ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20250107002242
Original scientific paper

Secure Cloud Data Distribution using Blockchain and Explainable Deep Learning for Enhanced Privacy

S. JAYANTHI*, A. VALARMATHI

Abstract: The distribution of sensitive information in the cloud presents significant privacy and security challenges, especially for industries such as defense and healthcare, where safeguarding data is critical for collaboration and decision-making. The growing reliance on cloud servers for data storage by enterprises and their clients exacerbates risks to user privacy and data security. This study proposes a novel, secure cloud data distribution system designed to offer dynamic user access while addressing confidentiality concerns. The methodology leverages blockchain technology to enable decentralized and distributed data storage, ensuring tamper-proof transactions and enhanced security through tokenized value systems. A feature attribution-explainable deep learning model (FA-XDLM) is integrated into the framework to enhance transparency and security. This model highlights the significance of individual data features in influencing predictions, offering interpretability for data access and processing. The encryption mechanism within the FA-XDLM framework further protects sensitive information by securing data during storage and transmission. Blockchain technology is employed to confidently transmit data to cloud servers, implementing advanced storage methods to uphold data privacy. Experimental evaluations reveal the proposed system's high effectiveness, achieving an accuracy rate of 99.12%. This approach not only addresses data security challenges but also fosters trust in cloud environments by providing reliable access, confidentiality, and privacy. The combination of blockchain technology with explainable AI ensures an innovative solution for secure cloud data distribution, meeting the growing demands of sensitive industries.

Keywords: blockchain; cloud data security; explainable AI; data privacy; secure storage solutions

1 INTRODUCTION

Data storage to cloud has gained prominence owing to its dynamic scalability, cost efficacy, and approachability [1]. Nonetheless, the simplicity of cloud storage presents the contest of safeguarding data, which has emerged as a vital concern for cloud service suppliers. Cloud data storage security presents several challenges as it must ensure the system accuracy, data privacy [2], and the information accessibility of the system [3]. Access control mechanisms must be implemented to limit unlicensed access to the data. Simultaneously, encryption methods of data offer an extra degree of security by making the data incomprehensible to unauthorized individuals [4].

Moreover, the significance and requirement of privacy-preserving aimed data search algorithms are becoming manifest in cloud based real time process.For instance, substantial corporations utilizing public cloud amenities such as Google, Amazon and others, may access delicate data; hence, concealing search queries and retrieved information is crucial for safeguarding the privacy of cloud service users [5]. Lately, numerous encryption systems are utilizing keyword search based methodologies to safeguard the privacy of outsourced data [6-8]. In all these approaches, the authorized source information initially encrypts the data prior to contract it out and subsequently retrieves it via keyword search [6] or ranked keyword search [7]. The symmetric-key cryptography [8] based systems and the public-key cryptography [7] based systems are commonly proposed by the researchers. However, these encryption algorithm protocols consume excessive CPU period and memory resources on the client during the encryption and decryption processes. The reedy client possesses limited bandwidth, CPU power, and memory; hence, typical encryption techniques are ineffective in a cloud setting.

AI-driven encryption is transforming cybersecurity by offering advanced security capabilities that were hitherto unachievable. A primary benefit of AI-driven encryption is its capacity to adapt and evolve in real world scenario, continuously assessing and learning from emerging threats to ensure data security [9]. Conventional encryption techniques frequently depend on fixed algorithms, rendering them susceptible to new cyber threats [10]; in contrast, AI can discern trends and abnormalities in data activity, proactively recognizing potential security issues [11]. In the dynamic field of AI-driven encryption [10, 11], certain issues and constraints require meticulous attention. A major disadvantage is the risk of excessive dependence on AI algorithms, which may result in a misleading sense of security [12]. Although AI can substantially improve cybersecurity protocols, it is imperative for enterprises to acknowledge that no system is impervious. Moreover, the application of AI in encryption raises issues about privacy and ethical considerations. The aggregation and examination of extensive data sets by AI systems may prompt inquiries over the utilization of this information and the potential for its misuse.To eliminate the above difficulties this study proposes the innovative integration of explainable artificial Intelligent (XAI) to Blockchain based secondary security protocol (FA-XDL-BCM) for secure privacy-preserving of cloud data storage and access.

2 RELATED WORKS

The novelists of the research article examined diverse methodologies and proposed procedures and strategies to safeguard data in cloud computing and edge computing environments [13]. The survey paper [14] examined contemporary privacy-preserving approaches, emphasizing various privacy-related frameworks for practical implementation. In [15], the storage of data in cloud atmospheres via frolicsome in addition to privacy-preserving delegable evidences is discussed. The resistant of storage method guarantees data privacy on one hand, while its accompanying functionalities facilitate the auditing of third-party access on the other hand. Consequently, the delegable declaration ensures security at all times with minimal computational time and achieves great efficiency in cloud data storage.

The work [16] examines alternative privacy-preserving approaches for managing the security of stored data in the cloud. This analysis is classified as probability dependent privacy, cryptography dependent privacy, ranking based privacy, and anonymization based privacy. This classification aids in the analysis and reviewing of data concerning unlawful access. Consequently, the aforementioned approaches effectively guarantee confidentiality and truthfulness of the data. In [17-19], rapid and confidential text categorization is executed with the abundantly homomorphic encryption practice. The plaintext system model is first created by encrypting consumer inputs and the training model with the encrypted information. This training procedure reduces the value of loss and enhances classification efficacy. The system uses a natural - Language processing public dataset to execute these tasks in approximately 0.182 seconds.

In [17], the author thoroughly analyzes three traditional [18-20] and seven hybrid cloud computing [21-24] access control systems, highlighting the significance of granularity in model selection and illustrating the advantages of delicate arrangement of access control mechanisms.

This paper [25] proposes a novel biometric authentication scheme for data security and redundancy reduction in cloud storage using Gabor filter and XOR encryption. Every authorized user is given a different "bio-key", permitting access to authentication only to the bio-key holder. The performance gain reduced the overhead of computation and communications are demonstrated through the proposed method. This method seeks to provide a secure and efficient redundancy to verify users' identities in the cloud environment, without imposing high computational costs, as data breaches and unauthorized access remain major problems. The scheme provides a highly effective security solution that utilizes biometric data and cryptographic techniques to mitigate such attacks. This scheme can be extended along with a multi-factor authentication mechanism to make it even more secure as a future scope of research. Gabor filters provide a practically efficient method for feature extraction from biometric data, while XOR encryption acts as an also efficient form of protection against data compromise.

