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

BDBC - Block-Chain Data Transmission Using Blowfish Security with Optimization in Cloud Network

Venkata Naga Rani Bandaru*[1], P. Visalakshi[2]

Submitted: 15/09/2023 **Revised:** 22/10/2023 **Accepted:** 14/11/2023

Abstract: Massive health-related records are continually being produced and kept in heterogeneous networks due to the fast rise of cloud technologies and data collecting. Because of the enormous data collection through things and wearables, the network needs a secure processing platform to preserve all. These data are maintained and secured by various managing systems, protocols, and algorithms as well as hardware's. We need to safeguard the data from illegal access with minimum resources. In proposed method, users and data proprietors will access the network through block chain and cloud technologies through the BDBC-block-chain data transmission using blowfish security with optimization in cloud network system. Before transmitting the data across blockchain to the cloud, the data proprietor encrypts it using the blowfish technique to protect from unauthorized entities and people.

Keywords: *Data Collection; Health Records; Encryption; Decryption; Blowfish; Unauthorized Access*

1. Introduction

The blockchain BC secures the data sharing process. There are several decentralised blockchain application platforms available currently. The cloud storage is used to save massive dataset into it, continuous dynamic data are commonly acquired throughout a protracted environment. BC is a ground-breaking system that enables reducing security risks and transparency in a scalable manner.

- The blockchain is a digital ledger otherwise database where encrypted data blocks are warehoused chained together.
- The data are dispersed rather than transferred, decentralized, and instantly accessible.
- Data are trustworthy and open.
- They are transparent that were produced with security in mind.

Through the protocol, the clients are connected to the cloud network. The protocol allows clients to search for a specific kind of dataset and displays all relevant data that is currently available in the storage. The customer will be sent a request for purchasing the selected dataset, the blockchain nodes will then send the dataset to the requested user. The server will send a linkage to the encrypted data once the transaction has been confirmed. The customer downloads the data and use the private keys to decode it. The protocol is compatible for smartphones, tablets, and laptops as well. Different wearable goods can communicate through wireless technology. The goods have sensors placed inside of them that sense and gather data from the human body and transmit it wirelessly to the server. The collected data will be sent to the assessment sector, where it will be evaluated and then combined with the required IDs. The identities are given out in accordance with the data's size, kind, and quality. The person's name, age, gender, address, mobile number, and country code are included in the data.

In BDBC the data will be encrypted using blowfish-key before being uploaded to the cloud storage to assure security and privacy. The key will then be divided into several shares and distributed among several systems to be used to decrypt the data. The overall number of systems and the blockchain security model define the bare minimum number of systems needed to decrypt the data. One must have both the link and authentication to the data to download the encrypted data. To decrypt it, they must obtain an adequate number of key shares for the encryption key. Users must obtain benefits in exchange for revealing their personal data to others;

*[1] *Research Scholar, Department of Networking and Communications, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, India*
Email: venkatanagarani.b@vishnu.edu.in

[2] Assistant Professor, Department of Networking and Communications, College of Engineering and Technology,
SRM Institute of Science and Technology, Kattankulathur, India

in certain cases, cash compensation is preferred. Personal data sharing may be difficult for a variety of reasons, including the need to carry out a vast number of transactions across numerous countries and among an equally enormous number of participants. We suggest creating our health data records, which can be done by putting the data on a system that is equipped with a blockchain to speed up transactions. In this process, encrypted data, blockchain transactions, and the sharing of decryption key are involved in the interactions between users.

