factor, and it is represented as A_e.

Computing its information collected of sensor nodes are added to the cluster that restricts most connectivity within the various network clusters and routes the release information to a sensor node. Routing protocol for energy consumption in the wireless body network for ensuring data transfer.

In a way, the existence of the path depends on the length of the connection. The lifetime of the connection among two neighboring devices is analyzed. Randomly scattered are the points in the system. The communication time is determined by assessing both networks' comparative rate and the points' position for a defined connection.

The network model with u and v points is regarded as the nearest route domain. The relation between the two devices is $\{u, v\}$ and the data transmission between nodes is transmitted to r. The oscillation vector u and vare implemented with an angle between those two point vector fields. The fog computing device has no positioning system such as Graphical Positioning System; hence, the two locations' close range cannot be calculated immediately. The interval among various domains can be calculated in many ways. The time variation of the signal among the two points is used to calculate the data transmission and detect the attacks. In the CBE-ECR process, the time gap is in microseconds, and as defined, time synchronization is essential. The specific approach is to use message transmit power among devices during the journey.

Many devices are often chosen for transitional networks or deeply integrated with conventional routing for fog computing, and the energy storage is thus quickly depleted. If the linkage node's energy is consumed, the whole network sometimes collapses, and unauthorized users can attack the data.

Results and discussion

The major challenge of third-party data transfer is intermediate attacks, data security, privacy, authentication, and reputation problems. This paper discussed the CBE-ECR based third-party data security in fog computing and IoT devices. The base station synthesizes the sensor node data. Protocol for energy consumption routing in the wireless network for secure data transmittals. The protocol contains many parameters of network nodes, including continue generating, implementation cost, frequency band, and jumps. The HMAC is an encryption technique that unpacks the mix of public keys, private keys. This paper uses the HMAC approach to encrypt the data as well as to validate data integrity. The most networking limitation of scalability in different network clusters and single hop routing from the sensor node's cluster head. The key-hash message authentication code-based encryption algorithm has been used for improving data management with the distributed head cluster and energy consumption routing protocol. The cluster head summarises the data produced by the sensor nodes. Energy consumption routing protocol for safe data transmission in the wireless sensor network. The protocol includes many network node parameters, including residual capacity, transmission efficiency, bandwidth, and hops numbers.

In this paper, discussion section we consider x-axis has a number of devices and Y-axis computation time, accuracy ratio, latency, energy consumption, performance, effective data management, detection rate, precision when compared to physical unclonable function (PUF)-based unified identity verification framework (PUF-UIVF) [27], Data Management Framework (DMF) [28], Data Flow and Distributed Deep Neural Network (DF-DDNN) [29], Low-rank-matrix-completion problem (LRMC) and topological interference management (TIM) [30]. Table 1 shows the discussion section results outcomes.

Table 1 Result outcomes

Number of parameters	PUF-UIVF	DMF	DF-DDNN	LMRC-TIM	CBE-ECR
Detection rate (%)	77.12	62.13	74.34	69.11	97.11
Precision ratio (%)	63.23	73.11	68.34	79.25	98.06
Effective data management ratio (%)	80.07	86.21	84.26	77.19	96.17
Accuracy ratio (%)	67.13	61.39	73.42	63.24	95.09

Detection rate and precision ratio (%)

The encryption technique has several different methods of detecting attacks on third-party servers. Many detecting instances, particularly those most suspect, can be identified by enterprise firewalls or intrusion detection systems. Assessors who intend to discover through firewalls and intrusion detection systems should understand which detect more likely to produce results without attracting the safety officers and how encryption techniques can be performed more steadily to increase their chances for success. The encryption technique can detect unwanted or rogue network devices. A third-party company using a few operating systems easily detects rogue machines using various devices. Figure explores the Fig. 6a Detection rate and Fig. 6b Precision Ratio (%)

A third-party data transmission challenge that requires studying and regularly solving to secure data's authenticity and integrity in this process successfully. Since the IoT is highly susceptible to different types of attacks such as passive eavesdropping, aggressive interference, spoofing, and blocking information, it cannot guarantee accurate and credible perceived information. Data collection and encryption phases in the form of the communicator and the recipient's energy absorbed for research performed per bit. Equation (7) is the connection between the devices and the energy used. The fog computing environment can be approximated correctly to collect sensor network data, achieve exact data, and enhance the available data. The primary processing method consists of finding, correcting, or excluding irregular information by examining the connection between third-party data. Combined with trust model data analysis technologies to ensure data authenticity from the source presented to ensure the source is reliable.

