European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 7, Issue 4, 2020

Cloud Computing Security for Electronic Healthcare Records Using Block-chain Model

[1]Dr. A. POOBALAN, [2]Dr. N. Uma Maheswari, [3]Dr. R. Venkatesh

[1]Assistant Professor, Dept of CSE, University College of Engineering, Dindigul

[2]Professor, Dept of CSE, PSNA College of Engineering and Technology, Dindigul

[3]Professor, Dept of IT, PSNA College of Engineering and Technology, Dindigul

Abstract

This paper presents detailed information about blockchain technology about how blockchain technology is applied for cloud security. Blockchain is one of the novels and ever breaking technology used for high security, which has been used in high-level government applications. In this paper, to tighten the cloud security, the blockchain security model is implemented and integrated with the cloud application. Thus, the healthcare application-based cloud environment is considered as the base application and experiment blockchain algorithm. From the obtained and compared results, it has been found that the blockchain security is highly suitable for cloud security and performs well in securing data during persistence and transmission.

Keywords: Cloud Computing, Security in Cloud, BlockChain Security, Remote Device Access.

1. Background Study

Cloud computing is an environment utilizing an interconnection of remote servers deployed on the internet to store, progress, and accomplish the data, not only using a local server or single system [1]. Cloud computing always performs tasks only on remote servers. It is one of the on-demand availability of various computing resources, such as storage medium and power [2]. It uses more numbers of hardware and software to provide services to cloud users through the internet. One of the significant examples is Gmail, through which users can access data and files [3]. Cloud computing offers an efficient way to store and access the data virtually from anywhere, using any devices connected with the internet [4]. Any hardware failure does not make any data loss in the cloud [5]. The only problem with the cloud is the data stored in the cloud can be seen by anyone and can access it. The merits of cloud computing are no need admirative management, easy to access, pay and use, and reliability.

Maintaining patients, old age, and other disabled people regarding their health condition, curing, and preventing them from diseases is called Healthcare Monitoring [6]. It can improve manual management, maintaining electronic health records and provide treatment, and so on. In recent days, a massive amount of people is coming and staying for the curing of health. Those patient's data and information are maintained in the form of records electronically. It is called Electronic Health Records (EHR) [7]. Each HER has information about diseases, treatment methods, medicine information, and personal information for future investigation. Because of increasing voluminous data in the healthcare industry, it goes for centralized storage in the cloud. Also, the HER comprises of more personal data of the patients. It is misused by attackers, unauthorized people, especially insurance industries [8]. To save the patient's personal data, it needs security to hide the data. Blockchain, initially a blockchain, contains a list of records linked with cryptography [9]. Each block includes the timestamp information of the current block to the next block. The data is encrypted before outsourcing to the cloud. The healthcare providers have to decrypt the data before going to use it [10].

2. Cloud Healthcare Application

Health care applications are one of the most essential applications which help to feed, store, process, and transfer health information about patients, older people, and general check. All the data are feed from different locations and stored in local server initially and transmit to the cloud distributed server. They may be in the form of manual records. The patients upload the data through the local system deployed in the healthcare industries and connected with the cloud. The overall functionality of the healthcare cloud system is illustrated in Figure-1.

