International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7462
***Article Received**: 22 May 2023 **Revised:** 13 July 2023 **Accepted:** 03 August 2023*

A Hybrid Multi-user Cloud Access Control based Block Chain Framework for Privacy Preserving Distributed Databases

Ch. Nanda Krishna[1], Dr.K.F. Bharati[2]
[1]Research Scholar, Department of Computer Science and Engineering
JNTUA
Anantapur, India
chnk1789@gmail.com
[2]Associate Professor, Department of Computer Science and Engineering
JNTUACEA
Anantapur, India
kfbharathi@gmail.com

Abstract— Most of the traditional medical applications are insecure and difficult to compute the data integrity with variable hash size. Traditional medical data security systems are insecure and it depend on static parameters for data security. Also, distributed based cloud storage systems are independent of integrity computational and data security due to unstructured data and computational memory. As the size of the data and its dimensions are increasing in the public and private cloud servers, it is difficult to provide the machine learning based privacy preserving in cloud computing environment. Block-chain technology plays a vital role for large cloud databases. Most of the conventional block-chain frameworks are based on the existing integrity and confidentiality models. Also, these models are based on the data size and file format. In this model, a novel integrity verification and encryption framework is designed and implemented in cloud environment. In order to overcome these problems in the cloud computing environment, a hybrid integrity and security-based block-chain framework is designed and implemented on the large distributed databases. In this framework,a novel decision tree classifier is used along with non-linear mathematical hash algorithm and advanced attribute-based encryption models are used to improve the privacy of multiple users on the large cloud datasets. Experimental results proved that the proposed advanced privacy preserving based block-chain technology has better efficiency than the traditional block-chain based privacy preserving systems on large distributed databases.

Keywords- Machine learning, privacy preserving, block chain, cloud computing.

I. INTRODUCTION

Cloud computing provides a cost-effective alternative for the IT infrastructure's scalability and adaptability. Cloud providers transmit users' programs, software, and databases to massive data centers globally, and consumers cannot directly control the remote data, introducing various new security challenges [1]. Cryptography systems that rely on unproven computational limits and mathematical approaches are typically implemented through insecure channels for applications involving secret message exchanges. The key distribution problem poses the greatest difficulty in traditional cryptographic techniques. Cloud computing offers large storage space and quick computing services to consumers via the internet. However, when data owners send their data to the cloud, there are privacy concerns as the outsourced data can contain sensitive information that must be protected. To address these privacy concerns, this paper introduces a searchable encryption technique that enables basic search operations on encrypted cloud data. The data owner is responsible for encrypting all documents and keywords before uploading them to the cloud. The encrypted documents and keywords are stored on the cloud, and the searchable encryption technique generates the encrypted trapdoor for multiple keywords. This trapdoor allows the data owner to search for encrypted keywords without revealing their actual contents, ensuring the privacy and security of the sensitive information stored on the cloud. The searchable encryption technique is designed to provide a secure solution for data owners who want to store and search for their sensitive information on the cloud while maintaining their privacy. This solution is based on cryptographic techniques and aims to provide a secure and efficient way to search encrypted data in the cloud environment. A block chain is the technology allowing all members to maintain a book containing all transaction data and to update their booklets in a new transaction, in order to maintain integrity. Safety in the cloud computing environment is primarily examined for the save and transfer of data such as privacy and integrity. Note, however,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7462
***Article Received**: 22 May 2023 **Revised:** 13 July 2023 **Accepted:** 03 August 2023*

that privacy and anonymity studies are not enough. A representative anonymity technology is the block chain. If combined with the cloud computing environment, the block chain can be upgraded to a comfortable and more secure service. User anonymity can be ensured if the block chain method is used in the cloud computing environment for saving user information. When using block chain technology, an electronic wallet is installed. If you don't correctly remove your electronic wallet, the user data may be left behind. The rest of the user data can be used for the evaluation of user information. The KP-ABE system offers a variety of features that align with multiple access structures [5]. On the other hand, CP-ABE is a specialized access structure that aligns with several attribute sets and is favored in various access control scenarios. Both KP-ABE and CP-ABE approaches are suitable for use in the keyword search process. Customers can choose their payment method based on their needs. Cloud computing provides clients with a range of services by reorganizing resources according to their requirements. It reduces the users' workload by managing multiple information systems. The users must outsource their data to a heterogeneous cloud environment, which may not be controlled by the customer [6]. With the growth of IoT, vast amounts of data are produced and transmitted, and data processing, analytics, and data mining help parties benefit from their data and others' data. Cloud computing allows users to access internet services from anywhere and at any time without having to worry about the technological or physical maintenance and management of the original capital. However, some still find the concept of cloud computing technology abstract, and it is essential to understand the elements that can impact its acceptance across different enterprises. Cloud computing is becoming a critical component of long-term IT strategies for many businesses, offering lower costs and reducing time-consuming efforts. It allows firms from any location to access cloud-based services and improves inter-organizational communication. However, businesses have been reluctant to use cloud computing due to privacy and security concerns. The benefits of cloud computing extend not only to consumers but also to businesses, governments, and private institutions. To enhance cloud adoption and performance, it is crucial to assess security issues comprehensively. Cloud computing provides consumers with vast storage space and fast computing over the internet. However, privacy concerns arise as the data being outsourced to the cloud often contains sensitive information that needs to be encrypted before submission to ensure its protection. To address this issue, searchable encryption techniques are used to perform basic search operations on encrypted cloud data. Before uploading, the data owner encrypts all documents and their associated keywords, while the search approach generates the encrypted trapdoor of multiple keywords. Despite the convenience of accessing data anytime and anywhere through cloud servers, users are still worried about losing control over their outsourced data. This is why data integrity in cloud computing is essential. Data integrity involves ensuring the accuracy of remote data stored on unsecured cloud servers, and a protocol is used to establish ownership of the data to prevent any unauthorized changes. This authentication system ensures that the data stored by the user remains unchanged, thus maintaining its quality [3-6].Medical data outsourcing to the cloud can benefit healthcare systems, clinicians, and patients by managing critical information across multiple branch hospitals while reducing the hospital's computing resources. However, traditional integrity verification algorithms for cloud networks are vulnerable to attacks and collisions and may not be effective for handling large amounts of data. Numerous research papers have been published on cryptographic integrity features to verify communication data in cloud networks. To authenticate each cloud client in the cloud network, traditional authentication models have been proposed. However, these approaches are impractical and time-consuming for large cloud networks, and they have limitations such as limited data capacity, difficulty in generating variable-size integrity values, and difficulty in generating dynamic hash values on large wireless networks.