2. Related Works

Virtualization, which divides actual computing machines into two or more virtual devices so that it can manage the computing chores simply, is the primary enabling technology for cloud computing. Pay-as-you-go cloud services are offered alongside major utilities like energy, telephone, and water [11]. A user's data, processing, and software are assigned to remote services through cloud computing. A shared pool of computer resources, such as servers, storage, networks, applications, and services, are made available on demand under this approach. Users and businesses can store and process their data in other people's data centres thanks to cloud computing and storage options [3]. The term "privacy" is also used to refer to a fundamental human right that pertains to the gathering, use, disclosure, storage, and erasure of personal data. Privacy violations and unauthorised access to cloud data can cause several problems for clients of the service. Users of the cloud anticipate high-level safety for all of their sensitive data and cloud-based applications [1]. The combination of current and upcoming new imperatives and problems for developing countries using cloud computing and mobile devices will be discussed in this article. Cloud service providers and mobile service providers have deployed hundreds of cloud-enabled applications and are continuing their cloud venture to offer an unending variety of products since the market for mobile phone and device users is too large to be ignored. [7]. Virtualization and service-oriented methodologies are used in cloud computing to distribute huge computing resources as services in order to lower costs, boost performance, or enable remote access. Large and powerful processing capabilities can now be supplied as services thanks to mobile cloud computing. This enables sophisticated computations that call for more powerful computer resources to be carried out on mobile devices with lower capabilities. [13]. It is crucial that we use cloud computing to address the problems and challenges in those fields as a result of the rapidly expanding e-learning industry and internet-based learning. This will enable us to improve these marketplaces' operational efficiency and effectiveness. Efficiency and effectiveness will help businesses simplify their operations and enable all potential clients to work quickly and move around more easily. [9]. This study examines the current patterns in the field of cloud computing and proposes a research area for potential future advancements of this technology in light of the current trends and the steadily expanding interest in this topic. Each of the key components of the opportunity in cloud research is listed and well explained [2]. The cloud infrastructure that is made available to a single user by a specific group of users from an organisation that has dealt with issues of common concern, such as security requirements, policy, mission, and compliance considerations, and the hybrid cloud, which combines two or more different cloud infrastructures [12]. The investigation into the technology and security issues surrounding cloud computing has produced a culminating understanding of the cloud computing phenomenon as a whole. The numerous, varied strategies used to address the security concerns posed by cloud computing have been left out of this article [5]. Since there is less need for powerful processing and large storage hardware, using clouds can help hardware designers produce smaller, less intrusive devices. When compared to conventional IT approaches, cloud computing provides many benefits. [8]. Users

of cloud computing can access a variety of programmes without needing a licence, to buy, install, or download any of this software, among other features. As there is no requirement for infrastructure, it also lowers the cost of maintaining and installing computers and software [4]. The viability of legal systems that impose obligations based on the location of data is one of these. Cloud computing service models are another. obtaining the data subject's consent; the efficacy of breach notification laws; the efficiency of cybercrime legislation in preventing and punishing cybercrime in the cloud; and, finally, the challenges associated with determining the relevant law and jurisdiction [10]. In order for enterprises to obtain a competitive edge from the adoption of the cloud, this paper adds to the work of the earlier researchers by recommending additional abilities that they should build. As stated before, a corporation's skills and abilities serve as both a source of innovation and a restraint on it. This study uses the resource-based theory as a theoretical framework to analyse how a firm's resources relate to its competitive advantage. [6].

3. BDBC Design and Implementation

3.1 Network Model

User devices U_R, access points A_S, internet gateways I_G, host servers C_H, and storage devices C_D are the elements of the hierarchical cloud network, also the development of distributed computing systems is referred to as "cloud network" as shown in Figure.1. Data is generated at the user end and transferred to the cloud server via access points and gateways, in addition, the users receive data from the server on the same path. In a similar manner, U_R will ask the server a query and wait for a reply, the servers respond to the user through relevant data. Effective storage entities are responsible for maintaining the cloud databases. The network was built with efficient blockchain data storage for safe data upload and download processes. Key-sharing encryption, short-term signatures, and other characteristics are built into a cryptosystem using the blowfish encryption and decryption methodology.