The author of [26] proposeda biometric authentication scheme using a Gabor filter and XOR encryption to improve data security and reduce redundancy in cloud storage. The proposed scheme generates a "bio-key" for authentication, accessible only to authorized users, and its performance is shown to have lower computation and communication costs. In [27], the author detailed the privacy vulnerability in CiphertextPolicy ABE where the exposed access policies leak sensitive information. It proposes a hashingbased technique to conceal these policies and uses signature validation to improve security, ultimately enhancing privacy and security in cloud computing.

To summarize, while prior research has presented encryption methods, it has failed to sustain a robust security framework for data storage in the cloud, despite researchers' emphasis on data security and privacy in cloud contexts. As a result, this study proposed reliable and plausible data privacy preservation protocol based on the explainable AI technique with blockchain protocol dependent secondary authentication system model. The proposed FA-XDL-BCM model having four stages of the execution protocol, in each stage it ensures the data security and integrity.

The Key contribution of the proposed methodology can be summarized as follows:

a. In the primary stage the actual source database has undergone preliminary process of data cleaning, noise reduction and the distributed sets areperformed to create the intermediate dataset of original dataset.
b. The second stage introduces the innovative FA-XDL (Feature attributed based explainable modified deep learning) model to execute the AI driven encryption to create the ciphertext-DB. This stage ensures the plausible data privacy preservation.
c. In the third stage, the study introduces the secondary level (both private and public) ciphertext key generation based on the blockchain technology. The stage improves the final secured cloud data storage.
d. The final stage ensures the accessibility of the authorized users, to access the stored ciphertext DB information via the proposed decryption method. This stage shows the overall system efficiency in terms of the processing time of access.

The rest of the paper is organized as follows: Section III gives the detailed mathematical derivation of the proposed FA-XDL (MM-PFG and XDL)model, secondary level security using blockchain protocol and finally the authorized user secure retrieval of the information from cloud storage. In section IV, the proposed system model performance is analyzed in terms of multiple KPI (Key Performance Index) parameters. Finally we conclude the work with future enhancement in Section V.

3 PROPOSED WORK

The Explainable AI-based modified deep learning model (XDL) incorporates feature attributions (FA) into its framework. Feature attributions (FA) denote the extent to which each feature in our model influenced the predictions for each specific case. The proposed model generates predictions accompanied with feature attribution data, the proposed methodology having four stages of the implementation procedure.

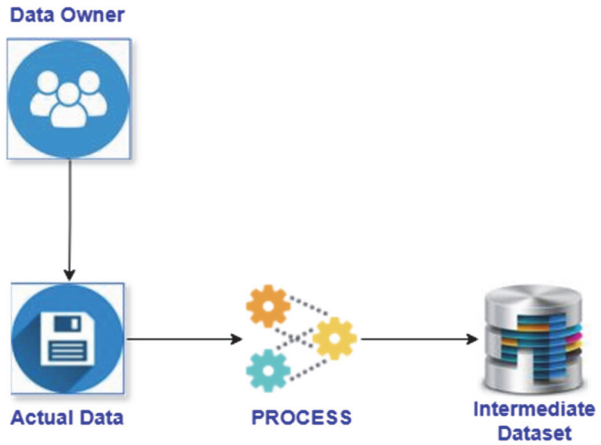

Figure 1 Proposed stage-1 process flow

Fig. 1 demonstrates the flow process of primary Phase. In primary phase the data proprietors upload their text

documents to cloud storage for subsequent usage. The stored data is substantial in size, resulting in increased time of process and expenses when implementing security measures. Consequently, the data owners manipulate the dataset in accordance with their specifications and generate intermediate data to facilitate their analysis.

The intermediate data is kept in an encrypted manner, executed in accordance with the FA-XDL model in subsequentsteps. The FA-XDL model offers local explanations by locally fitting an interpretable surrogate model to each prediction. This local explanation frequently elucidates the rationale behind the diagnosis of a network activity pattern.We employ a modified deep model based on the Explainable AI-FA framework. It additionally entails benchmarking black-box AI models, as seen in Fig. 2.

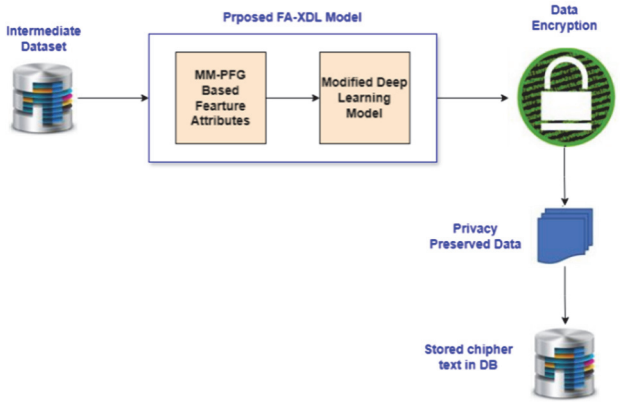

Figure 2 Proposed FA-XDL model

Proposed Stage 2 Model-1: Modified-FCM Algorithm

The original dataset $S=\{s_1,s_2,s_3\ldots..s_n\}$ represents the collection of n objects to be categorized based on an identity circumstance, where $S_i \in R^d$ for $i=1,2,3\ldots n$ and c is the total number of groups $1 \le c < n$.

The minimization function is expressed as:

$$Q = \text{minimize}\, J_m(X,Z) = \sum_{i=1}^{n}\sum_{j=1}^{c}\left(z_{ij}\right)^m s_i, x_j{}^2 \tag{1}$$

where $Z = z_{ij}$ denotes the every object i community matrix to the group of j, the vector $X=\{x_1,x_2,\ldots..x_c\}$ is the total number of centroids, where x_j represents the centroids of groups j; m is the weighting exponent used to measure the group overhead; $s_i, x_j{}^2$ represents the fitness Euclidean distance in the middle of the object s_i and the centroid x_j for $i=1,2,3\ldots n$ and $j=1,2,3\ldots c$.

