IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906294 |

Attribute-Based Encryption for Secure and Efficient Data Collaboration in Cloud Computing

Miss. Dumbre Anita S[1], Prof. Monika D. Rokade[2]

PG Student, Department of Computer, SPCOE, Dumbarwadi (Otur) Pune, India

Assistant Professor (ME Co-coordinator), Department of Computer SPCOE, Dumbarwadi (Otur) Pune, India

ABSTRACT: Cloud computing plays a major role in sharing data and resources to other devices through data outsourcing. During sharing resources, it is a challenging task to provide access control and secure write operations. The main issue is to provide secure read and write operations collaboratively and to reduce computational overload by effective key management. In this paper, a secure and an efficient data collaboration scheme blowfish hybridized weighted attribute-based Encryption (BH-WABE) for secure data writing and proficient access control has been proposed. Here, weight is assigned to each attribute based on its importance and data are encrypted using access control policies. The cloud service provider stores the outsourced data and an attribute authority revokes or updates the attributes by assigning different attributes based on the weight. The receiver can access the data file corresponding to its weight in order to reduce the computational overload. The proposed BH-WABE provides collusion resistance, multiauthority security and fine-grained access control in terms of security, reliability, and efficiency. The performance is compared with the conventional hybrid attribute-based encryption (HABE) scheme in terms of data confidentiality, flexible access control, data collaboration, full delegation, partial decryption, verification, and partial signing.

KEYWORDS: cloud computing; secure write operation; data encryption; key management scheme;

I.INTRODUCTION

Attribute-based encryption (ABE) is a popular cryptographic technology to protect the security of users' data in cloud computing. Cloud computing is one of the biggest areas because of its high-level features such as convenience, scalability, and cost-saving. Due to its vulnerability, the development of the security model is very difficult. Consequently, the economic benefit and availability will be affected [1,2]. The attacker constructs the attacks in mobile application and devices in that place develop the hypervisor to destroy the virtual machine (VM) side-channel attack and denial-of-service (DOS) attack. Cloud computing will be affected by the presence of traffic, in which case IP addresses are used to eliminate the traffic [3]. The data collaboration service, as a promising service offered by the cloud service provider (CSP), is to support the availability and consistency of the shared data among users.

In cloud storage devices, data are stored among multiple users, not only in the cloud. A technique like privacy-preserving is used to allow public auditing through this way. The data will be stored, the integrity of shared data will be checked, and then the information will be verified by the ring structures. The shared data have a number of blocks containing the signer identity and the information are kept secret from third parties until the verification of shared information [4].

An organization has owners, and users can store data in the cloud and check the data for security purposes. In cloud computing systems, strong security obstacles and privacy issues are adapted in which related terms like confidentiality, integrity, control, audit, and availability are provided to secure the data [5]. In order to secure the stored data by the decentralized access control scheme in which the stored information can be decrypted by the valid users and the key distribution process by manner of decentralized way. All files or records will be stored in the cloud by access policy, which is known by the cloud [6]. The network security attackers are "viruses, trojan horses, man in the middle attacks, back doors, denials of service" and so on. In order to obtain flexibility and economic savings, the local sites are transformed to the commercial public cloud and it will be motivated by the data owners to outsource the complex data [7,8].

Before storing the information on the cloud, the cloud checks the authenticity of the user without the estimation of the

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906294 |

user's identity. The valid users can decrypt the stored data and then support modification, creation, and reading the data due to the prevention of replay attacks [9,10]. Monika Rokade and Yogesh Patil [11] proposed a system deep learning classification using nomaly detection from network dataset. The Recurrent Neural Network (RNN) has classification algorithm has used for detection and classifying the abnormal activities. The major benefit of system it can works on structured as well as unstructured imbalance dataset.

The MLIDS A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset has proposed by Monika Rokade and Dr. Yogesh Patil in [12]. The numerous soft computing and machine learning classification algorithms have been used for detection the malicious activity from network dataset. The system depicts around 95% accuracy ok KDDCUP and NSLKDD dataset.
Monika D. Rokade and Yogesh Kumar Sharma [13] proposed a system to identification of Malicious Activity for Network Packet using Deep Learning. 6 standard dataset has sued for detection of malicious attacks with minimum three machine learning algorithms.