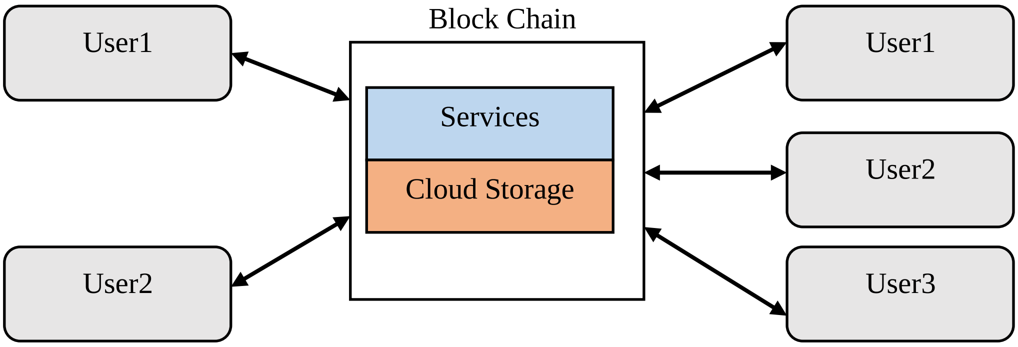

Fig. 1. Cloud Network

3.2 Data Access Method

The BDBC method secures cloud data by utilising the blockchain-based artificial intelligence system B_{CA}. The system processed human health records, thus the B_{CA} computed the, disparities, progress, and platforms for it. The B_{CA} based protection is used to prevent the data sharing among unreliable parties. Private data centres protect the data physically, so, they employ the method of artificial intelligence operational assistance. Data access control is a crucial feature of private data centres, so, the data must be registered in a data request broker to be made aware of the availability of transfers before being shared over the Internet. In addition to designating the data, the data request broker is in charge of validating the data and documenting the behaviour of transactions.

Each user and proprietor of the data sign up and be verified by the cloud network in order to access it. As soon as sign up and confirmation were successful, the proprietor was able to access the consoles. They can use the blowfish encryption technique to encrypt data, then upload the encrypted file to the cloud storage. Once the encrypted file has been successfully uploaded to the cloud, the access link to it and the private key required to decrypt it are saved in the block.

Each block's hash value id is created when the link has been stored on it, and the block is then kept on the BC, the data user has access to whatever file they desire. The user searches for the document using the exploration bar. The user will be prompted to request permission to view the warehoused data if they are able to find the requested file in the cloud.

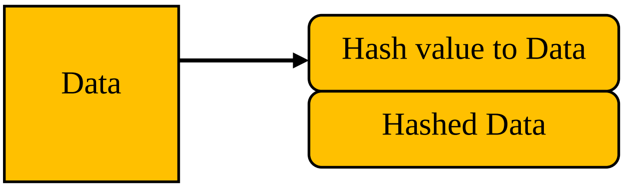

Fig. 2. Hash Function

If the proprietor accepts the user request and complies with the requirements, the user will receive the hash value required to obtain the access link and remote key of the uploaded encrypted file from the proprietor. After receiving the demand, the proprietor gives the key to the person who requested access. The user can then use the key to access the blockchain link.

3.3 Data Classification

In BDBC health records are used and they are classified as stable and changeable data collections. Secluded information of individual that does not change over the period of their epoch, such as a fingerprint, an eyeball, a gene, etc are known as stable data. The changeable data, which includes facts on pulse, temperature, blood pressure, heart rate, and so on as shown in Table.1, the changeable data are further classified into rapid changeable and normal changeable records, like breath, heart rate, sugar, pressure and so on are fluctuate frequently called as rapid changeable data, height, bones growth and weight as well are normal changeable data. Still, data can be classified into instantaneous and long-term recordable data. Instantaneous data is acquired right away and might be constant or changeable, whereas long-term data is continuously tracked over the period. On the basis of the data kind and gathering techniques, classification methods are taken into consideration. According to the health indicator's data may fall under several categories.

Table 1. Health Record

Person Records	Person Particulars
ID	Name
Symptom	ID
Blood Pressure	Gender
Heart Rate	Age
Cholesterol Level	Location
Echo	Phone Number
TSH	Address
Physician ID	City
Pulse	Pin code
Temperature	Country

3.4 Access Allocation

The majority of data is collected by sensors and wireless devices through wearable items, and we can update the data collections in the database. Due to non-operation, data expiration, and the data proprietor 's willing, the service provider may remove data from the database. Also, with some restrictions, the proprietor permits user to access the data and download it. In the cloud network, the server faces threaten from different attacks and viruses also they may grow through the compromise behaviour. Inadequate evidence, hazardous network interfaces, programmes, access controls, and resources, among other things, are the foundations upon which the risks were formed. To overcome this, the cloud service offers an access symbol to each user. So, they can retrieve mandatory data from storage through the access symbol.

