International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Efficient Big Data Storage in Cloud with Unique Authentication Approach for Privacy Access

S. Subbalakshmi[1], K. Madhavi[2]

Submitted: 25/01/2024 **Revised**: 03/03/2024 **Accepted**: 11/03/2024

Abstract: The growth of in-network services in the IT sector has a significant impact on the storage as well as distribution of data in the cloud. The main problem is addressing customers' worries about data security and privacy because this new computing along with service technology requires users to entrust their critical data to the cloud service provider (CSP). Due to these security and privacy concerns, organizations are still hesitant to put their data on the cloud. Existing encryption techniques can safeguard data secrecy, but there are several downsides, including the risk of sensitive data leakage due to access patterns. The proposed approach combines the production of distinct keys with a security algorithm. The improved Elliptic curve with Diffie-Hellman (IECDH) security technique is used in this study, where unique encryption and decryption data are used. This technique effectively decreased the computing difficulty and encrypted the data. In an experimental examination, evaluation metrics such as computing overhead, decryption time, encryption time, as well as key generation time are used to determine how well the proposed IECDH performs.

Keywords: *Big data; Data Storage; Cloud Computing; Security; Encryption.*

1. Introduction

The term "big data" refers to a vast along with varied collection of data that is expanding at an exponential rate. Due to the presence of malicious users as well as hackers, medical big data face numerous security issues in the modern healthcare system [3].The deployment of cloud and mobile cloud-based large-scale distributed systems, in particular, provides excellent services that enhance people's superiority of life along with boost organizational efficiency [1].The analysis, access, and retrieval of patients' personal and electronic health records (EHRs) are made possible by healthcare big data (HBD) [2].

During the storage phase, the greater part of medical big data are stored on a cloud computing platform. To guarantee the privacy and honesty of the data put away, encryption and it are much of the time used to evaluating systems. Access control components are generally utilized during the information sharing stage to direct the items that approach the information. The security insurance of clinical and wellbeing huge information is done under the management of AI during the information investigation stage [6]. A work investigates recent cybersecurity-related research on big data. It emphasizes how big data can be used for cybersecurity as well as how it can be protected. It has issues, open research challenges, along with presented trends, as well as a summary of current works in the form of tables [11].

The BD as a service as well as storage deployment model has recently gained momentum by provides perceptive insights into BD that drive business intelligence along with other applications for a viable advantage. This finding could be extended in future work by investigate the BD frameworks over equally PaaS as well as BDaaS[8].The best part of data is stored on cloud servers, which are highly vulnerable to threats along with breaches. As a result, they must be protected from unauthorized access immediately. Although they lack a foolproof mechanism, the existing smart health solutions offer a assured level of immunity. In this context, the widespread use as well as success of digital health care depend on a significant research breakthrough that maintains patients' trust and credibility [9].

Some existing methods offer a comprehensive analysis of blockchain for big data, focusing on the most recent methods, opportunities, and possible future paths. First, the methods discuss the relationship between blockchain along with big data and the reasons behind their integration. Then, the overview different blockchain administrations for large information, including blockchain for secure huge information obtaining, information capacity, information investigation, and information protection conservation is discussed [4]. However, despite the fact that current encryption techniques are capable of maintaining the confidentiality of data, access patterns have the potential to leak sensitive information. To enhance cloud data safety, the system employs the Elliptic curve with Diffie–Hellman (ECDH) algorithm for encryption as well as decryption.