Sunil S. Khatal and Yogesh kumar Sharma [14] proposed a system Health Care Patient Monitoring using IoT and Machine Learning for detection of heart and chronic diseases of human body. The IoT environment has used for collection of real data while machine learning technique has used for classification those data, as it normal or abnormal. Data Hiding In Audio-Video Using Anti Forensics Technique For Authentication has proposed by Sunil S.Khatal and Yogesh kumar Sharma [15]. This is a secure data hiding approach for hide the text data into video as well as image. Once sender hide data into specific objects while receivers does same operation for authentication. The major benefit of this system can eliminate zero day attacks in untrusted environments.

Sunil S.Khatal and Yogesh Kumar Sharma [16] proposed a system to analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. This is the analytical based system to detection and prediction of heart disease from IoT dataset. This system can able to detect the disease and predict accordingly.

The encrypted data are increased to introduce a large number of keywords and the trapdoor generation algorithm is used to solve the out of order problem without loss of data [18].

The personal data are kept secret in the cloud to protect sensitive data and remove the constraints. The data owner encrypts the data that will be outsourced to the cloud by the fine grained-access control. Between users and the cloud, the information will be leaked during the collusion time and it can be avoided by the safety data sheet (SDS) frame [19,20]. The similarity index is proposed to protect the data from insecurity and the m-index is encrypted to support the neighbor's queries. The key policy attribute based signature (KP-ABS) scheme composes the signer's private key into two components. The other users cannot forge the signature [21,22].

In this proposed work, blowfish hybridized weighted attribute-based encryption (BH-WABE) algorithm is developed for securing the data stored in the cloud. An attribute encryption scheme with more authority is more suitable for data access control cloud storage systems because the user can be held by multiple institutions to manage property, and access to policy data owners to use the property that may be defined in different institutions. Traditional single authority to manage all user attributes dense steel, easy to degrade system performance. In addition, a single authority solution requires a completely honest authorized body; it is difficult to meet the security requirements of cloud computing environments. Weighted attribute-based encryption is hybridized with the blowfish algorithm for encryption purposes. Encryption, key generation, and decryption are ensured with the blowfish algorithm.

II.LITERATURE SURVEY

Mobile devices, such as smartphones, which have been widely used by people to upload and download files, such as audio and video, also limit the sources in mobile devices. The cloud collects the files but the server does not have an idea about cloud security. Between users and the cloud, the data have been secured by classical access and provided lightweight security when the mobile accessing capacity of users became low. The watermarking scheme was developed by Wang et al. [23] in order to secure data between the cloud and users by authentication. The transmission errors could be minimized by combination of Reed–Solomon code with water marking.

In cryptographic techniques, the check ability was important and the versatility of access control had been enlarged by ABE method proposed by Li et al. [24]. The computational complexity, key issues, and decryption process were high in ABE method due to its high expensiveness. The constant efficiency was obtained by the user-

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906294 |

and authority-side. To get the clear solution, the computing task had to send the third party and address the verifiable results by the third party.

The necessary resources like authentication and access control for computation of cloud control and integration management. The practical solutions were not suggested by role-based access control (RBAC) and context aware RBAC to the clients, which was based on dynamic access control. The new model, ontology based access model control (Onto-ACM), was used to address the limitation of cloud computing suggested by Choi et al. [25].

A process such as resource virtualization, global replication, and migration assured quality of service by the computing paradigm. The cloud storage data had cloud users hopeful, but the clear computing results were not obtained. The computation auditing secure protocol was proposed by Wei et al. [26] to secure storage and the process was completed with the batch verification, the signature verified by the designator, and sampling technique through this size was optimized and cost was minimized. The effectiveness and efficiency were clearly obtained from the experimental results.

The novel patient-centric framework had been proposed by Li et al. [27] to store personal records and access the data. The personal health record (PHR) files of each patient had been encrypted. Through this, clear and scalable data had been obtained, but it will be differed from the outsourcing of secure data by attribute-based encryption techniques. The multiple security domains degrade the complexity of key management due to the PHR system division by the scenario of multiple data. The security, scalability, and efficiency were enabled by break glass and access policy.

Subashini and Kavitha [28] presented a detailed survey regarding security issues in service delivery models in cloud computing and they discussed each method, along with their pros and cons.

III.PROPOSED SYSTEM DESIGN

Hierarchical Attribute-Based Encryption

By merging the features of ciphertext-policy-attribute-based encryption (CP-ABE) and hierarchical identity-based encryption (HIBE), one can derive hierarchical attribute-based encryption (HABE). Further, this scheme deals for fine-grained access control and scalability and also achieves full delegation by yielding key delegation between attribute authorities. Compared to the conventional schemes, this scheme symbolically represents the hierarchical structure of the enterprise, which is more appropriate to the environment of an organization outsourcing data in a cloud.