Advanced artificial intelligence techniques used to assess the pattern of the data in order to make sure that it complies with validation patterns. It allows us to employ technology and to check the data's accuracy. If the sensor is from an authorized dealer, it is approved as competent product and the data made by it are unswerving. The protocol monitors the product information, otherwise it will not allow the communication. For this reason, a predetermined and up-to-date database of verified products should be created. The programme was created using to accurately classify the patterns in a time series dataset. The system produces high-quality classifiers for many types of data using related machine learning algorithms. The absurd data will be removed, leaving only the data with predetermined features saved. The data is divided as training and testing parts, the training sets are gathered the features and saved to validate the testing data.

3.5 Data Transmission

Data execution enables the blockchain ledger to control the exchange process. A vast volume of data is enabled with blockchain embedding and artificial intelligence. maintaining secure environment for the administration of health data by storing and sharing amongst reliable parties. The health data is currently housed in a variety of environments and is under the jurisdiction of several organisations, each of which may have different requirements. In order to address the aforementioned issues, block chain provides assurance service that controls data between reputable parties using artificial intelligence examinations. It observes packet size average P_A based on total data transferred P_{ST} and number of data D_N moved to the database. Also, P_D and R_D are defined as sending and receiving data at storage from user and vice versa, these values provide probability of transmission T_P between them. The transmission throughput is computed as below to find the bits transferred between them. Then the transmission noise is computed as T_N. The transmission noise is computed as gain of transmission $T_G$and occurred noise N during transmission. Then the per second receiving bits B_P are computed as per data size and noise of transmission. Also, maximum data tM_D ransferred to the data base is computed based on number of devices N_D.

$$P_A = \frac{P_{ST}}{D_N}$$

$$T_P = \frac{R_D + T_C}{R_D S_D}$$

$$T_T = \frac{T_P P_A}{(1 - T_P)F_T + T_P + T_P}$$

$$T_N = \frac{T_G}{N}$$

$$B_P = D_S log_2(1 + T_N)$$

$$M_D = \frac{D_S + T_G}{N_D}$$

The information is gathered and categorised according to kind of data, and the blockchain algorithm refined and confirmed the final information. After that, the producing block for verification is put in the middle. using this advanced blockchain technology, a convolutional neural network can then verify the data using the RELU activation function. The convolutional neural network received multiple range of data to process, the sigmoid function and probability are used to check the data once it has been collected as shown in Figure.3. The most error-prone variations are ultimately sent when the convergence of the gathered data has been confirmed.