[1] *Ph.D Scholar, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University Anantapur, Ananthapuramu, Andhra Pradesh, India*

[2] *Professor, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University Anantapur, Ananthapuramu, Andhra Pradesh, India*

** Corresponding Author Email: subbalakshmi.btech@gmail.com*

This calculation decreased the computational intricacy and scrambled information effectively [5]. Also, the contribution of the proposed security algorithm is given below

- In order to safeguard the data decryption key from external attackers, to assure data owner storage safekeeping, along with to retain privacy, this work proposes the Improved ECDH technique.
- The elliptic curve method used in this work is a straightforward encryption method. Hence, the proposed IECDH technique has a low level of complexity and requires less time to execute.
- In the proposed IECDH approach, all the minute details are likewise encrypted. This strengthens defences against threats and safeguards cloud data.
- A distinct key is created individually for encryption and decryption in the proposed approach.
- As a result, the proposed IECDH approach performs better when compared in terms of variables like processing overhead, decryption time, key generation time, as well as encryption time.

The respite of this work is prearranged as pursues: section 2 presents review some security algorithms proposed recently to solve the issues while storing big data in cloud. Section 3 discusses the proposed Improved ECDH algorithm. Section 4 presents the results achieved and dataset used for simulation.And finally, section 5 gives the conclusion followed by the references.

2. Background Study

Khan, Mudassir, and Mohd Dilshad Ansari. [10]discusses the main attributes in how registering foundations ought to be planned and shrewdly dealt with to achieve the most surprisingly security angles essential by Enormous Information applications. In addition to examining the most recent development for enhance Apache Hadoop security, which is to improve establish big data environments, we classify the accessible experimentation according to the cloud orientation architecture orchestration, corporal source, cloud service activities, along with source manage in various additional managed layers.

Kooet al. [7] confirms the recent standards established by international standardization organizations as well as analyzing related studies, recognizes threats along with security problem that arise throughout the life cycle of big data. What's more, we partition a most important information life cycle into five steps (i.e., examination, assortment, capacity, usage, as well as obliteration), along with characterize the safekeeping scientific categorization of the large information life cycle in light of the recognized dangers as well as security problems.

Yadavet al. [12] reviews traditional confidentiality methods (K-anonymity, T-propinquity, De-identification, along with L-diversity) as well as oversight regarding data confidentiality and security issues, and also reviews the current research challenges. Instructions to accommodate security and protection, security concern as well as security, diverse stage protection saving system, challenges present in remaining alive security along with protection component, investigation of a high-level strategy (Differential security, Character predicated anonymization) for hugely giant information protection in Sizably voluminous information.

Tanet al. [13] defines the access control permission for CPSS big data storage in blockchain in BacCPSS. The processes of authorization revocation, authorization, audit, and access control in BacCPSS are designed, as well as then a lightweight symmetric encryption algorithm is utilized to achieve privacy-preserving. The account address of the node in the blockchain is utilized as the individuality to access CPSS big data in BacCPSS. Finally, an Aliyun along with enviable EOS cloud experimental model is constructed. Results show that BacCPSS is plausible as well as successful, along with can accomplish safe access in CPSS while safeguarding protection.

Shahzad et al. [14] make the best use of our organization's resources, with a Blockchain-based Green big data Visualization (BGbV) solution that makes use of Hyperledger Sawtooth. BGbV will be compatible with the most recent distributed data visualization platforms, guarantee profit like data availability along with security, and reduce storage costs. It saves money by using fewer resources that are previously in use as well as uses less energy, creation it good for the environment.

Huet al. [15] highlights a trust evaluation-based dynamic access control model to address the trust problem posed by each medical cloud system node during interaction. The model fits the comprehensive communication trust value of nodes using the entropy weight method along with fuzzy theory. It also adds a role-based two-way choice mechanism along with a third-party real-time monitoring mechanism for dynamic access control. Give the specific methods as well as procedures. This model has significant advantages in terms of trust accuracy, dynamic controllability, and time complexity when compared to the traditional Eigen-Trust model along with RBAC through simulations as well as comparison experiments.

Hasanet al. [16] discuss about big data as well as the Internet that always offer a ground-breaking resolution to ensuring that the energy Internet, also known as the intelligent grid, is electrically linked. The blockchain has some critical elements, creation it a pertinent innovation for brilliant network norms to tackle the security issues along with trust difficulties. A comprehensive analysis of blockchain implementations, energy data protections, along with cyber security perception in smart grids will be presented in this study.