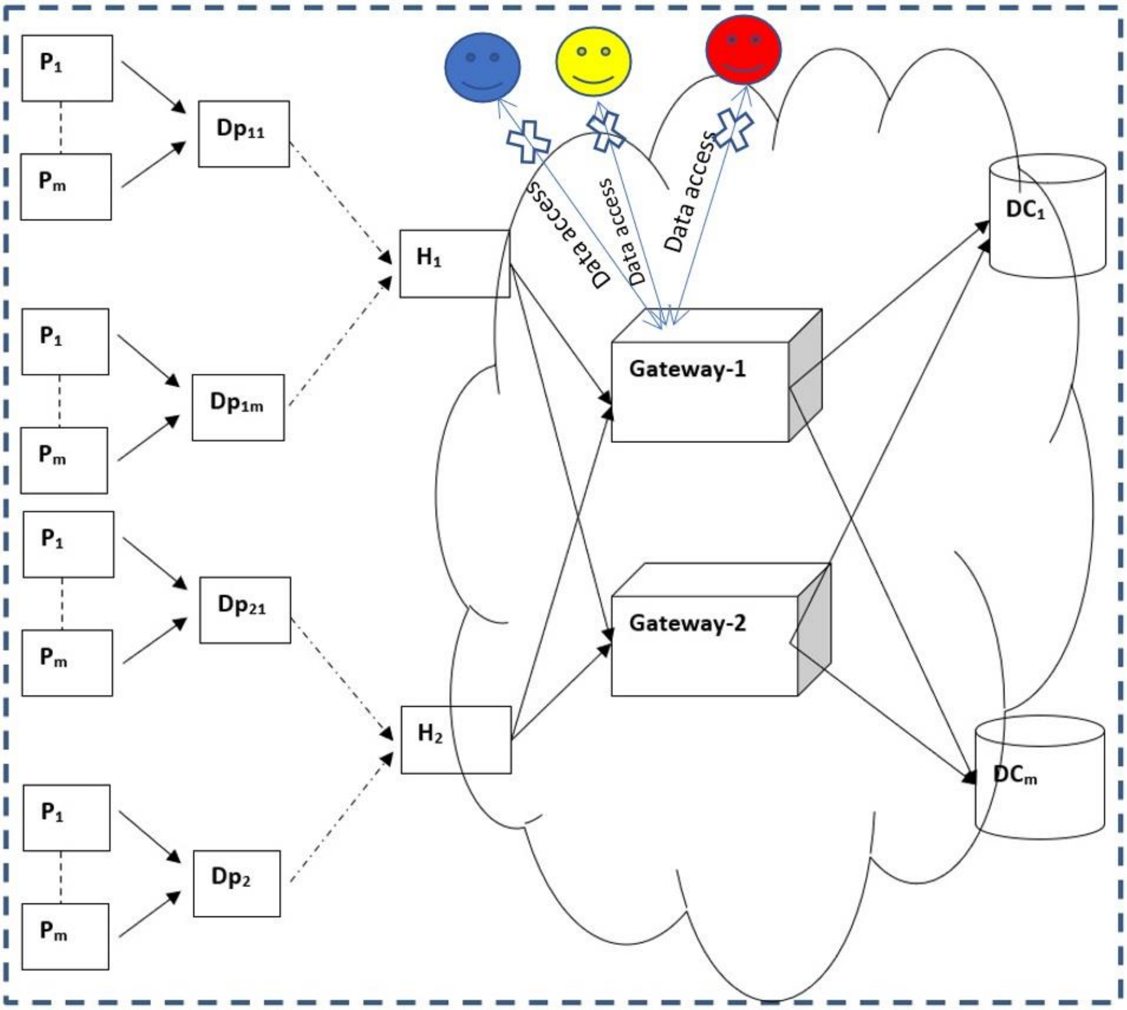


Figure-1. Cloud-Based Healthcare System

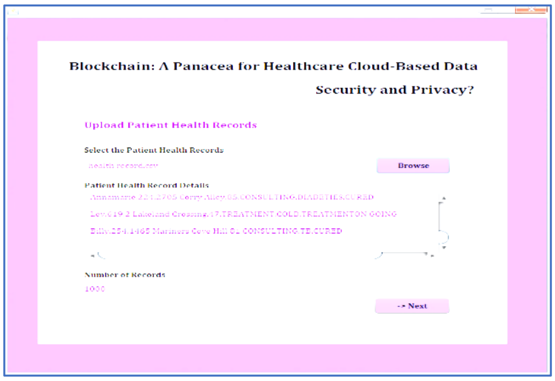
From each hospital $\boldsymbol{H}$, in $\boldsymbol{N}$ number of departments $\boldsymbol{DP}$, $\boldsymbol{m}$ number of patients are investigated for identifying medical abnormalities. The patient data is obtained from each hospital $\boldsymbol{H}$ is transferred to data centers $\boldsymbol{DC}$ in the cloud. Since the data is persisted in the cloud, any user can be fetched and misuse it. Thus, to avoid data theft, this paper provides blockchain security, which converts the data into secured blocks. Each block has encrypted data that cannot be used by any author, and it will be converted to an encrypted form. Thus, data security is provided for healthcare applications in the cloud. The overall functionalities of the healthcare architecture given in Figure-1 are programmed in the DOTNET framework and experimented verifying the performance.