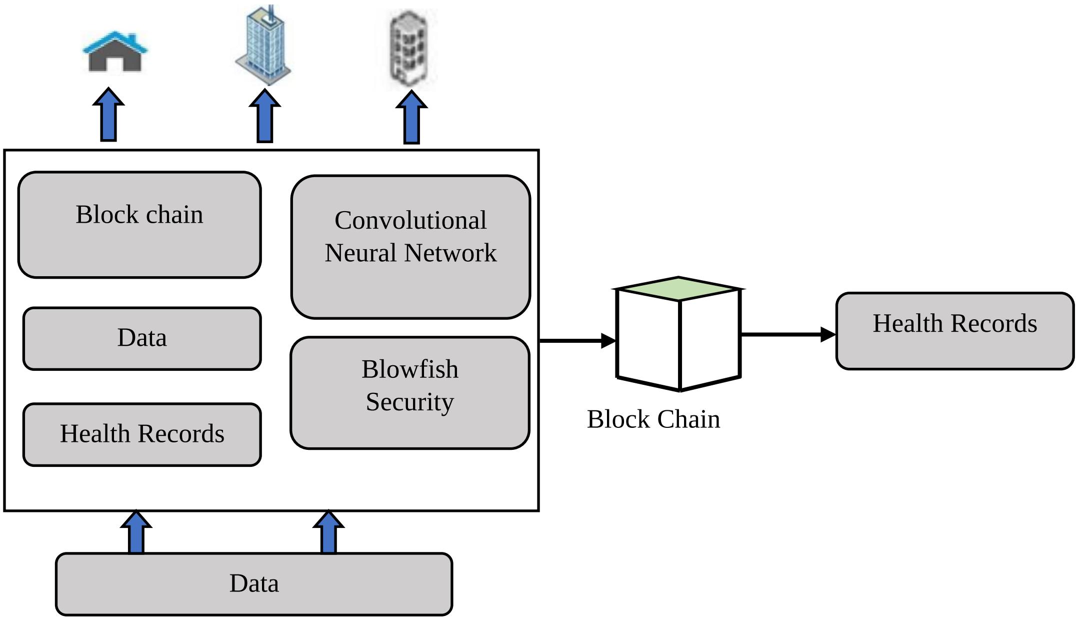

Fig. 3. BDBC System

3.6 Secure Key Process

In addition to receiving service advantages, the operator can upload, and exchange health records to the required users. Each user will be given a secure key to encrypt and decrypt the data during the data upload and download Although the maximum key length is predetermined, it can be changed for better performance and safety, in this context, one twenty eight blocks of data is converted into one twenty eight bit blocks of ciphertext. The blowfish algorithm uses thirty-two bits to four hundred- and forty-eight-bits ranges. The key is producing S-boxes $S_B$with a total of thousand twenty-four 32-bit entries, along with 32-bit sub-keys S_K, i input bits and n output bits make up the S-box. The keys are stored in an array A and take up in four thousand one hundred sixty-eight, bytes total:

$$A_1, \dots \dots . A_n$$

$$S_{K1} \dots \dots . S_{Kn}$$

$$\begin{cases} S_{B1} \dots . \dots . S_{B256} \\ S_{B2} \dots . \dots . S_{B256} \\ S_{B3} \dots . \dots . S_{B256} \\ S_{B4} \dots \dots . S_{B256} \end{cases}$$

Using the bits from the fractional part of the continual, prepare the sub keys array, followed by the S-boxes in that sequence. The most-left thirty-two bits of the fractional portion should then become S_{K1}, and so forth. Use key from the A-array as necessary when doing a bitwise-XOR of the $S_K$and A arrays.

$$S_{K1} = S_{K1} \oplus \ A_1, S_{Kn} = S_{Kn} \oplus \ A_n$$

Use the present S_K and S_B arrays to encrypt the sixty-four-bit block, and then replace S_{K1} and S_{K2} with the encryption's yield. The ciphertext created after encryption the yield with the current S_K and S_{B2} arrays should be used in place consecutive $S_{K3}$and S_{K4}. Use the yield of the computation uninterruptedly varying phases to apprise each section of S_K, then each section of S_B, one at a time.

A key- bowed according to variation, the key and data reliant according to replacement, and XORs all executions and include 32-bit in each round of the function's numerous repetitions. The new procedures for each round are the indexed data array lookup tables and the encryption method given below:

The array contains 18 sub keys

Split data d into dual 32-bit splits: dl, dr

$$For\ i = 1 - 16\ rounds$$

$$dl = dlXORS_K$$

$$dr = F(dl)XORS_B$$

$$switch\ dl\ and\ dr\ XORS_K\ \ undo\ last\ switch$$

$$Chipertext = concatenation\ of\ dl\ and\ dr$$

$$dl = dlXOR17$$

$$dl = dlXOR18$$

$$resyndicate\ dl\ dr\ to\ obtain\ chipertext$$

3.7 Data Notification

The data will then be encrypted and uploaded to the cloud network's storage. For security reasons, the decryption key will be separated and stored at various terminals. Following that, a transaction will be created and disseminated to all blockchain nodes. The transaction includes the data proprietor 's public key, a link to encrypted data with hash values, some rudimentary details, the dataset's cost, etc. A local device that is linked to the internet and running the key generation algorithm can obtain and securely store keys from the system. When a data transaction is verified, a notification is sent to the customer of that transaction to issue the relevant key.