3. Proposed Methodology

The term "big data" refers to the vast array of intricately dispersed data that has been produced from every current digital source. This work proposes a high-security IECDH technique for cloud storage environments. For effective data encryption, the IECDH employs the symmetric encryption approach. In order to secure cloud data, an improved DH technique based on elliptic curve functions is utilized.The cloud-based large data security paradigm employing the IECDH method is shown in Figure 1. The main components of the proposed architecture are the data owner, the encryption and decryption processes, the key generation, and the text retrieval method. The creation and secure sharing of keys is the main duty of the proposed big data-based security theory.

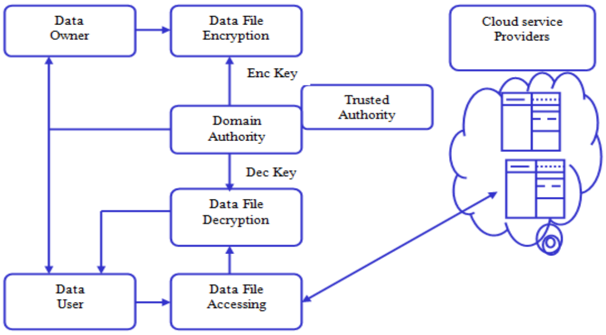

Fig 1. System Architecture

The primary advantage of the IECDH key generation mechanism is the use of smaller keys for encryption and decryption. Additionally, shared, unique secret key creation uses the protected key technique. The next parts provide an explanation of the proposed IECDH algorithm pseudocode. Figure 2 displays a thorough explanation of the suggested block diagram. The necessary trust for outsourcing data to the cloud will be provided by the distinctive integrity agreement between these companies for the data safety utilizes the unique key, which will also preserve the appropriate privacy during access to the data files. After setup, use IECDH to safely distribute the keys between the servers along with client. The data encryption along with decryption procedure used for user data storage as well as retrieval. A data input is divided into a number of segments. Encrypted data blocks are decrypted along with then combined into a single document when the data is accessed. The goal of the challenge as well as proof creation procedure is to validate the segments along with provide authorization for data modification to the authorized user.

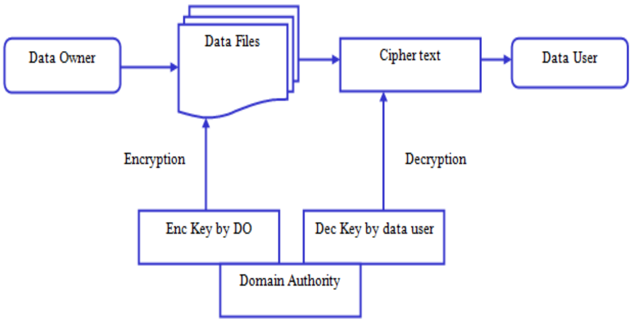

Fig 2. Proposed Encryption and Decryption Process

3.1 Data Owner

The term "data owner" refers to a company or an individual who holds a significant amount of private data. Due to the limited number of calculations and data storage capacities accessible in the cloud, the server configuration of data owners has limited storage capacity. By integrating all cloud databases, the communication module offers integrated database management. The SQL analyzer divides the user query into read-write queries as well as read-only. The SQL distributor chooses the best load-balancing method to carry out the query procedure. The database management system modifies the query request to optimize source use while synchronizing the whole database.

3.2 Key Generation

The data authority (DA) offers an interface for both the data consumer and the data owner to register and create their keys for data encryption. The registration procedure offers legitimate authentication credentials to verify the user's login for domain services. The security key created for the data owner (DO) supported by Trusted Authority (TA) upon its triumphant registration with DA is known as the Unique Encryption Key (E_{key}). This increases the privacy of data access while also making the "encryption" and "decryption" processes for data storage along with access from the cloud simpler.The Diffie-Hellman (DH) mechanism [18], [19] is used to develop the asymmetric key distribution techniques [17] to produce the E_{key}. The "Improved Diffie-Hellman mechanism" as stated in Algorithm1 is used to construct the necessary E_{key}utilizing the secret key values. In this algorithm T is the TA public key for DA, D is the domain service and C is a constant value. The initialization parameters have a condition like $D < T$ and the value of C is 100.