Effective data management ratio and accuracy ratio (%)

Third-party information is outsourced in fog computing, and third-party data management is transferred to the fog node, which involves the same security risks as in the cloud. First, it is difficult to protect data accuracy when outsourced data may be misplaced. Secondly, unauthorized parties may misuse the uploaded data for other reasons, in the context of the energy consumption routing protocol for data protection, auditable data storage services. Encryption techniques such as key-hash message authentication code and distributed cluster head are combined to allow a third party to verify the data stored on a non-confidential server to ensure the integrity, confidentiality, and verifications of the cloud server storage system. Figure express the Fig. 7a effective data management ratio and Fig. 7b accuracy ratio (%)

The low power consumption and unattended installation of the IoT and fog environment ensure more effortless internet protection. A fog sensing device based on the output rate restriction in this report solves source reliability. The increased throughput restriction provides an efficient representation of the information to minimize this confusion and volatility to produce more accurate stable data than the single sensor, boosting network and accurate data transmission in the third party.

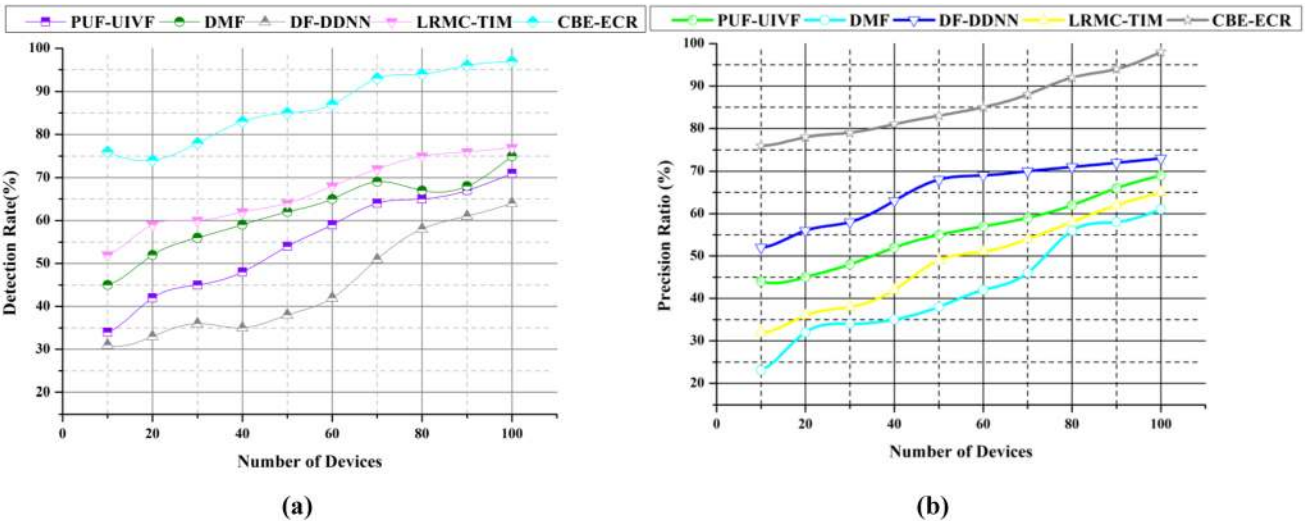

Fig. 6 **a** Detection rate and **b** Precision ratio (%)