Data proprietor provide their data to the clients, who then collect it and pay to the proprietors and service providers. Each of them receives support from the application according to their respective responsibilities.

Millions of records might be gathered through the sensors within short period, and the data size could exceed several gigabytes. The transactional data will be repeated among numerous nodes, including mining nodes, in the blockchain, which is a distributed datastore that is replicated. Large datasets, on the other hand, are kept in cloud storage, where the data is kept in an encrypted format and data pointers like hash pointers are used to identify the dataset's location to ensure its integrity and non-repudiation. Only the metadata of the unique dataset and minimum amount of data required for transactions will be stored and exchanged on the blockchain. After that, the key shares will be given to the systems and the data will be uploaded to the cloud storage.

The other participants will be notified by a transaction that the data has been uploaded and is ready for sharing. Following the user's confirmation, this transaction will be added to the blockchain via a compromise method and made visible to users and data verifiers. The data validator will validate the data as part of the data validation process by running the BDBC algorithms to ensure that the data is valid in accordance with the standards and requirements, and will then certify that the data is valid in accordance with the provided guidelines. A consumer selects the data they wish to use, confirms that it has received the necessary data validator certification, and then initiates a transaction to do so. The client will sign the transaction, and it will then be added to the blockchain.

A notification that a transaction for buying those data has been authorised will be sent to the key keeper of the associated dataset. Then, using an authenticated communication channel, key keepers give the client access to their key shares of the relevant dataset. The link to the encrypted data and sufficient key shares for decrypting it are sent to the client. The data can then be downloaded and decrypted by the user from the cloud storage. The workflow comes to an end since the data are usable.

The hash function and key of the blockchain safeguard the data transaction. The BC infrastructure protects the decryption key and enables the creation of authenticated channels with other contributors, approving the data to be securely decrypted for the intended receiver.

4. Results and Discussion

Accuracy				**Error**			
User	**ICKM**	**CK-CLOUD**	**BDBC**	**User**	**ICKM**	**CK-CLOUD**	**BDBC**
10	0.285714	0.571429	0.638547	10	0.714286	0.428571	0.368976
20	0.208333	0.708333	0.749297	20	0.791667	0.291667	0.268737
30	0.176471	0.676471	0.764858	30	0.823529	0.323529	0.276461
40	0.250000	0.659091	0.710956	40	0.750000	0.340909	0.308275
50	0.296296	0.759259	0.785675	50	0.703704	0.240741	0.206235