The projected model of X, Z with respect to minimizing J_m, is attained as

$$x_j = \frac{\left(\sum_{i=1}^{n}\left(z_{ij}\right)^m s_i\right)}{\sum_{i=1}^{n}\left(z_{ij}\right)^m} \quad 1 \le j \le c \tag{2}$$

$$z_{ij} = \frac{1}{\sum_{k=1}^{c}\left(\frac{\left(s_i, x_j{}^2\right)}{s_k, x_k{}^2}\right)^{\frac{1}{m-1}}} \tag{3}$$

$1 \le i \le n; 1 \le j \le c$

The vectors of s_i and x_i belong to the prime space R^d and are signified as,

$$s_i = \left(s_1, s_2, s_3, \ldots..s_d\right),\ 1 \le i < n \tag{4}$$

$$x_i = \left(x_1, x_2, x_3, \ldots\ldots x_d\right), 1 \le j < c \tag{5}$$

The improved fuzzy groupings are generated using the following criteria:

$$z_{ij} \in [0,1], 1 \le j < c-1, 1 \le i \le n+1 \tag{6}$$

$$\sum_{j=1}^{c} z_{ij} = 1, 1 \le i \le n+1 \tag{7}$$

$$0 < \left(\sum_{i=1}^{n} z_{ij} < n, 1 \le j \le c+1\right) \tag{8}$$

A value in the middle of zero and one is required for an object's degree of community to a group j, as shown in Eq. (6). According to Eq. (7), it is guaranteed to the total rank of community of entity i to all groups will be 1.

Algorithm 1: Proposed MM-PFG

---

1 Input: Actual Dataset S, c, m, ϵ' , J , L, flag_break;
2 Output: X, Z
3 Initializations;
4 $J = 1$;
5 do again
6 Level-1(S, c, P);
7 Return X'
8 Level-2(S, X', ϵ' , P);
9 Return X'';
10 $J = J + 1$;
11 while ($J \le L$) ;
12 Find lowest objective function value using Z''
13 Return Z
14 calculate:
15 Obtain the value of centroids using Eq. (2)
16 Return X
17 Using S, V'', m, P modify and measure the Community matrix via Eq. (3)
18 Return Z
19 IF $\max\left[z_{ij}^{q} - z_{ij}^{q+1}\right] < \epsilon'$ then;
20 flag_break = 0;
21 Else
21 $z^q = z^{q+1}$ and $q = q+1$;
22 Flag_break = 1;
23 IF flag_break = 1 Then go to calculate:
24 End

The Allgorithm-1 MM-PFG is delineated into three steps. Included in the list of involvement parameters are the following: dataset vector S, clusters count value c, the boundary value ϵ' Return and ϵ_0, the number of drift P, the iteration counter r_1, the repetition assigner i, and the flag of stop condition. The centroids Z and the values of the community matrix Z are the components that make up the output parameters. The collection of information pertinent to this stage can be found in Algorithm -1, namely lines 1 through 13.

The initial phase involves the parallelization of the Level-1 method. The subsequent stage involves the parallelization of the Level-2 method. Our approach executes Level-1 and Level-2 solitary times and chooses the iteration reference of minimal impartial function significance from the one outcomes. The aforementioned serves as the foundation for the selection of the end of the centroids. The end of the centroids are converted to a community matrix via the Eq. (3) of s function. The community matrix is supplied as input parameters to the improved-FuzCM protocol. The s function and the improved-FuzCM are parallelized in final phase.

Algorithm 2: Level-1 (*S*, *c*, *P*)

---

1 Initialization:
2 $S = \{s_1, s_2, s_3, \ldots..s_n\}$;
3 fixing the value of k_1;
4 Create null set vector $X = \varnothing$;
5 Random selection of primary centroid
$X = X \cup \{s_i\}$;
6 For $i = 1$ to k_1
7 Selecting the i^{th} centroid $s_i \in S$ using Probability function
8 $X = X \cup \{s_i\}$;
9 End For
10 Return X
11 Close of Level-1 Algorithm

Proposed MM-PFG protocol illustrates the centroids initialization using the Level-1 parallelized technique. With the dataset S and the specified value of k, the subsequent phase involves uniformly randomly selecting the initial centroid k_1 from dataset S. It should then be integrated into the cumulative centroids designated as X. The next fitness of the centroid calculation delays until the number of centroids reaches k, the i^{th} centroid must be chosen based on a distribution of probability function.

Algorithm 3: Level-2 (*S*, *X'*, ϵ', *P*)

---

1 Initialization:
2 $S = \{s_1, s_2, s_3, \ldots..s_n\}$;
3 $X = \{x_1, x_2, x_3, \ldots\ldots x_k\}$;
3 Assign convergence threshold value ϵ_0
4 Grouping:
5 For $s_i \in S$ and $x_k \in X$
6 Assign the cluster weight between [0, 1]
7 Measure the Euclidean distance of S_i to the k Centroids
8 Enumerate η
9 End For
10 IF $\eta < \epsilon_0$ then Stop:
11 Else Go to Grouping:
12 End of Level-2 Algorithm

The Level-2 Algorithm expedites the maximum boundary execution by terminating the procedure whenever the entire count of objects altering membership of cluster in a solitary repetition falls below a specified boundary. This value denotes the correlation in the middle of exertion for computing and solution superiority. In each iteration, the indicator η shows what proportion of objects switch clusters. Fig. 3 shows the complete flow diagram of the Modified Multiple Parallelized Fuzzy Groping (MM-PFG).

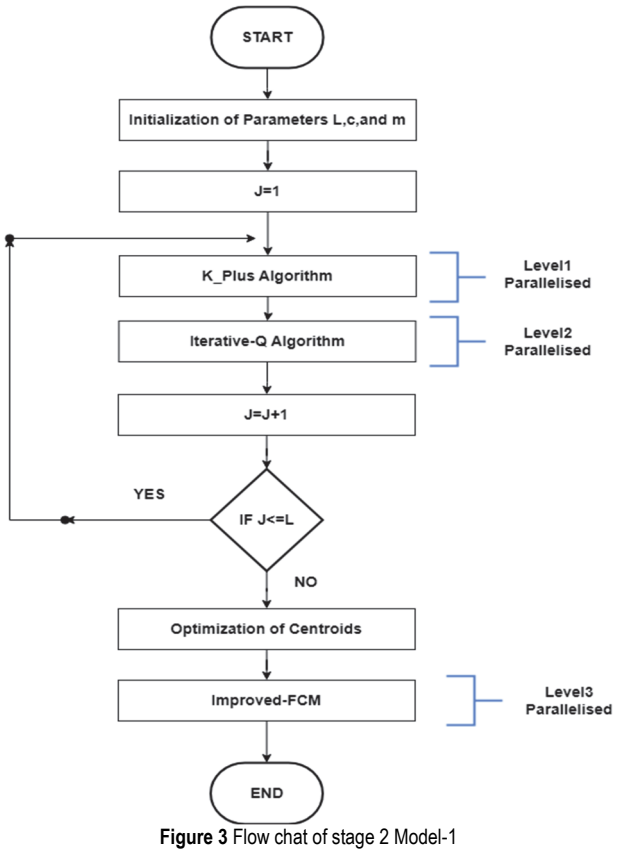

Figure 3 Flow chat of stage 2 Model-1

Our proposed XDL model offers capabilities to evaluate the critical impact of specific training data examples and detect network responses under poisoning attacks. The quality of individual data points requires thorough understanding when improving model reliability and robustness since data quality assurance might not always be feasible. We enhance model integrity using kernel techniques for FA because they discover and eliminate adverse data points which threaten model validity. This feature becomes crucial in safety-related systems which need predictions that remain trustworthy under data corruption conditions. Openness and responsibility increased trust in the deployment of deep learning models is dependent on FA techniques that offer deep learning model decision-making explanations.