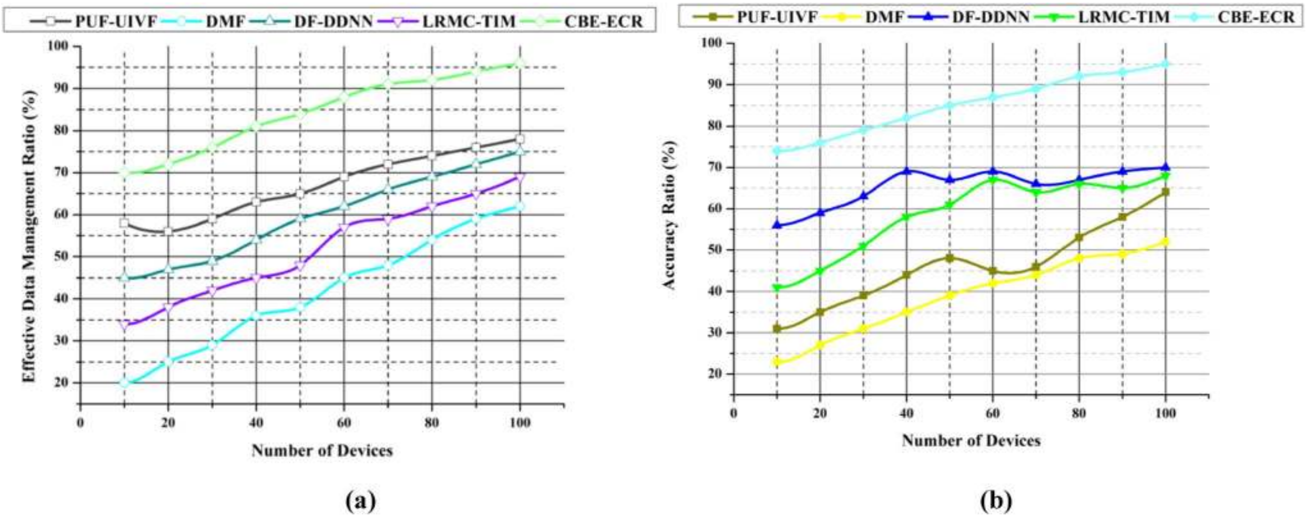

Fig. 7 **a** Effective data management ratio and **b** accuracy ratio (%)

Latency ratio (%)

The proposed method utilize sensor node's GPS cards to know their coordinates, distributing cluster head to maintain the network connection by still having a representative node on its virtual grid in active mode. The simulations' effects demonstrate that it works both in latency and packet loss, reducing energy consumption. Although ECR is a localized protocol on which the clusters are geographically dependent. A representative node serves as the leader to relay the data to other nodes for every specific third-party server location. The information shall be given, otherwise, the particulars are unnecessary at a specific time from the moment the information is sensed. Correspondingly, limited data latency for long-lasting applications is another requirement. The central concept is to analyze IoT devices and network data, perhaps to optimize the benefit of information while minimizing latency and bandwidth. Figure 8 deliberates the Latency ratio (%).

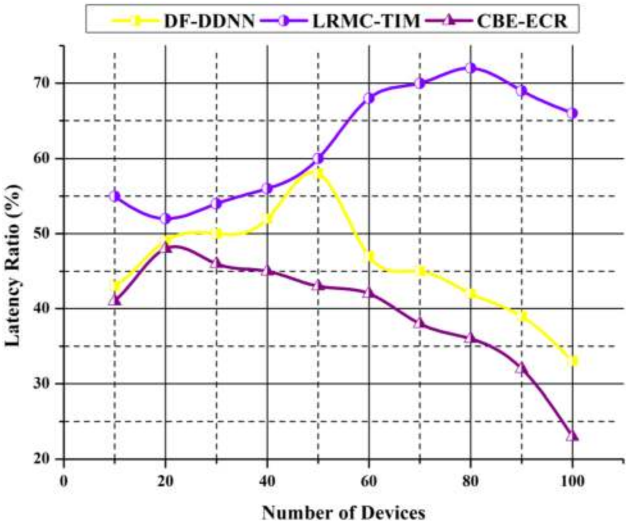

Fig. 8 Latency ratio (%)

Computation time ratio (%)

Fog computing scenario is the communication of many heterogeneous, ubiquitous, decentralized computers and the network to carry out storage processing activities without third parties. The proposed CBE-ECR offered an autonomous data query network-layer approach. Additional overheads in energy consumption and memory store can be given in the query layer on each sensor node. Second, synchronization among nodes is necessary (not all data is obtained simultaneously from incoming sources) for efficient data computation in-network before sending it to the top node. Thirdly, the top nodes should be managed dynamically to avoid hot spots. Figure 9 shows the computation time ratio (%).