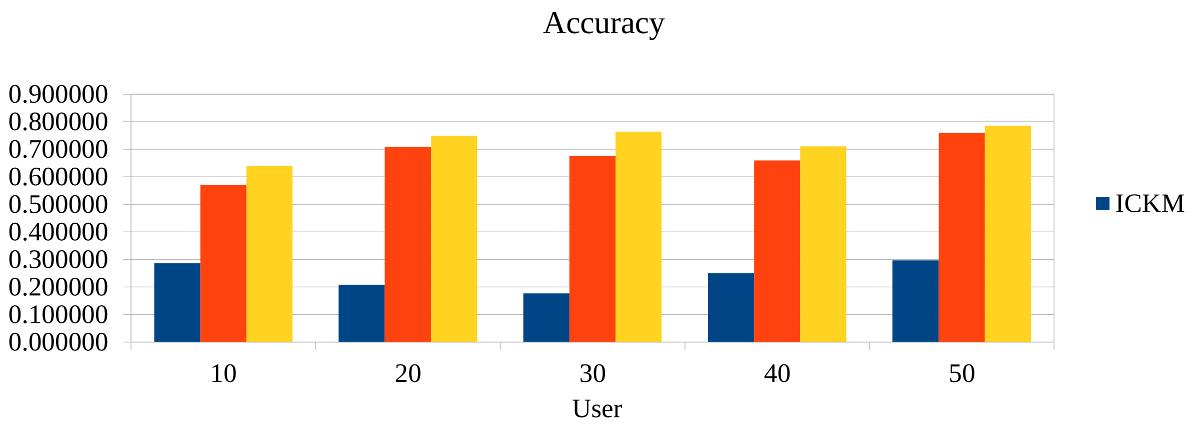

Fig. 4. User Vs Accuracy

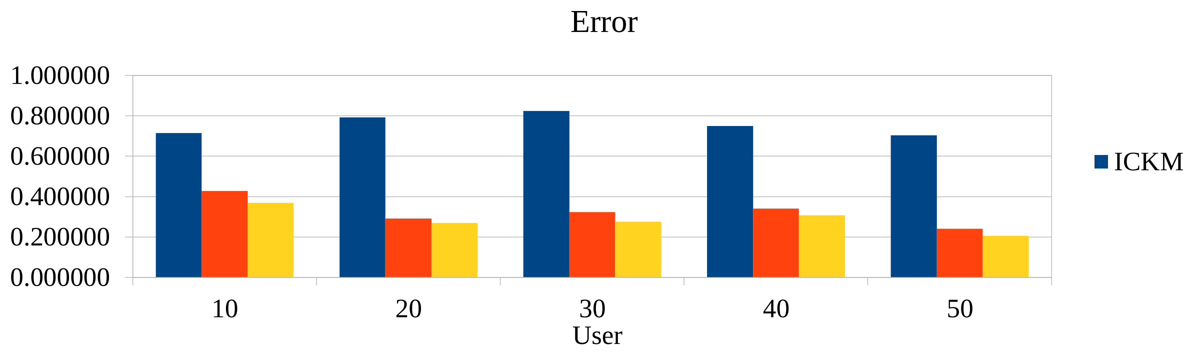

Fig. 5. User Vs Error

The accuracy, which goes from 0 to 1, is the proportion of data that are correctly classified. In this measure, we compared the previous implementations of CKM and CK_Cloud with the BDBC, among these BDBC technique accurately categorised the data and increased accuracy as shown in Figure.4. The technology employs blowfish encryption and decryption for safe data transfer, which increases the security of communication in a cloud network. The errors then indicate the transaction's uncertainty, as seen in Figure 5. In this case, the error in BDBC is lower than in the compared approaches, which explains, transmission uncertainty is minimised in the proposed method such as 70.37% for ICKM, 24.07% for CK_Cloud and 20.52% for BDBC.

5. Conclusion

In this BDBC effort, we proposed a blockchain and AI-based solution for users, data proprietors, and storage facilities to exchange health records. It enables data proprietors to securely kept through blowfish computation and distributed health records to the clients. In this study, human wearables were used to gather health records from several groups and they classified according to their categories and conditions. The BDBC suggested integrating cloud storage with blockchain, sharing varied sizes of changeable data to the storage through encryption of blowfish safe keys. The blockchain stores the qualities and transferred data, and the data is kept in the cloud in an encrypted way. The data is handled with the highest level of precision and the fewest errors based on blowfish methodology's encryption and decryption.

References

[1] Fatimah Khalil Aljwari, “Challenges of Privacy in Cloud Computing”, Journal of Computer and Communications, 2022.

[2] Deepak Putha, B. P. S. Sahoo, Sambit Mishra, and Satyabrata Swain, “Cloud Computing Features, Issues and Challenges: A Big Picture”, International Conference on Computational Intelligence & Networks, 2015.

[3] Deepak Kumar Verma, and Tanya Sharma, “Issues and Challenges in Cloud Computing”, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 8, Issue 4, April 2019.

[4] Nidal M. Turab, Anas Abu Taleb Shadi, and R. Masadeh, “Issues and Challenges in Cloud Computing”, International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 8, Issue 4, April 2019.

[5] Monjur Ahmed and Mohammad Ashraf Hossain, “Cloud Computing and Security Issues in the Cloud”, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[6] John Otieno Oredo, and James Njihia, “Challenges of Cloud Computing in Business: Towards New Organizational Competencies”, International Journal of Business and Social Science, Vol. 5 No. 3, March 2014.

[7] Satyakam Rahul and Sharda, “Cloud Computing: Advantages and Security Challenges”, International Journal of Information and Computation Technology, Volume 3, Number 8, 2013.