3. Experimental Results and Discussion

The experiment is carried out in DOTNET 2014 framework. The Blockchain security model is implemented in C#.net, and the functionality is verified. The healthcare application is developed in the ASP.net application with the backend module of C#.net. In the experiment, various performance factors are analyzed and verified. The overall security model proposed in this work has been completed using the following modules.

4. Healthcare Provider

The proposed work provides a secured healthcare application where it has various sub-modules, such as Loading patient Records, Key Generation, encrypt patient Records, Block Creation, Upload and Download Patient $\boldsymbol{t}$ Records, and Cloud ID. The first stage of this work is loading the patient records.



Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?

Upload Patient Health Records

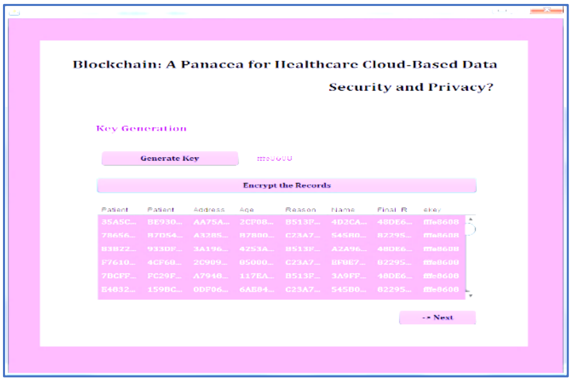
Select the Patient Health Records: health record.csv

Patient Health Record Details

```
Annamarie.221.2705 Corry Alley.65.CONSULTING.DIABETIES.CURED
Lev.619 2 Lakeland Crossing.47.TREATMENT.COLD.TREATMENTON GOING
Billy.254.1465 Mariners Cove Hill 61.CONSULTING.TB.CURED
```

Number of Records: 1000

Figure-2. Data Uploading



Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?

Key Generation

fffe8608

Patient	Patient	Address	Age	Reason	Name	Final_R	ekey
35A5C...	BE930...	AA75A...	2CF08...	B513F...	4D2CA...	48DE6...	fffe8608
78656...	B7D54...	A3285...	B7800...	C23A7...	545B0...	82295...	fffe8608
83B22...	933DF...	3A196...	4253A...	B513F...	A2A96...	48DE6...	fffe8608
F7610...	4CF68...	2C909...	85000...	C23A7...	EF8E7...	82295...	fffe8608
7BCFF...	FC29F...	A7948...	117EA...	B513F...	3A9FF...	48DE6...	fffe8608
E4832...	159BC...	0DF06...	6AE84...	C23A7...	545B0...	82295...	fffe8608

Figure-3. Key Generation Data Encryption

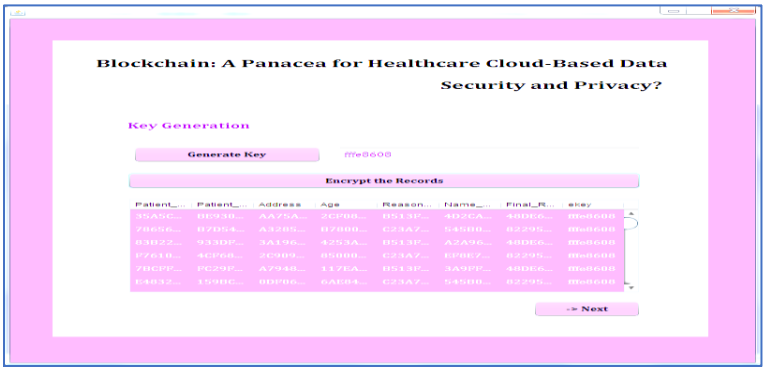
The healthcare application is implemented as a cloud application, where initially, it provides an option to upload all the data patient healthcare records into the application. The ability of the application is verified by examining the file size (that is the number of records). If the healthcare system is efficient, then it can able to upload as much as possible data for processing at a single time. The module will load the patient record and display the total number of records in the database**.** We also browse the data and upload it to the database**.** The GUI of the file uploading option in the healthcare application is shown in Figure-2. The data can be uploaded from the local hard disk, any secondary storage devices, or any FTP server—figure-2 shows, uploading a CSV file, with 1000 records in the file. While uploading the file, the number of documents in the file is counted automatically by the healthcare application, and it will be displayed on the GUI window

.