Performance ratio (%)

This paper using an energy consumption routing protocol, a distributed cluster head, to protect Privacy from the energy consumption routing protocol and protect Privacy from the server's data. Previous storage schemes have used error correction codes or network codes to address data detection and data restoration to ensure data storage security. The keyed-hash message authentication code allows for less storage, even quicker data recovery, and equivalent connectivity costs. Adequate data security, data collection storage

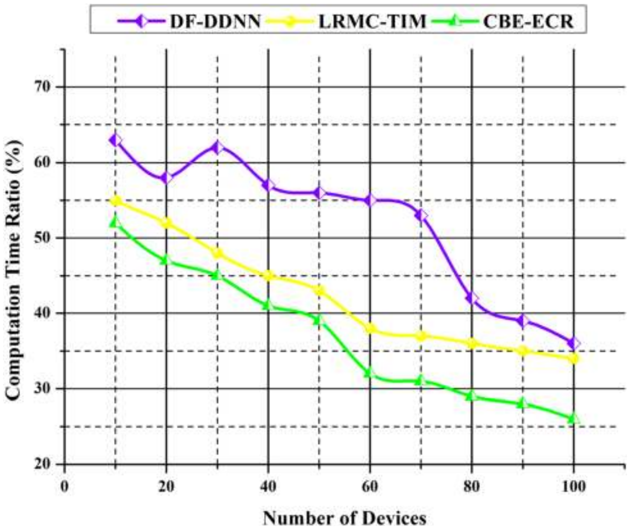

Fig. 9 Computation time ratio (%)

services have been developed. Verifiable computing makes it possible for a computer to unload a function's calculation to other servers, perhaps not trusted with the verified data. Table 2 shows the performance ratio (%).

Energy consumption ratio (%)

A sensor server structure where sensor nodes choose a top node sends base station (BS) data to a third party to carry out the aggregation. The third-party BS generates and transmits the information required for the data flow and in-network calculation to the incoming question schedule's appropriate nodes. The proposed CBE-ECR minimizes energy use and picks more reliable nodes for routing packets. The most critical element in server centrality becomes stability. Residual energy, connection quality, and the number of hops required to reach the server's destinations are characteristic of a node's reliability. With low latency and high bandwidth, computational power and storage space could be provided from fog computing and IoT environment. Table 3 explores the energy consumption ratio (%).

The CBE-ECR has been proposed to increase data transmission and enhance data security to achieve detection rate, precision ratio, accuracy ratio, effective data management, less latency, the low computational time when compared to physical unclonable function (PUF)-based unified identity verification framework (PUF-UIVF), Data Management Framework (DMF), Data Flow and Distributed Deep Neural Network (DF-DDNN), Low-rank-matrix-completion problem (LRMC) and Topological interference management (TIM)methods.

Conclusion

This paper analyses IoT and fog computing environment-based third-party server data collection and data storage. Third parties data have legitimate access to essential resources and customer confidentiality. A third-party cyberattack poses cyber protection, operations, conformity, and reputational threat to all vendor organizations. Hence in this paper, CBE-ECR is used in data security and data transmission protocol management with key-hash authentication services. The data is first processed, and the cluster head is selected stochastic energy clustering protocol used for transmission. The encryption technique minimizes transitional attacks like preimages, rainbows, birthdays. The proposed CBE-ECR created prevents unwanted access and controls both network life and data security management efficiently. The CBE-ECR has been proposed to increase data transmission and enhance data security to achieve detection rate 97.11%, accuracy ratio 95.09%, precision 98.06% effective

Table 2 Performance ratio (%)