Algorithm 1: Generation of Encryption Key

```
Input    : $T, D$ and $C$
Output   : $E_{key}$
    1.  Generate a random private key $(P)$
    2.  While $(P > T)$ do
```

```
        $P = P - T$
    End while
    $E_{key} = D^P mod(T)$
```

The "DO" uses the created E_{key} to safely store their encrypted data. The E_{key} lifespan lasts for the duration of a DO login session. The DO may communicate and keep their encrypted files without fear of data disclosure or revelation thanks to the unpredictability of E_{key}generation. The decryption of the data is done by a randomly generated decryption key known as D_{key}.Most users often obtain data files as well as decrypt them for their purposes, however in these circumstances, they DO have to share the encrypted key, leaving it vulnerable to key theft attacks. Therefore, it is crucial that the decryption key be secure and that only authorized people have access to it. Hence this work allows users to use a special decryption key, or D_{key}, to save computation time and improve the privacy of the service that users use. The DO encryption key, E_{key}, which is controlled by the DA, is interwoven with the production of the U_{key}.

Evaluate the DO encrypted E_{key} value with the DC decryption D_{key} value was necessary for the early validation of domain data service accessibility. If the comparing values are equal, the user is authenticated to access the relevant data files in that domain data service. Algorithm-2 uses the client's input of the TA public key for a Domain Data Service, S, to illustrate the validation and decryption key formation procedure. Algorithm 3 describes the matching of decryption key along with encryption key.

Algorithm 2: Generation of Decryption Key

Input : $T, D, S\ and\ C$

Output : D_{key}

```
Start
If $(S < T)$ {
    P = Generate Random Private Key $(C)$
    While $(P > T)$ do
        $P = P - T$
    End while
    $D_{key} = S^P mod(T)$
}
End
```

Algorithm 3: Key Validation

Input : $D_{key}\ and\ E_{key}$

Output : Confirm authentication

```
$E_{key} = D^P mod(T)$
$D_{key} = S^P mod(T)$
If $D_{key} = E_{key}$ {
    Decrypt$(data, D_{key})$}
Else
{
    Invalid file access of data
}
Else
{
    Invalid authentication
}
```

The goal of this dynamic key generation for decryption as well as encryption is to ensure that no client that has been invalidated may envisage or recognize the "unique secret key" to indirectly access the service. The results of the experiment along with the recommended method are described in the section below.

3.3 Data Encryption and Decryption

The proposed encryption and decryption mechanism for messages uses the IECDH algorithm. Within a secure channel, the IECDH algorithm is a completely homomorphic encryption technique. It includes a set of keys. One is a data encryption key as in algorithm 1, and the second is a decryption key for data decryption as in algorithm 2. Also, it uses a unique key from algorithm 3. Direct message sharing is derived from the encryption key, while decryption is derived from the decryption key. The keys generated as well as guaranteed among the channel's agreed-upon parties are used in subsequent data transactions.

The files are immediately encrypted for protection by the data owner before being stored in the cloud storage system. The $M$is the access structure of attributes, E_{key} data encryption key, along with M is the text message to be transferred, and that make up the IECDH encryption mechanism. The key generation parameter and the IECDH technique lower communication costs as well as overheads. The encryption procedure is shown in Equation (1).

$$CT = \left(A, E = E_{key}(M)\right) \tag{1}$$

the CTvariable is Cipher Text which is the encrypted data. It confirms that the encrypted data necessity have set correct characteristics and adhere to the access policy to be able to decode the query. The procedure makes the implicit assumption that CT has an access structure. With less data transmission and a higher level of security, an elliptic curve (EC) algorithm employs the session key negotiation function at both ends of a conversation. Compared to the EC method, the IECDH algorithm is more secure. IECDH uses shorter keys, uses less resources, and performs calculations quickly. The cloud data's encryption key is created with the aid of the IECDH technique.