5. Key Generation

Once the data successfully loaded into the cloud healthcare application, each patient records are encrypted using a blockchain security algorithm. So, an individual key is generated for encryption-decryption. The key generation follows the ECC algorithm, and it will be used to crypt the data. The generated keys are stored in the cloud DB with the corresponding records or DB automatically, and it will be used for future verification. Figure-3 shows the generated key and the encrypted data, where is unreadable and not understandable. And it increases the security level of the cloud data.

Figure-4 is also shown the generated key and the other portion of the data encrypted. The GUI has a navigation button, where it helps to browse the next level of the data. The patient records will be encrypted and stored in the cloud. If the provider needs to know about the patient details, the records need to be decrypted, and it can be downloaded, whereas the key is known only by the owner of the data, not by other third-party people. Hence it is highly secured in providing data security. So, it is accommodated for data security in any secured cloud applications. The backbone of blockchain security is the ECC algorithm, where it so has a proof, famous algorithm, and it can provide a tightened security.



Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?

Key Generation

fffe8608

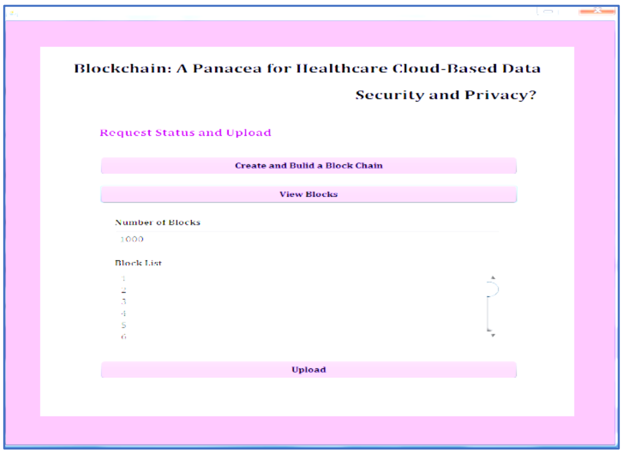
Patient_...	Patient_...	Address	Age	Reason...	Name_...	Final_R...	ekey
35A5C...	BE930...	AA75A...	2CF08...	B513F...	4D2CA...	48DE6...	fffe8608
78656...	B7D54...	A3285...	B7800...	C23A7...	545B0...	82295...	fffe8608
83B22...	933DF...	3A196...	4253A...	B513F...	A2A96...	48DE6...	fffe8608
F7610...	4CF68...	2C909...	85000...	C23A7...	EF8E7...	82295...	fffe8608
7BCFF...	FC29F...	A7948...	117EA...	B513F...	3A9FF...	48DE6...	fffe8608
E4832...	159BC...	0DF06...	6AE84...	C23A7...	545B0...	82295...	fffe8608

Figure-4. Key Generation and Encryption of Healthcare Data

6. Block Creation

Initially, a set of blocks are created and numbered sequentially from 1 to N, N depends on the size of the transaction. After uploading the dataset into the application, it enables the block creation operation and makes a chain for connecting each block created dynamically. All the blocks are connected in a hierarchical chain. The block is used to store the information of the patient details. We can also view the block and upload it to the cloud. The block creation and connection are shown in Figure-5. It is a GUI where it has various buttons to call the functions of creating and build Blockchain, view the blocks, and upload the blocks in the cloud where it shows only the transaction information, not the details. While calling the block uploading function, it automatically asks a location to save the blocks. The user can select a preferred and permanent place to store the blocks. Most of the time, the blocks are stored in cloud space where the HTTP / FTP location is not visible or shared to anybody, even to the data owner.

The next module will display patient records. Each block contains a timestamp and the details of the previous block, and it is shown in Figure-6. The timestamp information about the data blocks is more important where it identified when the transaction had happened from whom to whom.