Number of Devices	PUF-UIVF	DMF	DF-DDNN	LRMC-TIM	CBE-ECR
10	34.11	45.34	33.34	52.14	76.03
20	52.14	52.05	43.14	59.05	74.06
30	52.18	56.31	36.19	66.02	78.43
40	58.17	59.46	55.27	52.08	83.56
50	64.32	68.07	68.06	61.43	85.34
60	69.25	69.06	62.01	64.01	87.02
70	74.34	71.64	71.21	67.15	93.45
80	65.28	67.31	78.25	68.07	94.01
90	79.11	78.27	81.37	72.-13	96.08
100	81.09	86.32	84.19	77.09	97.09

Table 3 Energy consumption ratio (%)

Number of devices	PUF-UIVF	DMF	DF-DDNN	LRMC-TIM	CBE-ECR
10	55.11	66.34	42.23	33.44	78.34
20	59.53	69.22	49.28	38.22	71.28
30	62.67	72.15	56.35	48.38	69.24
40	68.45	79.17	58.21	52.45	61.27
50	75.31	69.49	62.26	58.31	49.15
60	72.25	62.34	56.29	47.29	42.36
70	69.05	59.29	52.25	45.11	31.43
80	67.09	54.11	47.21	42.29	29.28
90	61.07	51.22	44.22	39.11	24.09
100	58.06	48.14	42.24	32.17	21.11

data management 96.17%, performance 97.09% less latency 26.34%, low computational time 23.45%, energy consumption 21.11% when compared to other popular methods.