II. RELATED WORKS

The public space complexity is equivalent to hierarchy saving, private class information is linked with a single key, changes are processed locally and hierarchically, the system strongly resists collusion, and each node derives its descendant's key. To reduce the distance between nodes and hasten key generation, a minimizing strategy is employed. As an alternative method to secure data, two layers of encryption are implemented to ensure the protection of sensitive information. The first layer of encryption is imposed by the data owner while the server enforces the second layer, which can be modified as per policies. This approach is both reliable and robust, considering the changes in policies and ensuring the confidentiality of information while also detecting any potential risks of collusion. The data security technique outlined in [7-9] focuses on two main aspects of management: initializing the Multicast Group with a shared network key and rekeying the group. It plays a crucial role in key management for the multicast system and provides secure recovery of compromised systems while also resisting user collusion. The method optimizes transmission while minimizing the storage required for the group. When addressing the resource allocation problem in the cloud, it is important to identify both available resources and assigned assets. To protect information from cloud path planning in restricted cloud networks, Weiet.al introduced a cryptographic technique called the CP-ABE model, which

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7462
***Article Received**: 22 May 2023 **Revised:** 13 July 2023 **Accepted:** 03 August 2023*

focuses on the concept of cypher text and access control mechanisms, including concealed keys. The decryption method is only allowed if the properties meet the desired access strategy [10-11]. The CP-ABE model operates differently from the KP-ABE model and is more flexible, making it easily implementable in various applications. The KP-ABE technique struggles with managing who can decrypt the ciphertext, which is its primary limitation. CP-ABE tried to solve this issue using the KP-ABE method and as a result, it can be efficiently implemented in various real-world applications. However, the KP-ABE model still has a significant drawback that restricts its use in business contexts, as it has a less flexible nature and poor efficiency. To execute successful decryption, users must choose a single set of attributes from the available options. The issue of the CP-ABE method has been subject to further research, with CP-ASBE (Cipher Text Policy Attribute Set Based Encryption) being recognized as the ideal solution [12-15].

Cloud Service Providers (CSPs) use encryption to secure the data stored in the cloud, but the security of the key remains a potential weakness. Some cloud services, like Apple's "iMessage," hold a backup of the encryption key and keep it hidden from their clients, giving them the potential to theoretically access all the data stored on their servers. To ensure end-to-end encryption for messages, we do not inform clients that they are legally allowed to possess a copy of the key. CSPs control the keys, allowing customers to trust them completely. Some research suggests that customers encrypt the data before storing it in the cloud to secure sensitive and secret data. However, this solution requires a reliable key management solution, or the data could be lost forever. A robust cryptographic technique is needed to secure data storage and processing, with requirements such as a reasonable processing time, a minimum size for encrypted data, and the ability to perform remote calculations without decrypting. The proposed solution is to use a Homomorphic Encryption-based cryptosystem that allows encrypted data to be computed without decryption. This technique eliminates the need to provide the cloud provider with the encryption key. However, the fully homomorphic encryption proposed operates slowly, requiring more processing time and memory than unencrypted data operations. A parallel processing of Gentry's encryption has been proposed to improve performance, dividing FHE encrypted data operations across many processing engines. Many cloud environments do not encrypt their data, storing it in plain text on the disc, exposing secret information to potential employees or unauthorized users. High availability of infrastructure, data, and applications is a significant factor in choosing between private, public, and hybrid cloud service providers and delivery types. Enterprises should stress the provision of information in the service level agreement to ensure access to their data. Attacks such as the Malware Injection Attack, in which a hacker injects destructive code into transmitted data, and Distributed Denial of Service (DDoS) attacks, which deprive genuine users and partners of services and resources, can impair the availability of data and negatively impact business operations. To reduce this risk and provide resistance to the failure or misuse of sensitive data, various strategies employing the "cloud of clouds," "interclouds," or "multi-cloud" approach have been proposed[16-18].A Multi Cloud Solution creates a virtual cloud storage network using multiple commercial cloud storage services by dividing data into blocks and distributing it to various cloud storage providers. There are two methods of ensuring redundancy: storing a complete copy of a file on each provider or dispersing properly encoded data in a way that only a certain fragment of a file is needed to reconstruct it. Cloud service companies benefit from utilizing consumer data, but the most significant obstacles to cloud adoption are protection and privacy. When data is sent to and from a cloud provider's data center in encrypted form, the computers controlling the cloud cannot perform operations on it, so businesses must exchange the secret decryption key to perform calculations on the stored data. Homomorphic encryption solves this problem by allowing the client to receive executable code from the cloud, perform calculations on encrypted data, and return encrypted results. Since 2008, cloud computing has evolved from various technologies and has been implemented in many solutions and services, leading to the development of innovative cloud computing systems. The literature review examines all relevant research publications and discusses methods for user revocation in cloud storage. IoT satisfies business requirements by linking the real and virtual worlds, but it also raises privacy concerns. Blockchain technology offers a solution by ensuring the security of IoT from malicious attacks and fraud through decentralization, durability, immutability, and irreversibility.