During data retrieval the decryption process which is the reverse of encryption is done. In decryption the ciphertext is converted back to plain text with aid of D_{key}. The decryption happens only if the $E_{key}$is equal to D_{key}. If this condition is not satisfied then the user who is trying to access the data is not given access and is considered as unauthorized user. Only the user who satisfies the condition is only given data access. Finally, by this method the data is stored in the secure manner.This technique accomplishes encryption, decryption, and key generation while also offering the highest level of data security in the cloud. The next sections provide an experimental examination of the performance of the proposed IECDH and some approaches.

4. Results and Discussions

The experiment assessment technique along with knowledge used in the proposed approach are illustrated in this section.The Enron Email Dataset served as the source for the experimental data.

4.1 Dataset

This research work makes use of the Enron corpus database. Four tables make up the database, and the entities are employees, messages, recipients, and reference data. There are 158 users and 200,399 messages in the Enron Email dataset. To create an experimental dataset from the Enron emails, a few emails are chosen at random.

4.2 Discussion

Each set of input keywords was created at random by the user. The cloud server next does a database data search and extracts the pertinent qualified files. In this research, a number of criteria, encryption time, computational overhead, including key generation time, and decryption time, were utilized to assess the algorithm's efficacy.The development of the challenge, the creation of the proof, and the verification of the proof make up the auditing phase's computation overhead. The creation of private keys is what causes the computational overhead. Equation 2 illustrates the computation overhead.

$$Comp\ overhead\ = n(2\ exp\ exp\ + Mul + Hash\ ) \qquad (2)$$

where n stands for the blocks seen in standard files.While Mul denotes one multiplication action, exp denotes one exponentiation operation, and $Hash$ denotes one hash operation. When a user monitors any changes made to stored data blocks or files without user authentication, a challenge will be sent. The store will produce a proof message for a received challenge and send it to the user. It returns "success" in the case of "valid proof" and "failure" in all other cases.

Table 1. Comparison of Key Generation Time

Key length (bit)	Proposed (ms)	ECDH [5]	RSA [20]	MRSA [20]	AES -128 [21]
128	72	79	92	144	232
512	102	110	140	172	186
2048	757	781	2453	8125	8912

The key generation times for IECDH and other cryptographic techniques are shown in Table 1. When compared to previous approaches, the proposed IECDH algorithm generates keys in the shortest amount of time. The existing ECDH, RSA, modified RSA (MRSA), and Advanced Encryption Standard (AES) algorithms need the longest key generation times. The proposed IECDH approach offers a tiny encrypted key with minimal processing time and power requirements. As a result, the calculation time for the proposed approach is lower than the computation time for the present method for a 2048-bit key length, which is 757 ms.

Table 2. Comparison of Encryption Time

Key length (bit)	Proposed (ms)	ECDH [5]	RSA [20]	MRSA [20]	AES-128 [21]
128	10	12	49	205	287
512	11	19	93	1672	2654
2048	38	50	148	99891	9875

The decryption as well as encryption times of the input along with output data are shown in Tables 2 and 3, respectively. The performance of an existing as well as proposed approach is evaluated for several key lengths, such as 128, 512, and 2048 bits. The IECDH algorithm, which has been proposed, produces superior outcomes compared to the current approaches. With the proposed IECDH technique, encryption and decryption times are kept to a minimum. IECDH is a key exchange protocol that swiftly transfers keys between clients and servers. The existing approach, which relies on RSA, necessitates the use of a numerical key for encryption, which increases calculation time. The calculation time is shortened, and fewer encryption keys are generated by the proposed IECDH approach. For a key length of 2048, the newly proposed IECDH technique decrypts data in 89 milliseconds, as opposed to 53609 milliseconds for the existing approach. The use of fewer key creation processes significantly reduces calculation time. The IECDH also lessens the time it takes for information to reach the client from the server. Additionally, it is quicker than existing techniques like ECDH, RSA, MRSA, and AES-128.