Proposed Stage 2 Model-2: XDL Model

The modified deep learning model integerates with the Feature attribute MM-PFG protocol to evaluate the proposed Feature attributes based Explainable Deep Model (FA-XDL-Model). The Feature attribute based group-level protection uses some alliance function for the data and the definition of "neighbouring" FA-Group data is modified to include all samples from one group. The suggested encryption technique uses two datasets, *Z* and *Z*^', which are the adjacent group data, and are based on Feature Attribute (FA). In any case, the suggested XDL approach guarantees ϵ-differential privacy for two adjacent FA-based datasets.

$$Z\left[XDL(Z)\in S\right]\le \exp(\epsilon)\times Z\left[XDL(Z')\in S\right] \tag{9}$$

The parameter ε is referred to as the privacy parameter. It regulates the degree of protection afforded by Eq. (9) for the particular unit of privacy: smaller ε values yield greater protection as the output distributions of the mechanism on adjacent datasets groups converge.The modified deep network performs the extraction sensitive information from the FA-MPG outputs by utilizing its activation layers and enable function.The activation layer is determined using the input layer weight (W_{c1}) and bias (b_{c1}).

Algorithm 4: Proposed FA-XDL Model

---

1 INPUTS:

Training data *Z*, consisting of *X* users

$Z = U_{u=1,2,\ldots X} Z_u$,

User data $Z_u = (X_u, Y_u)$ consisting of Feature Attributes,

$f(a:\theta) \rightarrow$ The input "*a*" parameterized by θ ,

$L(b,b') \rightarrow$ Loss function of FA *b* and *b'*

$T \rightarrow$ Total number of rounds

$\eta_{s1} \rightarrow$ Learning rate of global updates

$\eta_{c1} \rightarrow$ Learning rate of local updates

$k \rightarrow$ Total number of local iterations

$H_c \rightarrow$ Number of user groups per round

$H_m \rightarrow$ Local Batch size

2 OUTPUTS:

θ_{T1} End model parameter

$\theta_0 \leftarrow$ Initialized values based on random manner

For Round of global $t \leftarrow 1$ to T_0 do again

The subset was selected at random from among users *S*^*t*.

Of H_c users

For each user $v \in S^t$ do again

Initialize $\omega_u^0 = \theta_{t-1}$; user model

For Local iteration $k_1 \leftarrow 1$ to K do again

$$\hat{\chi}_u^t \leftarrow \chi_u^t / \max\left(1, \frac{\chi_{u2}^t}{c}\right)$$

$$\chi^t \leftarrow \frac{1}{H_c}\left(\sum_{i\in S}\hat{\chi}_i^t + \mathcal{N}\left(0,\sigma^2 C^2 1\right)\right)$$

$$\theta_t \leftarrow \theta_t - \eta_{s1}\bar{\chi}^t$$

Update global model

Through MM-PFG protocol the modified deep learning model operates as an integrated solution. This integration allows the assessment of Feature attributes based Explainable Deep Model (FA-XDLModel). The Feature attribute based group-level protection requires data to apply an alliance function which redefines neighbouring FA-Group data to encompass all samples from the same group. The encryption procedure operates with two Feature Attribute (FA) based datasets which contain group data from neighbouring areas. One FA-Group dataset exists as a duplicate of another dataset except for having at least one record that differs between groups.

Key Generation and Encryption

The randomly selected two large prime numbers *e* and *f* are independent of each other. Assume $n = ef$ and $\lambda = (e-1, f-1)$ with the reference of assumption of the indiscriminate integer g necessity to be elected as $g \in \mathcal{Z}_{n^2}^*$. Work out the multiplicative $\left(L\left(g^\lambda \bmod n^2\right)\right)^{-1} \bmod n$. Here L_c is calculated *as* $L_c(x) = x - 1/n$.

The public key and private key are expressed as follows:

$$\text{PublicKey} = (n, g) \tag{10}$$

$$\text{PrivateKey} = (\lambda, \mu) \tag{11}$$

$$\text{Chipertext} = g^m \cdot r^n \bmod n^2 \tag{12}$$

The system reaches its data security level through its implementation of modified Paillier encryption (mPE) along with enhanced solitary sign-on (ISSO). ISS-O functions first by using a verification process to validate users through their trusted thirdparty websites before they obtain database access permissions. The authentication process uses credential sharing between the service provider and identity provider. After authentication processes are complete the system uses mPE to encrypt the data. The mPE method generates a partially homomorphicsystem to handle limited binary data encryption operations before adding decryption functions for building a complete homomorphic structure. The mPE algorithm contains three fundamental operational procedures as key generation followed by encryption and then decryption. The approach suits cloud computing platforms well since data processing operations run on third-party servers.

Secured Storage and Verification of the Ciphertext-DB using Blockchain Technology

The proposed method integrates with the block chain methodology to store the data in secure and confidential manner. Secure access control employs decentralized identity management and cryptographic user authentication.

For this purpose this work proposes the Innovative Master Access Control based on the data storage and the retrieval of the required information. Our system maintains an index of hashed pointers to the dataset records on the blockchain utilizing the permission-ledger platform. The specifics of ciphertext -DB data will be delegated to the cloud server. The Fig. 4 shows the proposed ciphertext database information end storage of the cloud platform utilizing the blockchain protocol.

Use of Blockchain Technology for a secure storage and verification of the ciphertext database for managing identities and attributes in a decentralized manner. There are two phases in the protocol, in which the first phase employs a smart contract as an interface and coordinates the identification and the attribute management. In the second phase, the smart contract focuses more on the digital address which is made of a private key and a number of properties such as public keys or signatures.