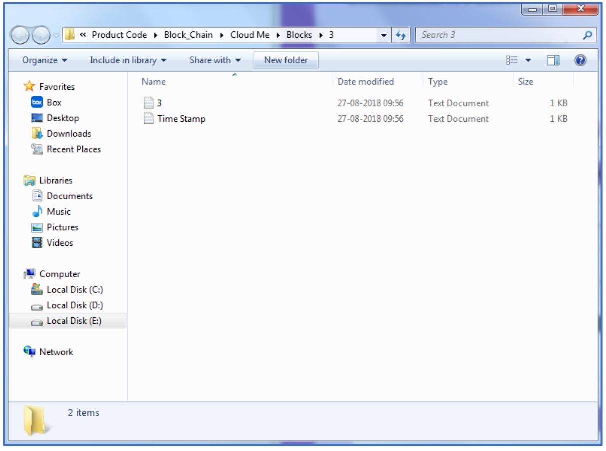


Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?

Request Status and Upload

Number of Blocks
1000

Block List
1
2
3
4
5
6



« Product Code ▸ Block_Chain ▸ Cloud Me ▸ Blocks ▸ 3

Name	Date modified	Type	Size
3	27-08-2018 09:56	Text Document	1 KB
Time Stamp	27-08-2018 09:56	Text Document	1 KB

2 items

Figure-5. Block Creation, Figure-6. Data Storage in Local/Global locations

7. Cloud ID

Every user should create a Cloud ID and use it to identify something with near certainty that the identifier does not duplicate one that has already been, or will be, designed to remember something else. Information that contains Cloud ID can be later combined into a single database or converted in a single-channel, and there will be no conflict between identifiers. Various factors evaluate the performance of the proposed approach. One of the factors is time complexity. The time complexity is calculated in the experiment, and the results compare with the other cryptographic methods. This comparison result is shown in Figure-7. The proposed BC method obtained less time for encryption and decryption. Other methods such as DES, TDES, Blowfish, and AES got little more time for the encryption-decryption process than the proposed BC. But the ADNA method obtained the highest time than other algorithms for encryption and decryption than the proposed BC. Hence in terms of time complexity, the proposed BC received better time complexity for the encryption-decryption process.