Table 3. Comparison of Decryption Time

Key length (bit)	Proposed (ms)	ECDH [5]	RSA [20]	MRSA [20]	AES-128 [21]
128	25	31	188	122	109
512	53	63	218	968	1076
2048	89	109	15203	53609	52219

Table 4. Comparison of Computational Overhead

No. of blocks/ Proof Verification	Proposed	ECDH [5]	RSA [20]	MRSA [20]	AES-128 [21]
20	0.74	0.78	0.80	0.84	0.87
40	0.83	0.94	0.95	0.89	0.90
60	0.74	0.78	0.80	0.83	0.87
80	0.73	0.78	0.80	0.83	0.87

Table 4 shows how computation overheads behave in relation to different block sizes. The proposed proof verification is considered as the less when compared to the existing approaches. The key generated are taken in a less time and hence it reduces the computational overhead. In encryption time, terms of key generation, decryption time, and computational overhead, the proposed IECDH method performed better.

5. Conclusion and Future Work

Due to its capability to store vast amounts of data and enable flexible processing, the cloud computing paradigm has lately gained popularity. Many data owners outsource their data along with data analysis activities to the cloud in order to take advantage of these benefits. A data owner may want to encrypt data prior to outsourcing due to security concerns. The IECDH technique is utilized in this study to secure cloud data. The cloud storage is used to store user data that has been encrypted using an algorithm. Based on the user query, the decryption function is used to obtain the stored data. In comparison to previous methods, the proposed IECDH approach can handle data with larger key sizes more quickly. Using several evaluation measures, encryption time, including key generation time, processing overhead, and decryption time, the performance of the IECDH method is experimentally evaluated. The IECDH algorithm performs around 90% better than the currently used encryption techniques in terms of execution time. In the future, a mix of access control and encryption techniques may be taken into consideration to maintain the security along with privacy of huge amounts of data.

Acknowledgements

Acknowledgment The authors declare that they have no conflict of interest. The manuscript was written through contributions of all authors. All authors have given approval to the final version of the manuscript. The article has no research involving Human Participants and/or Animals. The author has no financial or proprietary interests in any material discussed in this article.

Author contributions

The manuscript was written through contributions of all authors. All authors have given approval to the final version of the manuscript. Conflicts of interest

Conflict of Interest

The authors declare no conflicts of interest.

References

[1] Lo'ai, A. Tawalbeh, and GokaySaldamli. "Reconsidering big data security and privacy in cloud and mobile cloud systems." *Journal of King Saud University-Computer and Information Sciences* 33, no. 7 (2021): 810-819.

[2] Ghayvat, Hemant, Sharnil Pandya, Pronaya Bhattacharya, Mohd Zuhair, Mamoon Rashid, Saqib Hakak, and Kapal Dev. "CP-BDHCA: Blockchain-based Confidentiality-Privacy preserving Big Data scheme for healthcare clouds and applications." *IEEE Journal of Biomedical and Health Informatics* 26, no. 5 (2021): 1937-1948.

[3] Sharma, Pratima, Malaya Dutta Borah, and SuyelNamasudra. "Improving security of medical big data by using Blockchain technology." *Computers & Electrical Engineering* 96 (2021): 107529.

[4] Deepa, Natarajan, Quoc-Viet Pham, Dinh C. Nguyen, Sweta Bhattacharya, B. Prabadevi, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, Fang Fang, and Pubudu N. Pathirana. "A survey on blockchain for big data: approaches, opportunities, and future directions." *Future Generation Computer Systems* (2022).