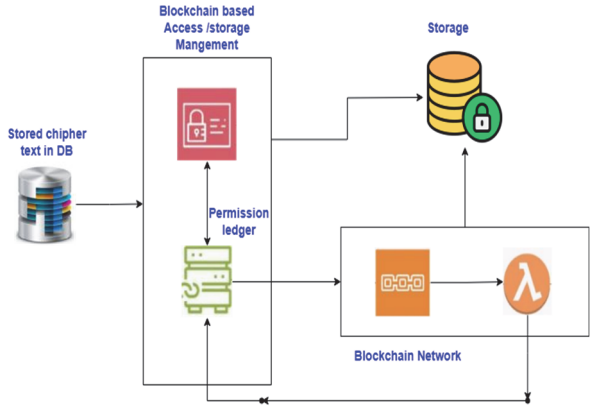

Figure 4 Secured blockchain based end cloud storage

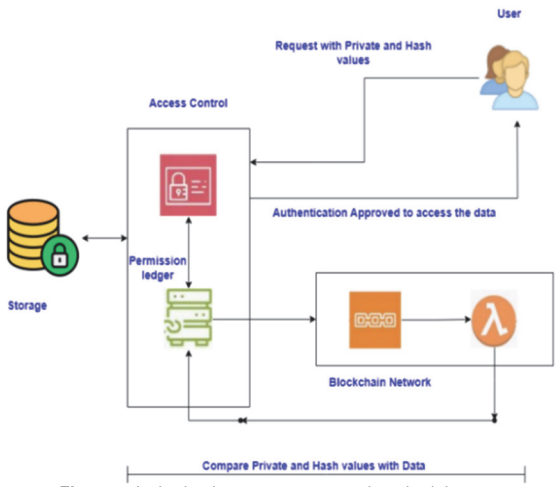

Figure 5 Authorized user access control methodology

The authorized entities have the capability to utilize their private keys for decrypting the ciphertext -DB. Furthermore, the user can produce a completely reliable zero-knowledge proof π_0 derived from their own data and present it to smart contracts on the blockchain. Utilizing the attributes of zero-knowledge proof, π_0 can ascertain whether user data satisfies the conditions proposed by the data owner.

Decryption

In the decryption process the ciphertext c_d need to decrypt and the c_d value fits in to $\mathbb{Z}^*_{n^2}$. Utilizing the decryption key, the plain text from the ciphertext DB is found as follows:

$$P_d = L\left(c_d^{\lambda} \operatorname{mon} n^2\right).\mu_d \bmod n \tag{13}$$

4 RESULTS AND DISCUSSION

The deliberated modified explainable deep learning model (FA-XDL) with second level security based on blockchain protocol system produces the outperform ability in the aspect of data security and privacy-preservation. The experimental process utilizes the Kaggle dataset [32]. This procedure calculates the connotation in the middle of the intermediate dataset features attributes and the respective contacts. This will help to forecast strong data privacy security and reduce the computational complexity of encryption stage redundancy issues.

The proposed FA-XDL with blockchain model key performance parameters like model-accuracy, model-Precision, model-Recall and finally the model-F1 values are computed. These values are compared with the recent conventional model KPI's.

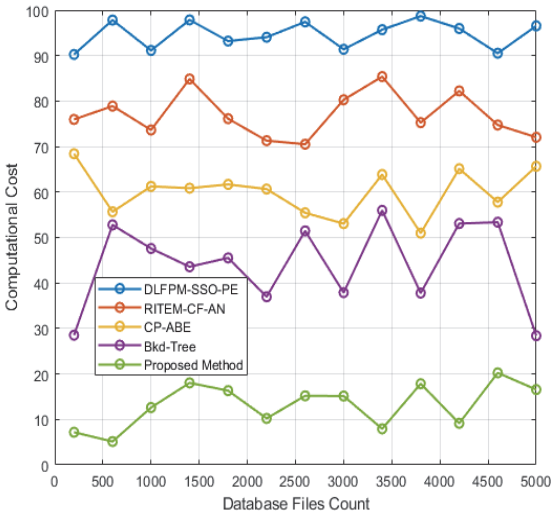

Figure 6 Comparisons of proposed technique computation cost

Fig. 6 demonstrated the computational expense associated with encrypting the information in the intermediate dataset. The technique incurs minimal costs for evaluating retrieval of the data, classifying delicate information, and executing encryption processes. In Fig. 7a, the innovated procedure reaches the diminished time of computation compared with the recent conventional methods of DeepLFPM-SS0PE [22], ReITEM-CLFAN [29], ConPABE [19] and BKDTree [16], the feature attribute based dataset parallelized protocol performing the initial authentication layer; in this layer itself the privacy of the user begins to increase. The suggested explainable modified deep learning model-based encryption and decryption performs better than the encryption and decryption of user/owner data details (Fig. 8) in comparison.

Fig. 9 exemplified the entire systems overall running process of privacy accuracy. The proposed model trained with respect to the MM-PFG model's outcome data points to feed these data points to the modified deep learning model. So this procedure compensates the network value

of bias and weight rendering to the Model-training function.

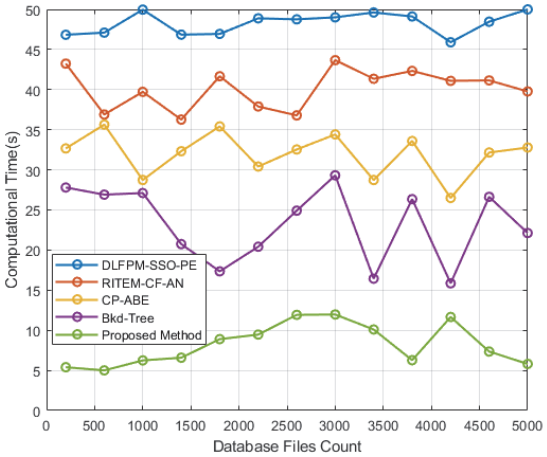

Figure 7 Computation time-proposed MM-PFG model

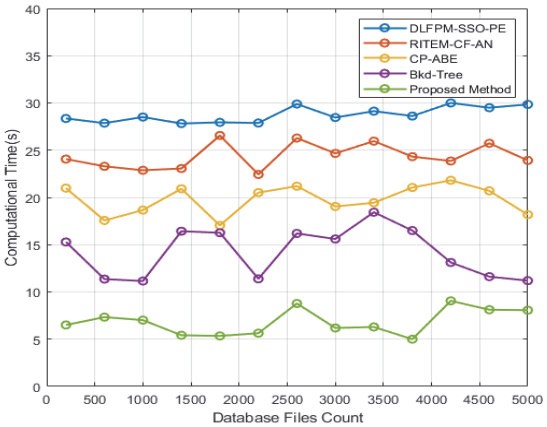

Figure 8 Computation time of proposed FA-XDL model

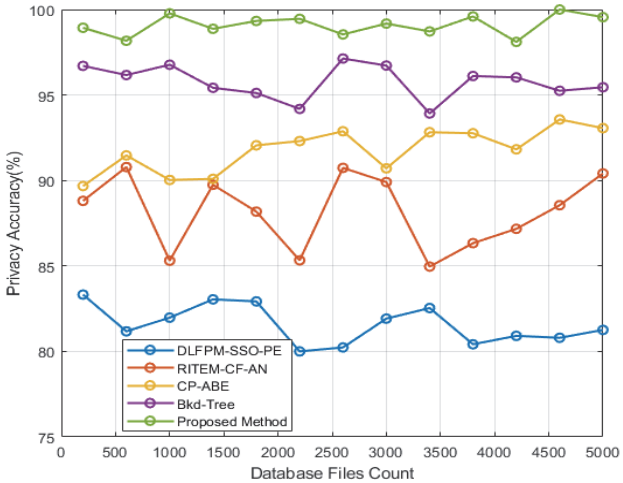

Figure 9 Comparison of the proposed FA-XDL–BC-model overall privacy accuracy with conventional methods