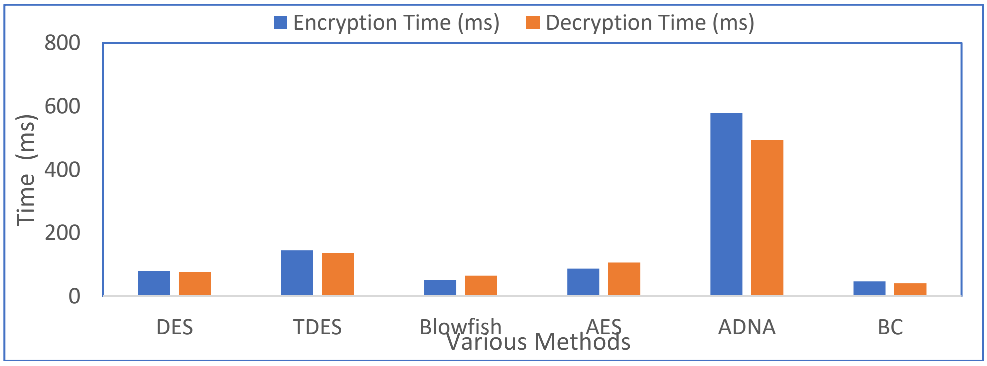


Figure. 7. Time Complexity Comparison Regarding Encryption-Decryption

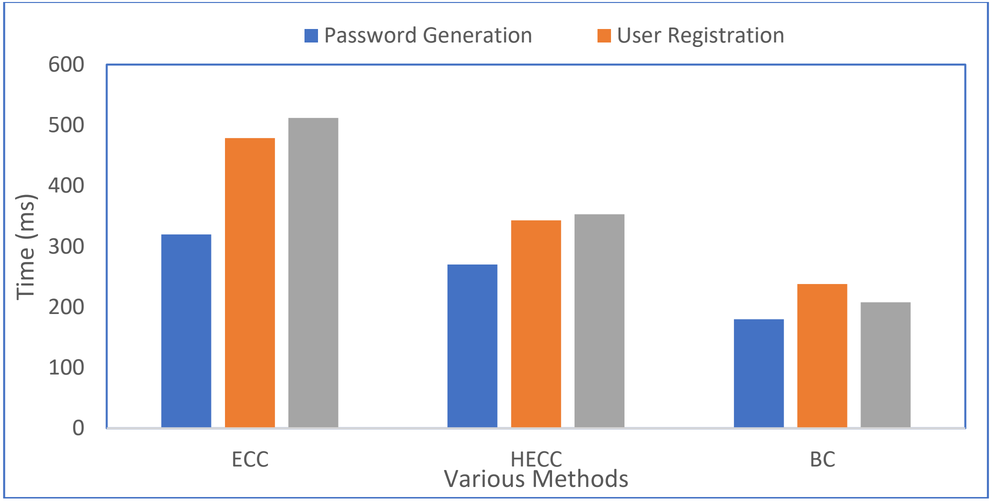
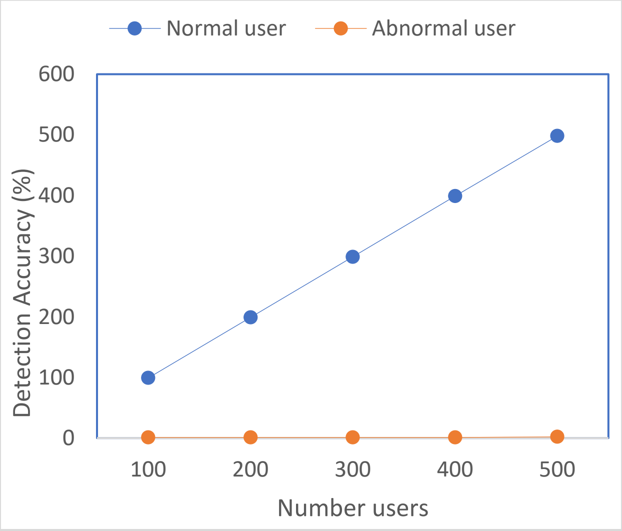


Figure. 8. Time Complexity Comparison Regarding User Activities

Another factor that determines the performance of the proposed approach is a key generation or parameter generation. For verifying and evaluate the performance, similar parameter, or key generation algorithms such as ECC, HECC methods are used for comparison. The proposed BC takes the time for password generation, user registration, and logging into the application are 180ms, 238ms, and 208ms time. It varies slightly depending on the number of bits used in the process. The time comparison for parameter/key generation process comparison is given in Figure-8. From the results, it is obtained that the proposed BC is considered an efficient approach for cloud security.



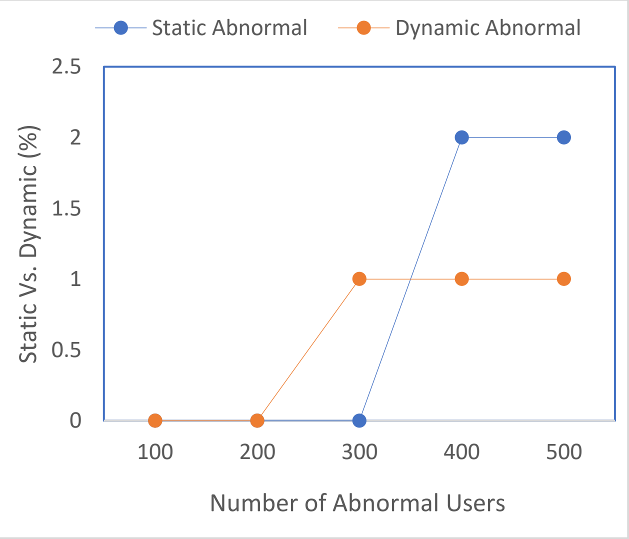
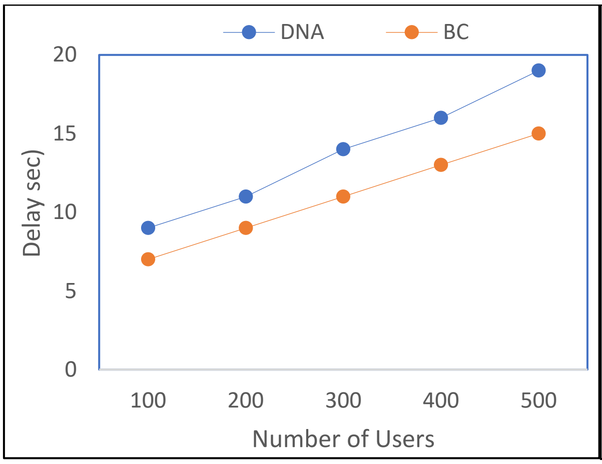