Public-private key networks in blockchain technology offer enhanced security for users by allowing access to the network only with a private key, which is a password for the public key, a long randomly generated number string that represents the user's address on the network. The majority of merchant bankers, including Goldman Sachs, believe that blockchains will have a bright future in the banking system and result in significant cost savings. Blockchain technology has also inspired the creation of value through the authentication of digital knowledge, such as the Aadhar card issued by the Indian Unique Identification Authority. Smart contracts are another example of how blockchain technology is rapidly gaining ground in the corporate world. These digitally signed contracts are automatically implemented when their terms are met and facilitate the representation of agreements in a way that eliminates the need for physical interaction between parties [16-23].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7462
***Article Received**: 22 May 2023 **Revised:** 13 July 2023 **Accepted:** 03 August 2023*

III. PROPOSED MODEL

In the proposed model, privacy preserving using block chain security framework is designed and implemented on the distributed applications in order to provide strong security against the third-party attacks. The overall framework of the proposed model is represented in figure 1.

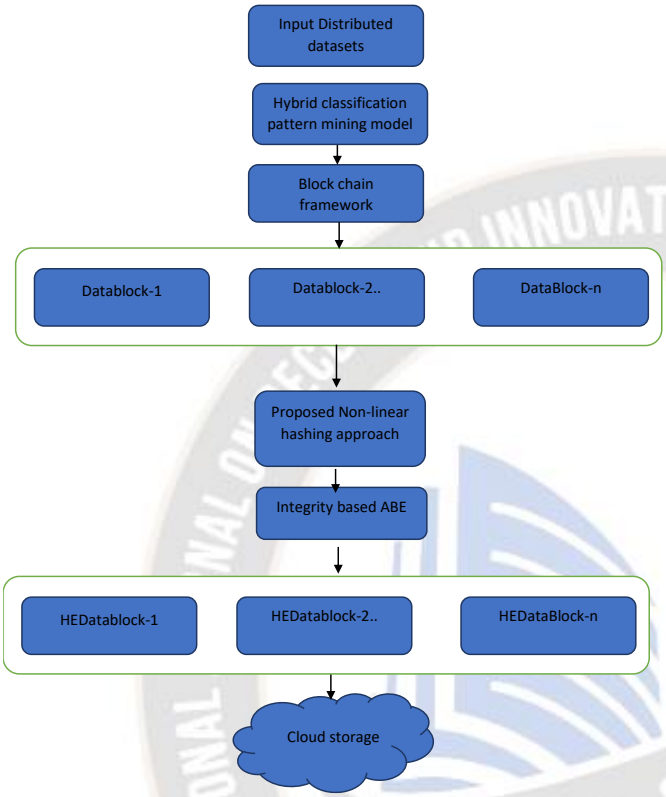

Figure 1. Overall Proposed Framework

The block chain framework in Figure 1 submits each medical dataset transaction for block security. The initial proposal proposes a hybrid classification model to uncover hidden patterns in remote databases. Security blocks compute the hash and encryption of the input transaction for added security. The framework encodes the current block hash and previous block hash data. The algorithm explores the generalization lattice in a bottom-up, breadth-first manner and generates paths based on a stable strategy that avoids the challenges of a vertical traversal while its execution time may vary depending on the input dataset representation. The algorithm scrutinizes all modifications for optimal performance and numerous optimizations. Each transaction's encoded data is saved on a cloud server for verification of its integrity. The proposed study implements a hybrid non-linear chaotic integrity-based encryption model on real-time distributed transactions for the block chain framework.