Fig. 10 illustrates that the proposed technique processes plaintext in the least amount of time, indicating that it provides security more rapidly than existing methods. Each instance, the secondary authentication key values are chosen randomly toenhance security, as transient users find it challenging to predict the key values. Fig. 11 shows the innovated FA-XDL-BCM procedure outperforms the overall system efficiency compared with the recent conventional methods of DeepLFPM-SS0PE, ReITEM-CLFAN, ConPABE and BKDTree.

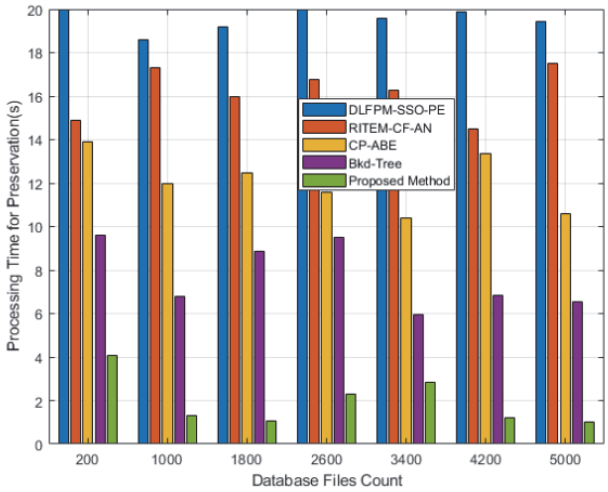

Figure 10 Comparison of the proposed model processing time

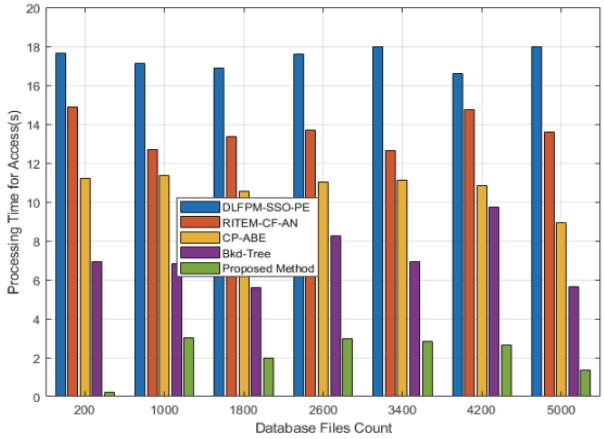

Figure 11 Proposed FA-XDL-BCM systems overall efficiency

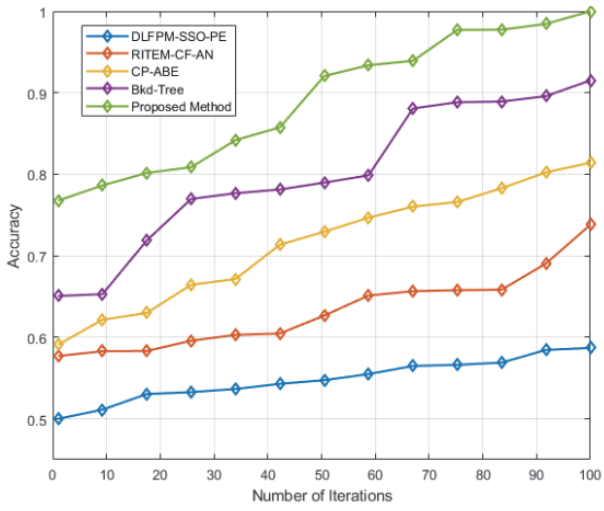

Figure 12 Proposed model accuracy curves

From Figs. 12, 13, 14, and 15 the proposed FA-XDL-BCM model KPIs(Key performance indicator) of $Accuracy_{\text{FA-XDL}}$,$(Precision)_{\text{FA-XDL}}$, $(Recall)_{\text{FA-XDL}}$, and finally $(F1-Score)_{\text{FA-XDL}}$ curve values are compared to the recent other algorithms named DeepLFPM-SS0PE, ReITEM-CLFAN,ConPABE and BKDTree. From these evalution results the proposed method obtains the outperform value of $Accuracy_{\text{FA-XDL}} = 99.89\%$ $(Precision)_{\text{FA-XDL}} = 98.89\%$, and recall value is 93.98%.