Figure. 9. Cryptographic Analysis, **Figure. 10. Static Vs. Dynamic Analysis**

In the next level, the number of users is changed at each iteration, and the user validation is applied. The number of users examined in each iteration is 100, 200, 300, 400, and 500 in round-1, round-2, round-3, round-4, and round-5, respectively. By examining each user, the abnormal user detection accuracy is predicted using membrane computing in each level of infrastructure. During the first and fifth rounds of the experiment, the proposed approach detected only 3% of malicious users are detected. From the result given in Figure-9, it is clear that the % malicious activity constant to the number of users participated in the cloud. Malicious activity is not only dynamic, but it is also static.

Many users are abnormal users created in the network from the beginning. Hence to identify, static and dynamic malicious activity is identified using membrane architecture simulation. The obtained result from the experiment is given in Figure-10. Comparing all the products with one another, it has determined that the overall % of the dynamic malicious activity is high than the static. Hence, it is clear that any approach which can examine the user data thoroughly in the deployment process itself can control the static malicious behavior. If the static malicious activity is controlled completely, then the % of malicious activity reduced. By design and implement an efficient security model, the dynamic malicious activities can be reduced. Because of the malicious activities, the entire cloud application performance will be degraded. An efficient intrusion detection system can control the dynamic malicious activities and improve the quality of service of the cloud. In this work, some of the QoS factors verified while implementing and experimenting with membrane computing-based security is delay and throughput. One of the QoS parameters is a delay. Time taken to transfer data from one source user (sender) to the destination is called a delay. Another way of defining delay is the time taken to complete one round of cloud operation. Based on this, the delay is calculated, and the obtained result is shown in Figure-11. The obtained delay is compared with the existing decision tree algorithm. From the result, it is identified that the delay increases when the number of users involved in the cloud activities increases.



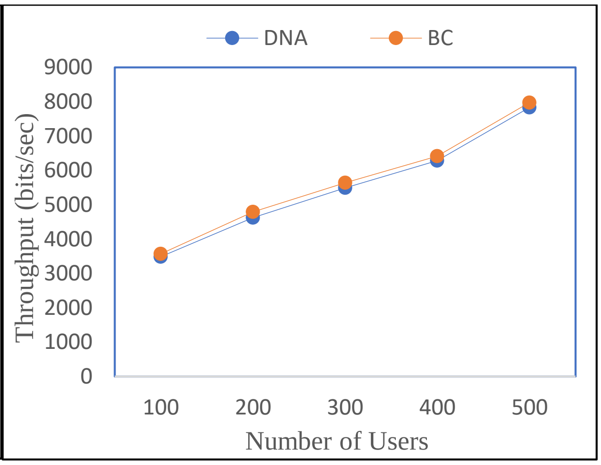


Figure. 11. QoS Regarding Delay, **Figure.12. QoS Regarding Throughput**

Another QoS factor throughput is calculated from the experiment, and it is shown in Figur-12. The throughput is given for both the existing decision tree and the proposed membrane computing. The throughput obtained using membrane computing is higher than the existing decision tree algorithm. Also, throughput increases when the number of users involved in cloud activities increases. From the above discussion, looking into malicious detection rate, classifying malicious types, delay, and throughput, the proposed membrane computing is superior to the other existing methodologies. Hence it is decided that membrane computing is highly suitable for cloud security.

8. Performance Evaluation

The performance of the proposed membrane computing is evaluated by comparing the obtained results with the results using existing systems such as Decision Trees and Membrane computing (MC). The performance factors such as sensitivity, specificity, and accuracy are calculated in the experiment and compared. So, the confusion matrix is calculated. True positive is the number of abnormal users identified correctly as bizarre. False-positive is the number of regular users correctly identified as usual. The real negative is the number of irregular users is not correctly identified as bizarre. False-negative is the number of regular users that are not correctly identified as normal. The confusion matrix is used to compute the inadequate % of accuracy. The rows and columns in the confusion matrix signify the experimental class and expected class, respectively.