Algorithm 1: Proposed Geometric Privacy Preserving data Mining Approach

Input: dataset D

Output: Privacy enabled dataset D'

1. Attribute Categorization: The attributes in the given dataset are separated into four categories: Identifiers, Quasi Identifiers, Sensitive Attributes, and Insensitive Attributes.
2. Identifier Removal: The Identifiers are removed from the dataset.
3. Quasi Identifier Identification: The Quasi Identifiers are identified within the dataset.
4. Numerical Quasi Identifier Anonymization: To anonymize the numerical Quasi Identifiers, a geometric data perturbation is applied to generate an intermediate dataset, Dm. Multi-user attribute encoding using algorithm 2 is then performed.
5. Categorical Quasi Identifier Anonymization: A k-anonymization technique is utilized to anonymize the categorical Quasi Identifiers within dataset Dm. Multi-user attribute encoding using algorithm 2 is then performed.
6. Privacy-Protected Dataset Creation: The privacy-protected dataset, D'm, is generated by applying the k-anonymization algorithm to dataset Dm.
7. Original Dataset Anonymization: The same k-anonymization process is applied to the original dataset, D, to produce the anonymized dataset, D'k.
8. Classification Method Comparison: Both datasets D'm and D'k are evaluated using classification algorithms including naive Bayes and a new classification algorithm. The accuracy of the two datasets is then compared

In this work, a hybrid feature estimation measure is given as

$Decisiontree$ best split measure $=Max\{\alpha,\beta,\gamma\}$

$Improvedconditional\ Pro\ bEstimation(ICPE)$

$$= \sum^{\sum x)\ exp(\frac{F(x)}{F(X,Y)}} lg(F$$

$ChiConditionalEntropy(CCE)$:

$$= \sum lg(F(x).chisquare(\Gamma\frac{F(x)}{F(X,Y)})$$

$$\alpha = \frac{-\sqrt{ICPE(Y/X)}}{(\sum X_i)^3.max\{E(D_i),GR(D_i)\}^3}$$

$$\beta = \frac{-ICPE(Y/X).ICPE(X/Y)}{\sum {D_i}^3\Gamma\sqrt{Chisquare/(N(k-1)}}$$

$\gamma = (\alpha+\beta)/2$

$N = total$ observations

$k = min(rows, columns)$

9. Statistical results are analyzed.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7462
***Article Received**: 22 May 2023 **Revised:** 13 July 2023 **Accepted:** 03 August 2023*

Process hash block

In this non-linear chaotic function, Q and R represent the dynamic permutation matrices. These matrices are generate using the function.

For each byte in P[i]

Do

$$R1 = SK^{T} \cdot [R.\ MaxEigen(SK).\ (MaxCoeffient(Poly(SK)))]$$

$$R_2 = \left(\frac{[Q.Avg(SK).Rank(SK)]}{(\sum SumofSqures(SK[i]))}\right)$$

$$R_3 = \sum PNLCF(n) * Eigen(Q.R)$$

$$H[i] = R_1 \oplus R_2 \oplus R_3$$

Done

A. Description

Initially, machine learning model is proposed in order to find the k-essential key patterns from the classification algorithm. In the step 1, input data is converted in to byte array using the medical user ID as S_id and its corresponding record as SData. This step is repeated to each multi-user data in the given transactions list. In the step 2, input data M is partitioned into k blocks with each size 8bits. In the step 3, padding operation is performed on the input data if the message size exceeds the block size. In the step 4, each block in the k blocks is partitioned into subblocks of each 32bits. In the step 5, a sequence of mathematical transformations is applied on the subblock partition for hash computation. In the step 6, all the subblock hash values are concatenated as final hash value.

In this work, a hybrid non-linear data integrity computation model to verify the integrity of each user in a multi-user setup for strong cloud data security is proposed. In this proposed process, we implement four different key phases on cloud-integrated medical data.

Multi-user access privacy preserving security model

Fuzzy Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is a cryptographic method that enables secure and efficient data sharing between multiple parties in unstructured databases. Here are the steps for implementing fuzzy CP-ABE in different unstructured databases:

Key Generation: The first step is to generate the public key and private key for each party involved in the data sharing process. The public key is used for encrypting the data, while the private key is used for decryption.

Attribute Definition: The next step is to define the attributes that describe the data in the unstructured database. Attributes can include information such as data type, data owner, data content, and more.

Policy Generation: Based on the attributes defined, a policy can be generated that specifies the conditions under which the data can be accessed. For example, a policy may specify that the data can only be accessed by parties that have a certain set of attributes.

Encryption: The data in the unstructured database is then encrypted using the public key and the policy generated in the previous step. The encrypted data is then stored in the database.

Decryption: When a party wants to access the encrypted data, they must first prove that they possess the attributes specified in the policy. If the attributes are verified, the encrypted data is then decrypted using the private key of the party.

Fuzzy Encryption: In fuzzy CP-ABE, a fuzzy set is used to encrypt the attributes. This allows for partial matches between the attributes specified in the policy and the attributes possessed by the party accessing the data. This makes the system more flexible and less prone to errors.