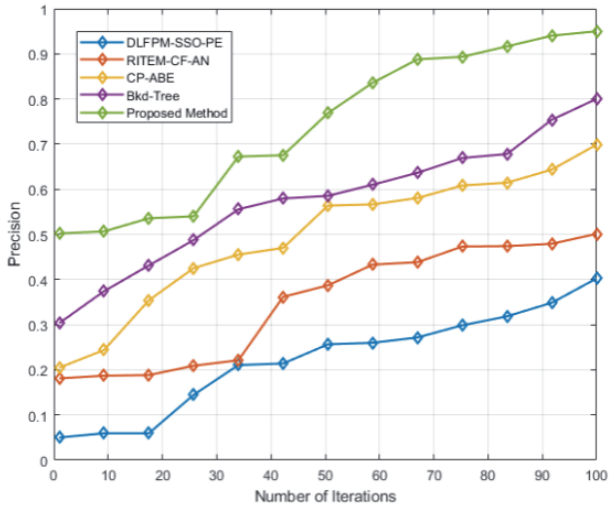

Figure 13 Proposed model precision curve

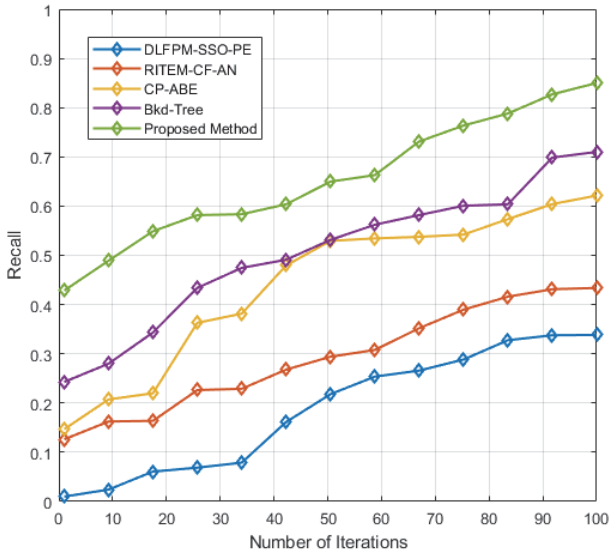

Figure 14 Proposed model recall curves

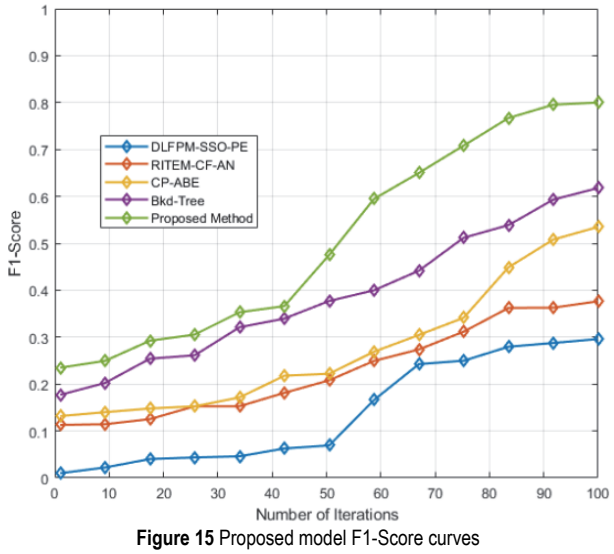

Figure 15 Proposed model F1-Score curves

Fig. 16 shows the different KPI parameters of the cloud data processing like data integrity, data confidentiality, data privacy and retrieval speed of the model. The following Tab. 1 proves our proposed method achieves optimal security and privacy for the shared intermediate data on the third-party server. The achieved efficiency surpasses that of the methods examined in the analytical review.

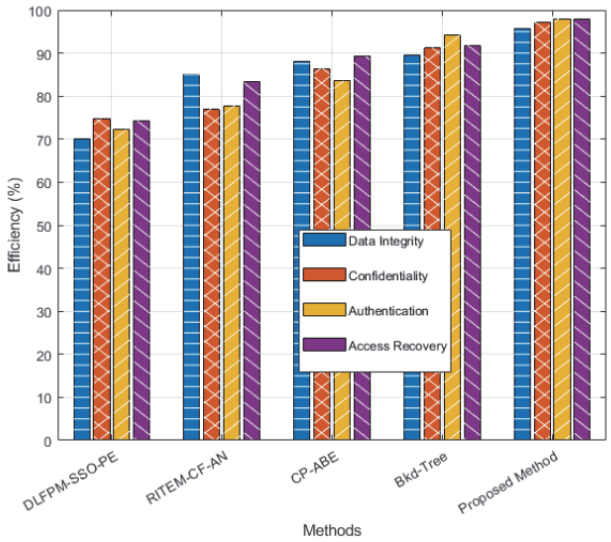

Figure 16 Proposed model overall system KPI efficiency

Table 1 Proposed FA-XDL-BCM model efficiency analysis

METHODS	DI	CFD	AT	AZ
DeepLFPM-SS0PE	78.78	79.56	81.28	84.45
RelTEM	91.61	89.10	78.12	84.52
CLFAN	92.89	91.10	89.87	89.52
ConPABE	94.45	93.14	91.52	93.92
Proposed FA-XDL	94.86	95.62	98.81	98.72

DI - Data Integrity, CFD - data Confidentiality, AT - Authentication, AZ - Authorization

5 CONCLUSION

This article evaluates the Feature attribute based explainable modified deep learning model's encryption protocol. The proposed explainable AI model encryption with blockchain dependent secondary secured protocol is utilized for storing or access the data to the cloud environments. This method results show that the user /owner can utilize their information with plausible security concerns. The source data convert to the intermediate data, this process diminishes the entire computation cost value and the complexity. The proposed XDL network modernizes all the feature attributes of the entire information. This will increase the system efficiency in terms of data access time. The system is utilizing the blockchain based secondary security protocol. This will produce the privacy accuracy value of 96.45% compared to all other conventional methods. The experimental findings indicate a remarkable proposed model accuracy rate of 99.12%. Finally, based on the results of these suggested approaches, future implementation should concentrate on more explainable AI models that require a lot of database data and plan to integrate the IDS system with explainable AI models to improve system dependability.

6 REFERENCES

[1] Shanthi, R., Babu, M. D., Kousika, N., Vijayaraj, C., Choubey, S. B., & Sambooranalaxmi, S. (2024). Advanced Privacy-Preserving Framework Using Homomorphic Encryption and Adaptive Privacy Parameters for Scalable