References

1. Gao J, Wang H, Shen H (2020) Smartly handling renewable energy instability in supporting a cloud datacenter. In: 2020 IEEE international parallel and distributed processing symposium (IPDPS) (pp. 769–778). IEEE
2. Nguyen TN, Liu BH, Nguyen NP, Chou JT (2020) Cybersecurity of smart grid: attacks and defenses. In: ICC 2020–2020 IEEE International Conference on Communications (ICC) (pp. 1–6). IEEE.
3. Manogaran G, Varatharajan R, Lopez D, Kumar PM, Sundarasekar R, Thota C (2018) A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. Fut Gen Comput Syst 82:375–387
4. Shakeel PM, Baskar S, Fouad H, Manogaran G, Saravanan V, Xin Q (2020) Creating collision-free communication in IoT with 6G using multiple machine access learning collision avoidance protocol. Mob Netw Appl. https://doi.org/10.1007/s11036-020-01670-9
5. Gao J, Wang H, Shen H (2020) Task failure prediction in cloud data centers using deep learning. IEEE Trans Serv Comput. https://doi.org/10.1109/TSC.2020.2993728
6. Alshammari H, El-Ghany SA, Shehab A (2020) Big IoT healthcare data analytics framework based on Fog and cloud computing. J Inform Process Syst 16(6):1238–1249
7. Caiza G, Saeteros M, Oñate W, Garcia MV (2020) Fog computing at industrial level, architecture, latency, energy, and security: a review. Heliyon 6(4):e03706
8. Alzoubi YI, Osmanaj VH, Jaradat A, Al-Ahmad A (2021) Fog computing security and Privacy for the Internet of Thing applications: State-of-the-art. Secur Priv 4(2):e145
9. Manogaran G, Vijayakumar V, Varatharajan R, Kumar PM, Sundarasekar R, Hsu CH (2018) Machine learning based big data processing framework for cancer diagnosis using hidden Markov model and GM clustering. Wirel Pers Commun 102(3):2099–2116
10. Billah MFRM, Saoda N, Gao J, Campbell B (2021) BLE can see: a reinforcement learning approach for RF-based indoor occupancy detection. In: Proceedings of the 20th International Conference on Information Processing in Sensor Networks (co-located with CPS-IoT Week 2021) (pp. 132–147).
11. Pham DV, Nguyen GL, Nguyen TN, Pham CV, Nguyen AV (2020) Multi-topic misinformation blocking with budget constraint on online social networks. IEEE Access 8:78879–78889
12. Zhang Y, Wang P, Fang L, He X, Han H, Chen B (2020) Secure transmission of compressed sampling data using edge clouds. IEEE Trans Ind Inf 16(10):6641–6651
13. Haseeb K, Islam N, Saba T, Rehman A, Mehmood Z (2020) LSDAR: a lightweight structure-based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks. Sustain Cities Soc 54:101995
14. Mehta D, Saxena S (2020) MCH-EOR: multi-objective cluster head based energy-aware optimized routing algorithm in wireless sensor networks. Sustain Comput Inform Syst 28:100406
15. Kumar R (2020) Energy-efficient dynamic cluster head and routing path selection strategy for WBANs. Wirel Pers Commun 113(1):33–58
16. Rezaeipanah A, Nazari H, Abdollahi M (2020) Reducing energy consumption in wireless sensor networks using a routing protocol based on multi-level clustering and genetic algorithm. Int J Wirel Microw Technol (IJWMT) 3(1):1–16
17. Sureshkumar C, Sabena S (2020) Fuzzy-based secure authentication and clustering algorithm for improving the energy efficiency in wireless sensor networks. Wireless Pers Commun 112(3):1517–1536
18. Saba T, Haseeb K, Ud Din I, Almogren A, Altameem A, Fati SM (2020) EGCIR: energy-aware graph clustering and intelligent routing using supervised system in wireless sensor networks. Energies 13(16):4072
19. Ilyas M, Ullah Z, Khan FA, Chaudary MH, Malik MSA, Zaheer Z, Durrani HUR (2020) Trust-based energy-efficient routing protocol for Internet of things–based sensor networks. Int J Distrib Sens Netw 16(10):1550147720964358
20. Gomathy V, Padhy N, Samanta D, Sivaram M, Jain V, Amiri IS (2020) Malicious node detection using a heterogeneous cluster-based secure routing protocol (HCBS) in wireless adhoc sensor networks. J Ambient Intell Humaniz Comput 11(11):4995–5001
21. Koyuncu H, Tomar GS, Sharma D (2020) A new energy efficient multitier deterministic energy-efficient clustering routing protocol for wireless sensor networks. Symmetry 12(5):837
22. Bhola J, Soni S, Cheema GK (2020) Genetic algorithm-based optimized leach protocol for energy-efficient wireless sensor networks. J Ambient Intell Humaniz Comput 11(3):1281–1288
23. Haseeb K, Islam N, Javed Y, Tariq U (2021) A lightweight secure and energy-efficient fog-based routing protocol for constraint sensors network. Energies 14(1):89
24. Haseeb K, Almustafa KM, Jan Z, Saba T, Tariq U (2020) Secure and energy-aware heuristic routing protocol for wireless sensor network. IEEE Access 8:163962–163974
25. Gonzalez-Gil P, Martinez JA, Skarmeta AF (2020) Lightweight Data-Security Ontology for IoT. Sensors 20(3):801
26. Dib O, Huyart C, Toumi K (2020) A novel data exploitation framework based on blockchain. Pervas Mob Comput 61:101104
27. Huang Z, Wang Q (2020) A PUF-based unified identity verification framework for secure IoT hardware via device authentication. World Wide Web 23(2):1057–1088
28. Zahoor S, Mir RN (2020) A parallelization based data management framework for pervasive IoT applications. Scal Comput Pract Exp 21(3):463–477
29. Sankaranarayanan S, Rodrigues JJ, Sugumaran V, Kozlov S (2020) Data flow and distributed deep neural network-based low latency IoT-Edge computation model for big data environment. Eng Appl Artif Intell 94:103785
30. Doumiati S, Assaad M, Artail HA (2019) A framework of topological interference management and clustering for D2D networks. IEEE Trans Commun 67(11):7856–7871
31. Viejo A, Sánchez D (2020) Secure monitoring in IoT-based services via fog orchestration. Fut Gen Comput Syst 107:443–457
32. Sarrab M, Alshohoumi F (2021) Assisted-fog-based framework for IoT-based healthcare data preservation. Int J Cloud Appl Comput (IJCAC) 11(2):1–16