Let H _Attlist is the 4096 value of all the supply chain purchasers list.
G1,G2 are the cyclic groups
A set of random generators from cyclic groups are r, g_r, g_p, r_j

$$\text{Cauchy distribution=CD(d)} = \frac{q}{\pi[(d-p)^2 + q^2]}$$

Cyclic_Element Ahash = Bipair(G1,bytes(H _Attlist[i]).CD(m).getBytes()).pow_Zn(rj));
SecrK.Dj = {Attlist[i], g_r.mul(H _Attlist)};
Secretkey = {Bipair(Zr), SecrK.attr, Attlist, SecrK.Dj, PK.gp.powZn(r_j), H _Attlist}

Multi-user purchase ordering integrity verification: In the decryption phase, cipher text, secret key,Access tree, policies are used to decode the input data .

IV. EXPERIMENTAL RESULTS

Experimental results are performed on different textual datasets using the java programming environment and third-party java libraries such as JABE, JAMA, JECC, AWS JDK etc. Amazon cloud storage is used to store the cipher text and secret key for data decryption process. In this study, we evaluate the performance of the proposed method by comparing it to standard methods using several performance metrics such as data size, sensitivity (mean change in bits), and runtime. We measure the sensitivity by determining the effect of changing the input data bits on the integrity bits. We calculate the runtime for the integrity computation, data encryption, and decryption procedures. Our proposed approach for privacy-preserving data mining is applied to the adult dataset, medical datasets, and German credit dataset from the UCI machine learning repository. We conduct a comparative performance analysis between our proposed privacy-preserving model and traditional models on various datasets. We perform experiments using credit and adult datasets collected from the UCI repository and implement our method using the JAVA programming language to determine its efficiency and execution time. We identify quasi-identifiers and apply geometric data perturbation to numerical quasi-identifiers. Categorical quasi-identifiers are generalized based on their

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7462
***Article Received**: 22 May 2023 **Revised:** 13 July 2023 **Accepted:** 03 August 2023*

generalization hierarchies and k-value. Our study highlights a transition with minimum loss.

1) Secret key generated using the encryption algorithm

SecretKey SK = SerializeUtils.unserialize(SecretKey.class, new File(SKFileName));

This describes the secret key value generation script for the input data during the encryption process. This key is generated using the integrity value and the attributes list.

2) MasterKey generation in the encryption process

MasterKey MK = SerializeUtils.unserialize(MasterKey.class, new File(MKFileName));

This describes the master key value generation script for the input data during the encryption process. This master key is generated in the setup phase of the proposed encryption model. This key is generated using the integrity value, policies list and the attributes list.

3) Public Key for PPDM

PublicKey PK = SerializeUtils.unserialize(PublicKey.class, new File(PKFileName));

This describes the public key value of the input data which is generated in the encryption process. This public key is generated in the setup phase of the proposed encryption model. This key is generated using the integrity value, policies list and the attributes list.

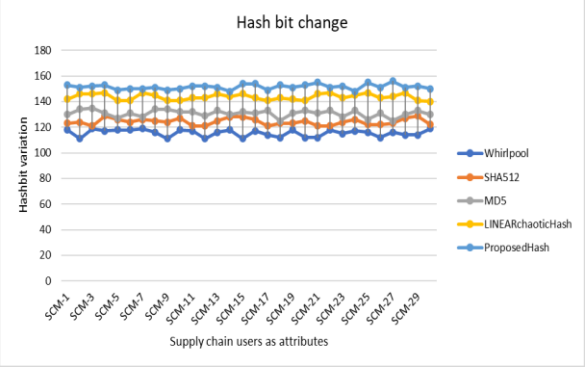

Figure 2. Performance of proposed integrity verification model to existing hash based approaches on variable size attributes(Hash size =4096)

Figure 2, illustrates the hash bit variation of the nonlinear multi-hash approach to the existing integrity approaches on different MEDICAL transactions with variable size attributes. In this figure, it is noted that the non-linear integrity model has better hash bit variation on different MEDICAL transactions.

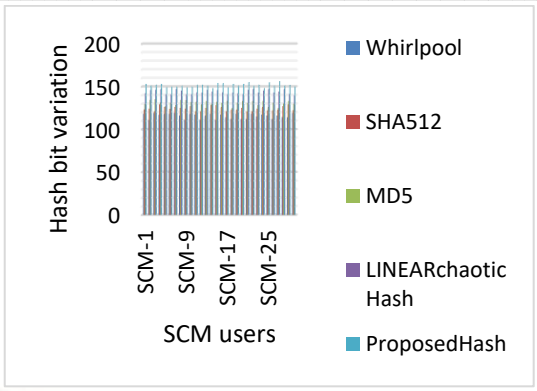

Figure 3. Performance of proposed integrity verification model to existing hash based MEDICAL approaches on variable size attributes with heterogeneous datatype (Hash size =4096)

Figure 3, illustrates the hash bit variation of the nonlinear multi-hash approach to the existing integrity approaches on different MEDICAL transactions with variable size attributes. In this figure, it is noted that the non-linear integrity model has better hash bit variation on different MEDICAL heterogeneous data.