CP-ABE: It is an inverted model of key policy-attribute-based encryption (KP-ABE) that enables the data holder to explain the access strategy over the whole attributes that the data consumer wants to retain with the intention of decrypting the ciphertext. By doing so, confidentiality and data access control can be assured.

The CP-ABE algorithm involves four steps and it is represented below.

(1) **Setup ()**: This is a randomized part and it accepts only the unstated security parameter. Consequently, it yields the public key P_K and the master key M_K.

(2) **Encrypt** (P_K, S_a, m): This step fetches P_K, a message m and the descriptive attribute S_a as input. It outputs a cipher text C_T. 3).

(3) **Keygen** (M_K, AS): This step takes M_K and non-monotonic access structure AS as input and provides attribute secret key S_K for users as output.

(4) **Decrypt** (C_T, S_K): The input in this step is cipher text C_T, which contains the access tree T and the user's secret key S_K that is related to their descriptive attribute S_a, and the output is message m. This step is completed only if S_a satisfies T.

The access structure of CP-ABE is attached with the cipher text until the key for decryption process is interpreted with the pack of descriptive attributes as shown above. Consequently, the responsibility of KP-ABE is to change the characters of the cipher text and the decryption key. Furthermore, in this system, encryption provides the monotonic access form along with a threshold value for appropriate attributes. However, when the decryption key attributes fulfill the access policy in a known ciphertext, then only the ciphertext can be decrypted with the key. This method is more enthusiastic though the trusted server is negotiated. Generally, the CP-ABE approach is greater than the KP-ABE in terms of imposing encrypted data's access control. The major constraints of CP-ABE are that it cannot fulfill the necessities of initiatives in their access control as it requires efficiency and flexibility.

HIBE: The hybrid identity-based encryption (HIBE) is extended from IBE. Here, the private key is delivered by a solo private key generator (PKG) with the public keys as their primitive ID (PID), so-called as 1-HIBE in an

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906294 |

overall identity-based encryption scheme and carry a drawback like heavy key managing. Therefore, to overcome this, a 2-HIBE scheme via a detailed definition of security is introduced that consists of domain PKG and a root PKG. The consumers and these are connected with a random string of PID. However, the domain PKG produces the private key to provide the requested domain secret key, which is acquired from the root PKG. Moreover, a root certificate authority (trustworthy third party) is involved by the cryptosystem, which permits a hierarchy of certificates. Through several levels of HIBE, the allotment of key escrow and root server workloads can be diminished.

IV.PROPOSED BLOWFISH HYBRIDIZED WEIGHT ATTRIBUTE-BASED ENCRYPTION

In cloud computing, a secure and efficient data collaboration is achieved by the proposed BH-WABE approach. Most of the conventional ABE methods only have a single authority to handle both the secret and public keys. However, in many circumstances, the consumers hold attributes from multiauthority, and the data holders share data with consumers who are managed by a distinct authority. Many different multiauthority attribute-based access control structures have been developed to solve this problem. In access control systems with the intention of updating the ciphertext, a data holder has presented online for all time, besides the attributes that are given similar status. In the proposed scheme, the weighing of attributes is given by the blowfish algorithm to provide secure data in cloud computing.

The system involved five basic things: (a) the data holder, who encodes the data before uploading the data to the cloud under an access control policy; (b) a cloud server who provides data storing;
(c) a weight attribute authority (WAA) to authorize, update and validate the attributes of users that are assigning different weights with respect to their prominence; (d) a Central Authority (CA), which allocates a global user identifier for each consumer as well as allots user public key to the WAA; and (e) the data consumers, as illustrated in Figure1. In the proposed system, a blowfish algorithm is hybridized with weighted attributed authority as illustrated in Figure1.