[5] Subramanian, E. K., and Latha Tamilselvan. "Elliptic curve Diffie–Hellman cryptosystem in big data cloud security." *Cluster Computing* 23 (2020): 3057-3067.

[6] Dhiman, Gaurav, Sapna Juneja, Hamidreza Mohafez, Ibrahim El-Bayoumy, Lokesh Kumar Sharma, Maryam Hadizadeh, Mohammad Aminul Islam, Wattana Viriyasitavat, and Mayeen Uddin

Khandaker. "Federated learning approach to protect healthcare data over big data scenario." *Sustainability* 14, no. 5 (2022): 2500.

[7] Koo, Jahoon, Giluk Kang, and Young-Gab Kim. "Security and privacy in big data life cycle: a survey and open challenges." *Sustainability* 12, no. 24 (2020): 10571.

[8] Awaysheh, Feras M., Mohammad N. Aladwan, MamounAlazab, Sadi Alawadi, José C. Cabaleiro, and Tomás F. Pena. "Security by design for big data frameworks over cloud computing." *IEEE Transactions on Engineering Management* 69, no. 6 (2021): 3676-3693.

[9] Chenthara, Shekha, Khandakar Ahmed, Hua Wang, and Frank Whittaker. "Security and privacy-preserving challenges of e-health solutions in cloud computing." *IEEE access* 7 (2019): 74361-74382.

[10] Khan, Mudassir, and Mohd Dilshad Ansari. "Security and privacy issue of big data over the cloud computing: a comprehensive analysis." *IJRTE-Scopus Indexed* 7, no. 6s (2019): 413-417.

[11] Rawat, Danda B., Ronald Doku, and Moses Garuba. "Cybersecurity in big data era: From securing big data to data-driven security." *IEEE Transactions on Services Computing* 14, no. 6 (2019): 2055-2072.

[12] Yadav, Dharminder, Dr Maheshwari, and Dr Chandra. "Big data hadoop: Security and privacy." In *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*. 2019.

[13] Tan, Liang, Na Shi, Caixia Yang, and Keping Yu. "A blockchain-based access control framework for cyber-physical-social system big data." *IEEE Access* 8 (2020): 77215-77226.

[14] Shahzad, Iqra, Ayesha Maqbool, Tauseef Rana, Alina Mirza, Wazir Zada Khan, Sung Won Kim, Yousaf Bin Zikria, and Sadia Din. "Blockchain-based green big data visualization: BGbV." *Complex & Intelligent Systems* 8, no. 5 (2022): 3707-3718.

[15] Hu, Xiaohan, Rong Jiang, Mingyue Shi, and Jingwei Shang. "A privacy protection model for health care big data based on trust evaluation access control in cloud service environment." *Journal of Intelligent & Fuzzy Systems* 38, no. 3 (2020): 3167-3178.

[16] Hasan, Mohammad Kamrul, Ali Alkhalifah, Shayla Islam, Nissrein BM Babiker, AKM Ahasan Habib, AzanaHafizah Mohd Aman, and Md Arif Hossain. "Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations." *Wireless Communications and Mobile Computing* 2022 (2022): 1-26.

[17] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, W. Xie, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing", IEEE Transactions on Information Forensics and Security, Vol. 11 (6), 2016.

[18] Y. Meng and Y. Meng, "A novel attribute-based signcryption scheme in cloud computing environments", In Proc. IEEE International Conference on Information and Automation, pp. 1976-1979, 2016.

[19] H. Hong, Y. Xia, Z. Sun, X. Liu, "Provably secure attribute-based signcryption with delegated computation and efficient key updating", KSII Transactions on Internet & Information Systems, vol. 11, no. 5, pp. 2646-2659, 2017.

[20] Anbuchelian, S., C. M. Sowmya, and C. Ramesh. "Efficient and secure auditing scheme for privacy preserving data storage in cloud." Cluster Computing 22 (2019): 9767-9775.

[21] R. Glenn S. Frankel and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", September 2003. http://tools.ietf.org/html/rfc3602.