TABLE I. COMPARATIVE ANALYSIS OF INTEGRITY BASED PPDM MODEL ON DISTRIBUTED MEDICAL RECORDS

Hdata	Whirlpool	SHA512	MD5	LINEARchaotic Hash	ProposedHash
DDTEST-1	3210	3173	2930	2949	2475
DDTEST-2	2825	3225	3190	2812	2592
DDTEST-3	3137	3158	2850	2884	2351
DDTEST-4	3104	2833	3111	3224	2369
DDTEST-5	3170	2880	2995	3178	2582
DDTEST-6	3046	3286	3142	3112	2376
DDTEST-7	3153	2989	3086	3074	2293
DDTEST-8	3009	3096	3234	2867	2497
DDTEST-9	3244	2890	3023	2891	2548
DDTEST-10	3231	3090	3097	3047	2508
DDTEST-11	2957	3021	3230	3235	2342
DDTEST-12	2883	3006	2997	3228	2355
DDTEST-13	2964	3117	3193	3005	2495
DDTEST-14	3215	2992	3092	2914	2532
DDTEST-15	2812	2952	3272	3142	2492
DDTEST-16	3134	3043	3078	2921	2640

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7462
***Article Received**: 22 May 2023 **Revised:** 13 July 2023 **Accepted:** 03 August 2023*

DDTEST-17	3182	3269	2853	3070	2645
DDTEST-18	3004	2901	2928	2998	2566
DDTEST-19	3061	2999	2810	3140	2411
DDTEST-20	2910	2838	3260	2873	2631
DDTEST-21	2868	3042	3180	3157	2589
DDTEST-22	3204	3133	2895	2821	2428
DDTEST-23	3088	3229	2982	3151	2670
DDTEST-24	3161	2815	3083	3012	2620
DDTEST-25	2997	2941	3112	3023	2587
DDTEST-26	3119	2788	3168	2918	2601
DDTEST-27	3146	2857	3127	2980	2535
DDTEST-28	2968	2861	3110	3247	2563
DDTEST-29	3075	3234	3250	3018	2330
DDTEST-30	3150	2863	3271	2978	2680

Table 1, represents the runtime analysis of non-linear integrity model to the conventional models on MEDICAL transactions data. In the setup, different attributes and transactions are used to compute the runtime of each transaction.

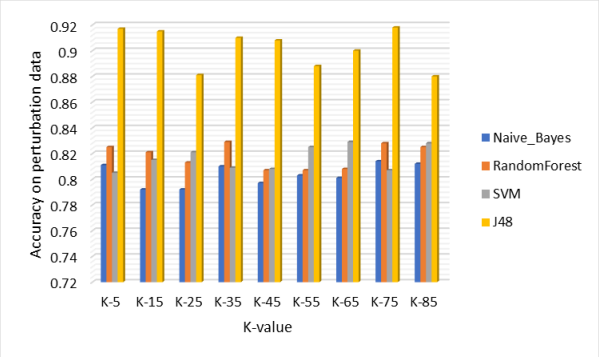

Figure 4. Comparative analysis of different classification models on perturbation distributed data.

Figure 4, describes the performance analysis of different classification algorithms such as SVM,J48, random forest and Naïve bayes on perturbation credit dataset. The classification accuracy of each model is plotted against the k-value in the figure 4.

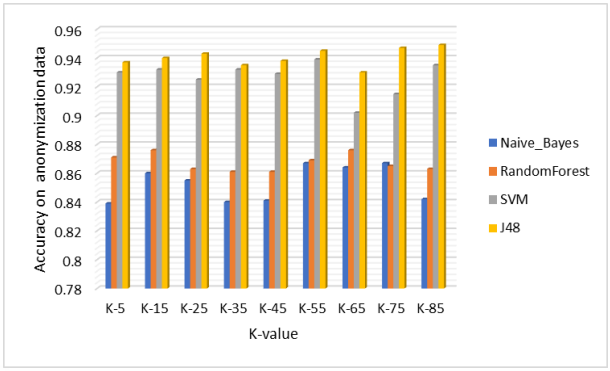

Figure 5. Comparative analysis of different classification models on anonymization credit data.

Figure 5, describes the performance analysis of different classification algorithms such as SVM, J48, random forest and Naïve bayes on anonymization credit dataset. The classification accuracy of each model is plotted against the k-value in the figure 5.

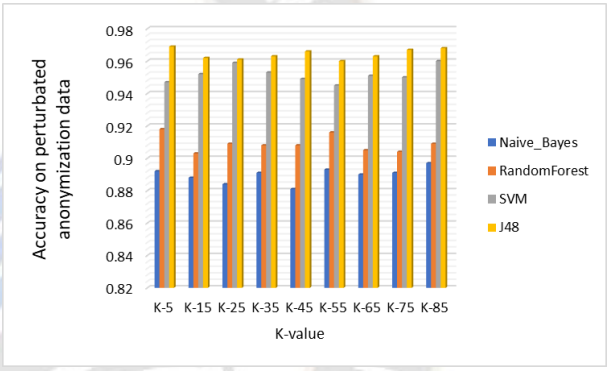

Figure 6. Comparative analysis of different classification models on perturbation anonymization credit card data.

Figure 6, describes the performance analysis of different classification algorithms such as SVM, J48, random forest and Naïve bayes on perturbation credit dataset. The classification accuracy of each model is plotted against the k-value in the figure 6.