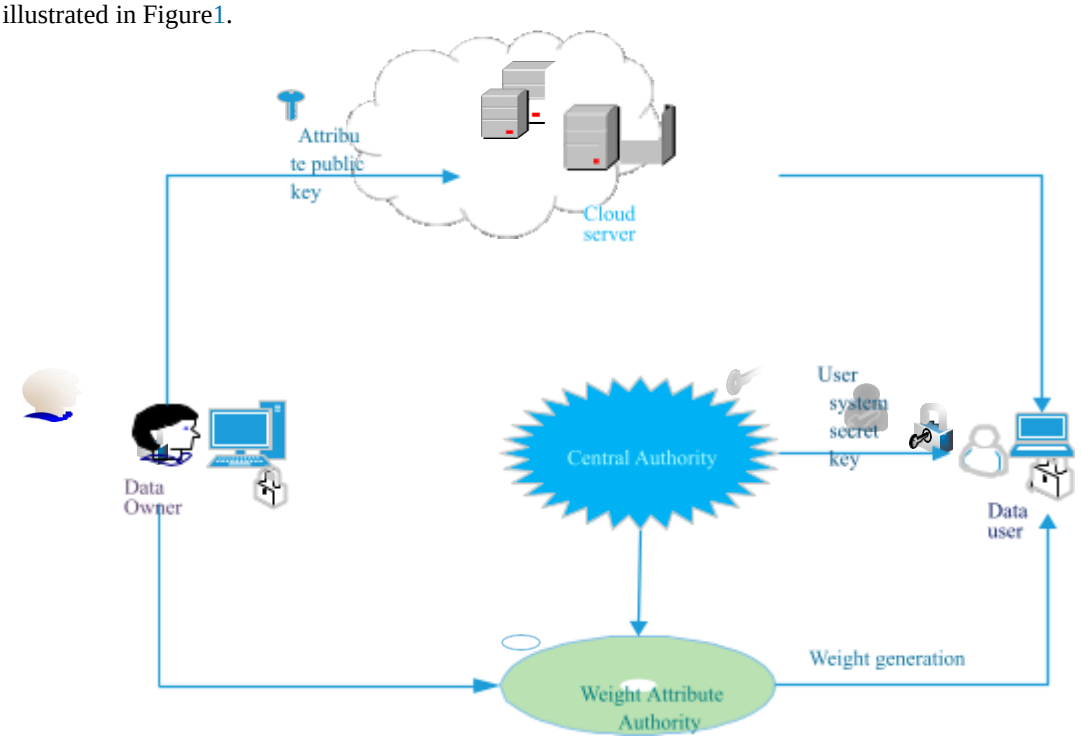

Figure 1. Proposed blowfish hybridized weighted attribute-based Encryption (BH-WABE) scheme.

In the proposed BH-WABE system model, the blowfish algorithm is applied to encrypt and decrypt data and to generate keys randomly. Moreover, an image-matching technique is employed for security purposes. Subsequently, the system generates weight value for users based on its attributes. For example, if User A = Dhoni from the HR department and User B = Sachin from the R&D department, both users initially encounter the security phase. Assuming that the system acknowledges that User A is valid, then the system generates weight values for User A based on its attributes. According to the weight value, User A can decrypt the document, which is assigned to its

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906294 |

corresponding weight. In contrast, User B cannot decrypt the document of User A. Though User B is a valid user, their weight rate does not match the weight rate of User A, but User B can decrypt its corresponding document based on its weight value. This approach is more prominent, reliable, and secure; besides, it is more applicable for real-time applications than the conventional methods in a cloud computing environment. BH-WABE encryption deals fine-grained access control, multiauthority security, and collusion resistance. The proposed scheme is represented in two phases: the algorithm phase and the system phase. At the algorithm phase, the blowfish algorithm is described along with system-level operations. Conversely, at system level, the high-level operations such as System Setup, User Annulment, New File Creation, New User admit, File Access and Deletion are explained.

Algorithm Level Operations

Blowfish Algorithm

Blowfish is a symmetric encryption algorithm [29]. It consists of a single key that is used for both encryption and decryption process. This blowfish encryption scheme's secret key ranges from 32 to 448 bits. If the range of key is 448 bits, then it needs 2448 groupings to define all the entire keys. Furthermore, this key has a fixed 64-bit block size with variable-length key block cipher. The cipher is a 16-round Feistel network, which uses password-dependent S-boxes to develop the structure by which the encryption and decryption process has taken place. This cipher divides messages into 64 bits blocks and then encrypts them separately.