[8] Zunair Mahmood, and Waleed Iftikhar, “A study on Cloud Computing issues and challenges in higher education institutes of Middle EasternCountries”, International Journal of Creative Research Thoughts (IJCRT), Volume 6, Issue 2, April 2018.

[9] Debabrata Nayak, “Understanding the Security, Privacy and Trust Challenges of Cloud Computing”, Journal of Cyber Security and Mobility, Vol. 1, 2012.

[10] Moulika Bollinadi, and Vijay Kumar Damera, “Cloud Computing: Security Issues and Research Challenges”, Journal of Network Communications and Emerging Technologies (JNCET), Volume 7, Issue 11, November 2017.

[11] Shaitan Singh Meena, and Dr. Satwinder Singh, “A Review on Security Challenges: Communication Level in Cloud Computing”, International Journal of Engineering Research & Technology (IJERT), 2016.

[12] Talal H. Noor, Sherali Zeadally , Abdullah Alfazi , and Quan Z. Sheng, “Mobile cloud computing: Challenges and future research directions”, Journal of Network and Computer Applications,2018.

[13] Communication Engineering (IJARCCE), Vol. 8, Issue 4, April 2019.

[14] Monjur Ahmed and Mohammad Ashraf Hossain, “Cloud Computing and Security Issues in the Cloud”, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[15] John Otieno Oredo, and James Njihia, “Challenges of Cloud Computing in Business: Towards New Organizational Competencies”,

International Journal of Business and Social Science, Vol. 5 No. 3, March 2014.

[16] M. Rajendra Prasad, Jayadev Gyani, and P.R.K. Murti, "Mobile Cloud Computing: Implications and Challenges", Journal of Information Engineering and Applications, Vol 2, No.7, 2012.

[17] Satyakam Rahul and Sharda, "Cloud Computing: Advantages and Security Challenges", International Journal of Information and Computation Technology, Volume 3, Number 8, 2013.

[18] Subhashini, B., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.

[19] Sharma, V., & Kumar, A. (2014). Cloud computing security issues and solutions: A survey. International Journal of Computer Applications, 96(6), 37-43.

[20] Alqahtani, S. M., & Alahmadi, H. A. (2019). Data security and privacy in cloud computing: A review on current standards, issues, and solutions. IEEE Access, 7, 73040-73057.

[21] Awan, I., Owen, G., & Crosbie, M. (2014). Cloud computing: A review of the security issues and the solutions. International Journal of Information Management, 34(3), 365-376.

[22] Jagadeesan, V., & Manickam, N. (2015). Security and privacy issues in cloud computing: A survey. Procedia Computer Science, 50, 1009-1014.

[23] Wang, C., Zhang, Q., Ren, K., & Lou, W. (2010). Privacy-preserving public auditing for data storage security in cloud computing. In Proceedings of IEEE INFOCOM.

[24] Subashini, S., & Kavitha, V. (2010). A survey on cloud computing security management. International Journal of Computer Applications, 1(10), 18-25.

[25] Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud security and privacy: An enterprise perspective on risks and compliance. O'Reilly Media, Inc.

[26] Zhang, Q., Cheng, L., & Bout Aba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7-18.

[27] Rittenhouse, J. W., & Ransome, J. F. (2016). Cloud computing: Implementation, management, and security. CRC Press.

[28] Anand, R., Ahamad, S., Veeraiah, V., Janardan, S.K., Dhabliya, D., Sindhwani, N., Gupta, A. Optimizing 6G wireless network security for effective communication (2023) Innovative Smart Materials Used in Wireless Communication Technology, pp. 1-20.

[29] Basaligheh, P. (2021). A Novel Multi-Class Technique for Suicide Detection in Twitter Dataset. Machine Learning Applications in Engineering Education and Management, 1(2), 13–20. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/14

[30] Ricci, A., Jankowski, M., Pedersen, A., Sánchez, F., & Oliveira, F. Predicting Engineering Student Success using Machine Learning Algorithms. Kuwait Journal of Machine Learning, 1(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/118