Big Data Analysis. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(11s), 160-165.
[2] Martyushev, N. V., Malozyomov, B. V., Sorokova, S. N., Efremenkov, E. A., Valuev, D. V., & Qi, M. (2023). Review models and methods for determining and predicting the reliability of technical systems and transport. *Mathematics*, *11*(15), 3317. https://doi.org/10.3390/math11153317
[3] Kaissis, G., Ziller, A., Passerat-Palmbach, J., Ryffel, T., Usynin, D., Trask, A., & Braren, R. (2021). End-to-end privacy-preserving deep learning on multi-institutional medical imaging. *Nature Machine Intelligence*, *3*(6), 473-484. https://doi.org/10.1038/s42256-021-00337-8
[4] Kumar, P., Kumar, R., Srivastava, G., Gupta, G. P., Tripathi, R., Gadekallu, T. R., & Xiong, N. (2021). PPSF: A privacy-preserving and secure framework using blockchain-based machine learning for IoT-driven smart cities. *IEEE Transactions on Network Science and Engineering*, *8*(3), 2326-2341. https://doi.org/10.1109/TNSE.2021.3089435
[5] Kethireddy, R. R. (2021). AI-Driven Encryption Techniques for Data Security in Cloud Computing. *Journal of Recent Trends in Computer Science and Engineering*, *9*(1), 27-38. https://doi.org/10.70589/JRTCSE.2021.1.3
[6] Zhang, H., Gao, P., Yu, J., Lin, J., & Xiong, N. (2021). Secure and verifiable outsourcing of machine learning tasks using blockchain in cloud computing. *IEEE Transactions on Network Science and Engineering*, *8*(4), 3190-3202. https://doi.org/10.1109/TNSE.2021.3110101
[7] Gao, H., Duan, P., Pan, X., Zhang, X., Ye, K., & Zhong, Z. (2024). Blockchain-enabled supervised secure data sharing and delegation scheme in Web3.0. *Journal of Cloud Computing: Advances, Systems and Applications*, *13*(1), 21. https://doi.org/10.1186/s13677-023-00575-8
[8] Chinnasamy, P., Deepalakshmi, P., Dutta, A. K., You, J., & Joshi, G. P. (2022). Ciphertext-Policy Attribute-Based Encryption for Cloud Storage: Toward Data Privacy and Authentication in AI-Enabled IoT System. *Mathematics*, *10*, 68. https://doi.org/10.3390/math10010068
[9] Alanazi, J., Algahtani, M. M., Alanazi, M., & Alharby, T. N. (2023). Application of different mathematical models based on artificial intelligence techniques to predict the concentration distribution of solute through a polymeric membrane. *Ecotoxicology and Environmental Safety*, *262*, 115183. https://doi.org/10.1016/j.ecoenv.2023.115183
[10] Pérez-Ortega, J., Rey-Figueroa, C. D., Roblero-Aguilar, S. S., Almanza-Ortega, N. N., Zavala-Díaz, C., García-Paredes, S., & Landero-Nájera, V. (2023). POFCM: A Parallel Fuzzy Clustering Algorithm for Large Datasets. *Mathematics*, *11*, 1920. https://doi.org/10.3390/math11081920
[11] Lee, S. J., Song, D. H., Kim, K. B., & Park, H. J. (2021). Efficient fuzzy image stretching for automatic ganglion cyst extraction using fuzzy C-means quantization. *Applied Sciences*, *11*, 12094. https://doi.org/10.3390/app112412094
[12] Fu, Y., Fu, J., & Wei, J. (2023). Encryption and decryption using deep neural networks. Frontiers in Artificial Intelligence and Applications. https://doi.org/10.3233/FAIA230762
[13] Liu, L., Gao, M., Zhang, Y., & Wang, Y. (2022). Application of machine learning in intelligent encryption for digital information of real-time image text under big data. *EURASIP Journal on Wireless Communications and Networking*, *2022*. https://doi.org/10.1186/s13638-022-02111-9
[14] Ding, Y., Tan, F., Qin, Z., Cao, M., Choo, K. K. R., & Qin, Z. (2021). DeepKeyGen: A deep learning-based stream cipher generator for medical image encryption and decryption. *IEEE Transactions on Neural Networks and Learning Systems*, 1-15. https://doi.org/10.1109/TNNLS.2021.3062754
[15] Badri, S. et al. (2023). An efficient and secure model using adaptive optimal deep learning for task scheduling in cloud computing. *Electronics*, *12*(6), 1441. https://doi.org/10.3390/electronics12061441
[16] Hasimi, L., Zavantis, D., Shakshuki, E., & Yasar, A. (2024). Cloud computing security and deep learning: An ANN approach. *Procedia Computer Science*, *231*, 40-47. https://doi.org/10.1016/j.procs.2023.12.155
[17] Samanta, R. K., Sadhukhan, B., Samaddar, H., Sarkar, S., Koner, C., & Ghosh, M. (2022). Scope of machine learning applications for addressing the challenges in next-generation wireless networks. *CAAI Transactions on Intelligence Technology*, *7*(3), 395-418. https://doi.org/10.1049/cit2.12114
[18] Ali, A., Al-Rimy, B. A. S., Alsubaei, F. S., & Almazroi, A. A. (2023). HealthLock: Blockchain-based privacy preservation using homomorphic encryption in Internet of Things healthcare applications. *Sensors*, *23*, 6762. https://doi.org/10.3390/s23156762
[19] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021). BEdgeHealth: A decentralized architecture for edge-based IoMT networks using blockchain. *IEEE Internet of Things Journal*, *8*(14), 11743-11757. https://doi.org/10.1109/JIOT.2021.3058953
[20] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Blockchain and edge computing for decentralized EMRs sharing in federated healthcare. *2020 IEEE Global Communications Conference (GLOBECOM)*, 1-5. https://doi.org/10.1109/GLOBECOM42002.2020.9347951
[21] Deshmukh, J. Y., Yadav, S., & Bhandari, G. (2021). Attribute-based encryption mechanism with privacy-preserving approach in cloud computing. *Materials Today: Proceedings*, *80*, 1786-1791. https://doi.org/10.1016/j.matpr.2021.05.609
[22] Xiong, S., Ni, Q., Wang, L., & Wang, Q. (2020). SEM-ACSIT: Secure and efficient multi-authority access control for IoT cloud storage. *IEEE Internet of Things Journal*, *7*(4), 2914-2927. https://doi.org/10.1109/JIOT.2020.2963899
[23] Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *IEEE Access*, *8*, 131723-131740. https://doi.org/10.1109/ACCESS.2020.3003150
[24] Henze, M. (2020). The quest for secure and privacy-preserving cloud-based industrial cooperation. *2020 IEEE Conference on Communications and Network Security (CNS)*, 1-5. https://doi.org/10.1109/CNS48642.2020.9162199
[25] Khan, B. U. I., Olanrewaju, R. F., Baba, A., & Lone, S. A., Zulkurnain, N. F. (2015). SSM: Secure-Split-Merge data distribution in cloud infrastructure. *IEEE Conference on Open Systems (ICOS)*. https://doi.org/10.1109/ICOS.2015.7377275
[26] M, V., Venkatachalam, K., P, P., Almutairi, A., & Abouhawwash, M. (2021). Secure biometric authentication with deduplication on distributed cloud storage. *PeerJ Computer Science*, e569. https://doi.org/10.7717/peerj-cs.569
[27] Patil, S. P., Basthikodi, M., Kumaraswamy, S., Prabhu, G. A., & Raga, A. (2024). Enhancing data privacy protection in cloud computing through ciphertext-policy attribute-based encryption. *Journal of Electrical Systems*, e1425. https://doi.org/10.52783/jes.1425

Contact information:

S. JAYANTHI
(Corresponding author)
Department of CSE, University College of Engineering,
Anna University (BIT Campus) Trichirappali, Tamil Nadu, India
E-mail: dharsh02@gmail.com

A. VALARMATHI
Department of MCA, University College of Engineering,
Anna University (BIT Campus) Trichirappali, Tamil Nadu, India
E-mail: valarmathicsebit@outlook.com