The algorithm possesses two main sub-key groups, namely, the 18-entry P-boxes (permutation boxes) to perform bit-shuffling and four 256-entry S-boxes (substitution boxes) to perform simple nonlinear functions. Here, the S-boxes receive 8-bit as input and yield 32-bit output. The working principle of a single blowfish round is shown in Figure2. The function F is the Feistel Function of Blowfish that splits half the 32-bit block in 8-bit chunks (quarters) and employs this quarter as input to the S-box. Subsequently, the outcomes of S-boxes are supplemented with the dropped carry, consequential in MOD 232 addition, and finally XOR operation has been performed. Conversely, the decryption process has been carried out by reversing the blowfish algorithm and is simply done by inverting P_{17} and P_{18} cipher blocks as well as by employing the P-entries in reverse order. Blowfish algorithm is generally divided into two sections, namely key-expansion and data encryption.

Key-expansion: In the Key expansion part, a 448-bit key is converted into numerous sub-key groups of 4168 bytes in aggregate. Normally, P-array is composed of 18 and 32-bit sub-keys (P_1, P_2, P_{18}) and four 32-bit S-Boxes, each containing 256 entries.

The procedures that involved in the key expansion process are given as follows:

Step 1: Set and Initialize S-box and P-box with values from the hexadecimal numbers of pi (<initial 3)

Step 2: The variable length of the user input key is XOR[ed] with the P-entries until the entire P-array has been XOR[ed] with input key bits.

Step 3: A block of zeroes is encrypted; subsequently the results are applied for P_1 and P_2 entries. Step 4:Again, encrypt the ciphertext obtained from the encrypted zero block, then utilize for P_3 and P_4. Step 5:Continue the process till each P-box entry and the S-box entry have been exchanged thus; totally,

521 iterations are necessary to generate all the essential sub-keys (i.e., 521 key generations).

V.CONCLUSIONS

In a cloud environment, user authentication and data security are the challenging issues. Therefore, an efficient and scalable access control scheme has been proposed in this paper. Further, this scheme employs a blowfish hybridized weight attribute-based encryption mechanism not only to provide data security against the semi-trusted cloud service provider, but also the weight attribute authority and the central authority provides lightweight key management in large scale-consumers. Besides, the partial signing construction implemented in this scheme can reduce the computation overhead of user to the cloud server, which is efficient and appropriate for resource-constrained devices. Here, blowfish encryption and decryption algorithms are used to transmit data securely. When the authenticated user makes a request to the cloud, the corresponding files are sent to the consumer in an encrypted format based on its weight. Subsequently, the data consumer can decrypt the data using the key generated by the blowfish algorithm. The result shows that the proposed method BH-WABE is efficient in terms of security, reliability, and efficiency, as well as performing well when it is juxtaposed to the conventional HABE scheme by means of data confidentiality, flexible access control, data collaboration, full delegation, partial decryption, verification, and partial signing.

The future extent of the proposed work can be accessible, quality-based encryption and protection-saving property-based information-sharing with re-encryption. These are territories in which we can look into going ahead

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906294 |

to use diverse methods to accomplish information-sharing.