TABLE II. COMPARATIVE ANALYSIS OF PROPOSED MODEL RECALL TO THE CONVENTIONAL METHODS RECALL ON MULTI-CLASS PRIVACY DETECTION PROCESS

Data size	J48	RF	RIPPER	Proposed Rule Model
Testdata-1	0.87	0.91	0.92	0.954
Testdata-2	0.88	0.9	0.92	0.965
Testdata-3	0.89	0.9	0.92	0.957
Testdata-4	0.89	0.9	0.93	0.958
Testdata-5	0.88	0.9	0.92	0.956
Testdata-6	0.88	0.91	0.93	0.97
Testdata-7	0.88	0.91	0.91	0.967
Testdata-8	0.88	0.92	0.92	0.964
Testdata-9	0.88	0.92	0.94	0.954
Testdata-10	0.88	0.92	0.94	0.964

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7462
***Article Received**: 22 May 2023 **Revised:** 13 July 2023 **Accepted:** 03 August 2023*

Table 2, illustrates the comparison of proposed privacy preserving model to the conventional model for precision prediction. From the table, it is noted that the proposed approach has better precision than the conventional models.

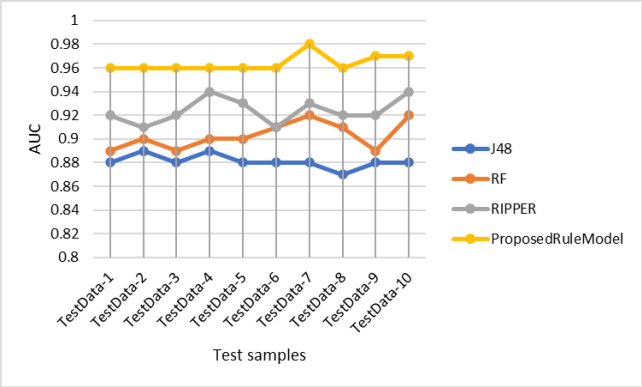

Figure 7. Comparative analysis of proposed model AUC to the conventional methods AUC on multi-class privacy detection process

Figure 7, illustrates the comparison of proposed privacy preserving model to the conventional model for AUC prediction. From the table, it is noted that the proposed approach has better AUC than the conventional models.

V. CONCLUSION

In this paper, a novel privacy preserving mode is implemented on the distributed database for strong cloud data security. A hybrid block-chain framework is implemented on the large databases. This framework is tested on the both the private and public cloud servers. Most of the conventional block-chain frameworks are based on the existing integrity and confidentiality models. In this framework, a novel machine learning classification model is proposed along with the non-linear chaotic function-based hash algorithm and advanced attribute-based encryption models on the large cloud datasets. Experimental results proved that the proposed advanced block-chain technology has nearly 8% improvement than the traditional security models in terms of accuracy and security factors are concerned. In future scope, proposed model is integrate to quantum based privacy preserving model for real-time cloud databases.

REFERENCES

[1] A. Smahi et al., "A blockchainized privacy-preserving support vector machine classification on mobile crowd sensed data," Pervasive and Mobile Computing, vol. 66, p. 101195, Jul. 2020, doi: 10.1016/j.pmcj.2020.101195.

[2] Z. Xu, Y. Lin, V. K. Arthur Sandor, Z. Huang, and X. Liu, "A lightweight privacy and integrity preserving range query scheme for mobile cloud computing," Computers & Security, vol. 84, pp. 318–333, Jul. 2019, doi: 10.1016/j.cose.2019.04.003.

[3] D. Ahamad, S. Alam Hameed, and M. Akhtar, "A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization," Journal of King Saud University - Computer and Information Sciences, Oct. 2020, doi: 10.1016/j.jksuci.2020.10.015.

[4] Y. Tian, M. M. Kaleemullah, M. A. Rodhaan, B. Song, A. Al-Dhelaan, and T. Ma, "A privacy preserving location service for cloud-of-things system," Journal of Parallel and Distributed Computing, vol. 123, pp. 215–222, Jan. 2019, doi: 10.1016/j.jpdc.2018.09.005.

[5] A. Cuzzocrea, C. K. Leung, B. H. Wodi, S. Sourav, and E. Fadda, "An Effective and Efficient Technique for Supporting Privacy-Preserving Keyword-Based Search over Encrypted Data in Clouds," Procedia Computer Science, vol. 177, pp. 509–515, Jan. 2020, doi: 10.1016/j.procs.2020.10.070.

[6] J. Hua, G. Shi, H. Zhu, F. Wang, X. Liu, and H. Li, "CAMPS: Efficient and privacy-preserving medical primary diagnosis over outsourced cloud," Information Sciences, vol. 527, pp. 560–575, Jul. 2020, doi: 10.1016/j.ins.2018.12.054.

[7] Chinmay Rawat. (2023). AI for Effective use of Water in India for Crop Cultivation. International Journal of Intelligent Systems and Applications in Engineering, 11(3s), 266–270. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2683

[8] Z. L. Jiang et al., "Efficient two-party privacy-preserving collaborative k-means clustering protocol supporting both storage and computation outsourcing," Information Sciences, vol. 518, pp. 168–180, May 2020, doi: 10.1016/j.ins.2019.12.051.