Table.1. Performance Evaluation

Evaluation Criteria	**DT**	**MC**	**Proposed BC**
Sensitivity	**95.52**	**97.01**	**98.89**
Specificity	**96.96**	**96.96**	**99.34**
Accuracy	**94.11**	**97.05**	**99.61**

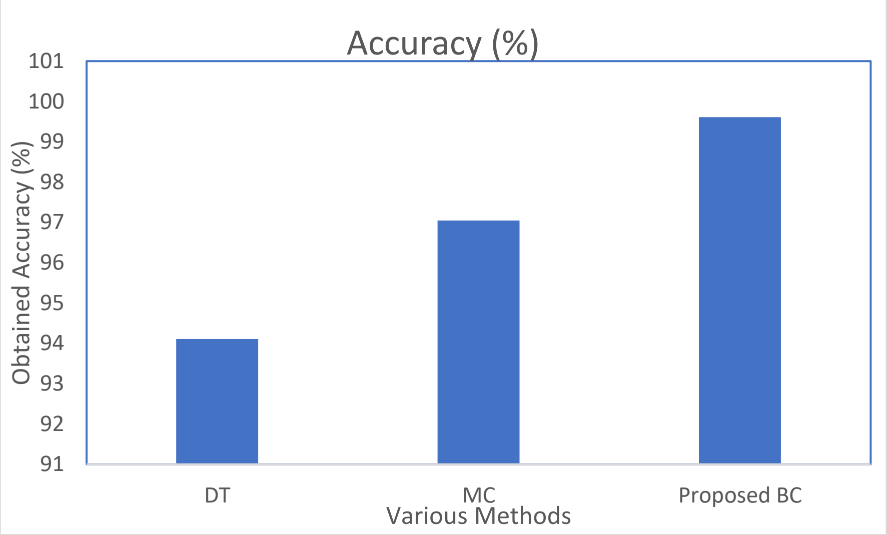


Figure-13. Comparison of accuracy

The comparison of sensitivity, specificity, and accuracy is given in Table-1. From the comparison, it is noticed that BC obtained the highest accuracy in both kinds of classification. To highlight the accuracy comparison alone, Figure-13 shows only the accuracy value obtained using all the three methods. From the comparison, it is identified that membrane computing received high accuracy than the other existing methods. Accurate calculation of accuracy is obtained by repeatedly experimenting with the BC, which is 10-fold cross-validation is carried out. Finally, the accuracy obtained by DT, MC, and BC is 94.11%, 97.05%, and 99.56%, respectively. From the % of accuracy, it is concluded that BC outperforms than the other methods.

Conclusion

This study presents detailed theory and practical information about the BC cryptography method used in this work for user identification and data security. User identification security is obtained by creating strong passwords, and data security is obtained by data encryption and decryption with less complexity. Form the experimental results and discussion, and comparison, it is identified that the proposed BC is highly suitable for user identity security and data security.

References

1. Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang, (2011), “A survey of mobile cloud computing: architecture, applications, and approaches”, Wireless Communications, Vol. 13, No. 18, pp. 1587-1611.
2. https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/
3. Derrick Rountree, Ileana Castrillo, (2014), “The Basics of Cloud Computing”, Book, Science Direct.
4. https://www.guru99.com/cloud-computing-for-beginners.html
5. Rao U.H., Nayak U. (2014) Data Backups and Cloud Computing. In: The InfoSec Handbook. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4302-6383-8_13.
6. Al-khafajiy, M., Baker, T., Chalmers, C. et al. Remote health monitoring of elderly through wearable sensors. Multimed Tools Appl 78, 24681–24706 (2019). https://doi.org/10.1007/s11042-018-7134-7.
7. Evans R. S. (2016). Electronic Health Records: Then, Now, and in the Future. Yearbook of medical informatics, Suppl 1(Suppl 1), S48–S61. https://doi.org/10.15265/IYS-2016-s006.
8. Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: A survey. Journal of Healthcare Engineering, 2019.

9. Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Rodrigues, J. J. (2018, December). BHEEM: A blockchain-based framework for securing electronic health records. In 2018 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.

10. Zhang, A., & Lin, X. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Journal of medical systems, 42(8), 140.