REFERENCES

1. Modi, C.; Patel, D.; Borisaniya, B.; Patel, A.; Rajarajan, M. A survey on security issues and solutions at different layers of Cloud computing. J. Supercomput. **2013**, 63, 561–592
2. Singh, S.; Young-Sik, J.; Park, J.H. A survey on cloud computing security: Issues, threats, and solutions. J. Netw. Comput. Appl. **2016**, 75, 200–222.
3. Yan, Q.; Yu, F.R. Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Commun. Mag. **2015**, 53, 52–59.
4. Ranchal, R.; Bhargava, B.; Othmane, L.B.; Lilien, L.; Kim, A.; Kang, M. An Approach for Preserving Privacy and Protecting Personally Identifiable Information in Cloudcomputing.
5. Zhou, M.; Zhang, R.; Xie, W.; Qian, W.; Zhou, A. Security and privacy in cloud computing: A Survey. In Proceedings of the Sixth International Conference on Semantics Knowledge and Grid (SKG), Washington, DC, USA, 1–3 November 2010; pp. 105–11
6. Ruj, S.; Stojmenovic, M.; Nayak, A. Decentralized access control with anonymous authentication of data stored in clouds. IEEE Trans. Parallel Distrib. Syst. **2014**, 25, 384–3
7. Younis, Y.A.; Kifayat, K.; Merabti, M. An access control model for cloud computing. J. Secur. Appl. **2014**, 19, 45–60.
8. Cao, N.; Wang, C.; Li, M.; Ren, K.; Lou, W. Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Trans. Parallel Distrib. Syst. **2014**, 25, 222–233.
9. Lacuesta, R.; Lloret, J.; Garcia, M.; Peñalver, L. Two secure and energy-saving spontaneous ad-hoc protocol for wireless mesh client networks. J. Netw. Comput. Appl. **2011**, 34, 492–505.
10. Ruj, S.; Stojmenovic, M.; Nayak, A. Privacy preserving access control with authentication for securing data in clouds. In Proceedings of the 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Ottawa, ON, Canada, 13–16 May 2012; pp. 556–563.
11. Monika D.Rokade ,Dr.Yogesh kumar Sharma,"Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic." IOSR Journal of Engineering (IOSR JEN), ISSN (e): 2250-3021, ISSN (p): 2278-8719
12. Monika D.Rokade ,Dr.Yogesh kumar Sharma"MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset", 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE
13. Monika D.Rokade, Dr. Yogesh Kumar Sharma. (2020). Identification of Malicious Activity for Network Packet using Deep Learning. *International Journal of Advanced Science and Technology*, *29*(9s), 2324 - 2331.
14. Sunil S.Khatal ,Dr.Yogesh kumar Sharma, "Health Care Patient Monitoring using IoT and Machine Learning.", **IOSR Journal of Engineering (IOSR JEN),** ISSN (e): 2250-3021, ISSN (p): 2278-8719
15. Sunil S.Khatal ,Dr.Yogesh kumar Sharma, "Data Hiding In Audio-Video Using Anti Forensics Technique ForAuthentication ", IJSRDV4I50349, Volume : 4, Issue : 5
16. Sunil S.Khatal Dr. Yogesh Kumar Sharma. (2020). Analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. *International Journal of Advanced Science and Technology*, *29*(9s), 2340 - 2346.
17. Li, J.; Chen, X.; Huang, Q.; Wong, D.S. Digital provenance: Enabling secure data forensics in cloud computing. Future Gener. Comput. Syst. **2011**, 37, 259–266.
18. Xu, Z.; Kang, W.; Li, R.; Yow, K.; Xu, C.Z. Efficient multi-keyword ranked query on encrypted data in the cloud. In Proceedings of the 2012 IEEE 18th International Conference on Parallel and Distributed Systems, Singapore, 17–19 December 2012; pp. 244–251.
19. King, N.J.; Raja, V.T. Protecting the privacy and security of sensitive customer data in the cloud. Comput. Law Secur. Rev. **2012**, 28, 308–319.
20. Samanthula, B.K.; Elmehdwi, Y.; Howser, G.; Madria, S. A secure data sharing and query processing framework via federation of cloud computing. Inf. Syst. **2015**, 48, 196–212.
21. Kozak, S.; Novak, D.; Zezula, P. Secure metric-based index for similarity cloud. In Proceedings of the Workshop on Secure Data Management, Istanbul, Turkey, 27 August 2012; pp. 130–147.
22. Hong, H.; Sun, Z. An efficient and traceable KP-ABS scheme with untrusted attribute authority in cloud computing. J. Cloud Comput. **2016**, 5, 1–8.
23. Wang, H.; Wu, S.; Chen, M.; Wang, W. Security protection between users and the mobile media cloud. IEEE Commun. Mag. **2014**, 52, 73–79.
24. Li, J.; Huang, X.; Chen, X.; Xiang, Y. Securely outsourcing attribute-based encryption with checkability.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 6, June 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0906294 |

IEEE Trans. Parallel Distrib. Syst. **2014**, 25, 2201–2210.

25. Choi, C.; Choi, J.; Kim, P. Ontology-based access control model for security policy reasoning in cloud computing. J. Supercomput. **2014**, 67, 711–722.
26. Wei, L.; Zhu, H.; Cao, Z.; Dong, X.; Jia, W.; Chen, Y.; Vasilakos, A.V. Security and privacy for storage and computation in cloud computing. Inf. Sci. **2014**, 258, 371–386.
27. Li, M.; Yu, S.; Zheng, Y.; Ren, K.; Lou, W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans. Parallel Distrib. Syst. **2013**, 24, 131–143.
28. Subashini, S.; Kavitha, K. A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. **2011**, 34, 1–11. [CrossRef]
29. Mousa, A. Data encryption performance based on Blowfish. In Proceedings of the 47th International Symposium ELMAR, 2005, Zadar, Croatia, 8–10 June 2015; pp. 131–134.
30. Huang, Q.; Yang, Y.; Shen, M. Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing. Future Gener. Comput. Syst. **2017**, 72, 239–249. [CrossRef]

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details