[9] Q. Zhang, G. Wang, and Q. Liu, "Enabling Cooperative Privacy-preserving Personalized search in cloud environments," Information Sciences, vol. 480, pp. 1–13, Apr. 2019, doi: 10.1016/j.ins.2018.12.016.

[10] B. Denham, R. Pears, and M. A. Naeem, "Enhancing random projection with independent and cumulative additive noise for privacy-preserving data stream mining," Expert Systems with Applications, vol. 152, p. 113380, Aug. 2020, doi: 10.1016/j.eswa.2020.113380.

[11] X. Liu, R. H. Deng, Y. Yang, H. N. Tran, and S. Zhong, "Hybrid privacy-preserving clinical decision support system in fog–cloud computing," Future Generation Computer Systems, vol. 78, pp. 825–837, Jan. 2018, doi: 10.1016/j.future.2017.03.018.

[12] C. Zhang, L. Zhu, C. Xu, and R. Lu, "PPDP: An efficient and privacy-preserving disease prediction scheme in cloud-based e-Healthcare system," Future Generation Computer Systems, vol. 79, pp. 16–25, Feb. 2018, doi: 10.1016/j.future.2017.09.002.

[13] Diksha Siddhamshittiwar. (2017). An Efficient Power Optimized 32 bit BCD Adder Using Multi-Channel Technique. International Journal of New Practices in Management and Engineering, 6(02), 07 - 12. https://doi.org/10.17762/ijnpme.v6i02.57

[14] S. Sheela and K. Sathesh Kumar, "Privacy –Preserved in cloud based data sharing for energy management system using big data analytics," Materials Today: Proceedings, Nov. 2020, doi: 10.1016/j.matpr.2020.09.621.

[15] E. Ezhilarasan and M. Dinakaran, "Privacy preserving and data transpiration in multiple cloud using secure and robust data access management algorithm," Microprocessors and Microsystems, vol. 82, p. 103956, Apr. 2021, doi: 10.1016/j.micpro.2021.103956.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7462
***Article Received**: 22 May 2023 **Revised:** 13 July 2023 **Accepted:** 03 August 2023*

[16] W. Fan, J. He, M. Guo, P. Li, Z. Han, and R. Wang, "Privacy preserving classification on local differential privacy in data centers," Journal of Parallel and Distributed Computing, vol. 135, pp. 70–82, Jan. 2020, doi: 10.1016/j.jpdc.2019.09.009.

[17] N. Domadiya and U. P. Rao, "Privacy Preserving Distributed Association Rule Mining Approach on Vertically Partitioned Healthcare Data," Procedia Computer Science, vol. 148, pp. 303–312, Jan. 2019, doi: 10.1016/j.procs.2019.01.023.

[18] S. Li, N. Mu, J. Le, and X. Liao, "Privacy preserving frequent itemset mining: Maximizing data utility based on database reconstruction," Computers & Security, vol. 84, pp. 17–34, Jul. 2019, doi: 10.1016/j.cose.2019.03.008.

[19] X. Ma, F. Zhang, X. Chen, and J. Shen, "Privacy preserving multi-party computation delegation for deep learning in cloud computing," Information Sciences, vol. 459, pp. 103–116, Aug. 2018, doi: 10.1016/j.ins.2018.05.005.

[20] A. Alabdulatif, I. Khalil, H. Kumarage, A. Y. Zomaya, and X. Yi, "Privacy-preserving anomaly detection in the cloud for quality assured decision-making in smart cities," Journal of Parallel and Distributed Computing, vol. 127, pp. 209–223, May 2019, doi: 10.1016/j.jpdc.2017.12.011.

[21] J. Domingo-Ferrer, O. Farràs, J. Ribes-González, and D. Sánchez, "Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges," Computer Communications, vol. 140–141, pp. 38–60, May 2019, doi: 10.1016/j.comcom.2019.04.011.

[22] Y. Zhao, S. K. Tarus, L. T. Yang, J. Sun, Y. Ge, and J. Wang, "Privacy-preserving clustering for big data in cyber-physical-social systems: Survey and perspectives," Information Sciences, vol. 515, pp. 132–155, Apr. 2020, doi: 10.1016/j.ins.2019.10.019.

[23] Jackson, B., Lewis, M., Herrera, J., Fernández, M., & González, A. Machine Learning Applications for Performance Evaluation in Engineering Management. Kuwait Journal of Machine Learning, 1(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/126

[24] J.-S. Lee and S.-P. Jun, "Privacy-preserving data mining for open government data from heterogeneous sources," Government Information Quarterly, vol. 38, no. 1, p. 101544, Jan. 2021, doi: 10.1016/j.giq.2020.101544.

[25] H. Rong, J. Liu, W. Wu, J. Hao, H. Wang, and M. Xian, "Toward fault-tolerant and secure frequent itemset mining outsourcing in hybrid cloud environment," Computers & Security, vol. 98, p. 101969, Nov. 2020, doi: 10.1016/j.cose.2020.101969.

[26] P. Kumar, G. P. Gupta, and R. Tripathi, "TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning," Journal of Systems Architecture, vol. 115, p. 101954, May 2021, doi: 10.1016/j.sysarc.2020.101954.