Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 8882 - 8893
Received 25 April 2021; Accepted 08 May 2021.

A Persuasive Rabbit Algorithm Enhanced with Map Reduce Security Mechanism for ECG Data Security in Cloud Storage

Sreehari Kundella[1]*, R.Gobinath[2]
[1]*Research Scholar, Department of Computer Science, VISTAS, Chennai, India.*
[2]*Department of Computer Science, VISTAS, Chennai, India*
**kundella.sreehari@gmail.com*
drgobinathramar.scs@velsuniv.ac.in

ABSTRACT

The present trend of adopting big data technologies in medical sectors, to digitize their workflow by moving electronic records of their patients becomes an architype shift in the field of healthcare. As there is a continuous growth in quantity of clinical data storage and it is easily adopted using big data, still they have challenges and barriers while maintaining sensitive health information in cloud computing. There arises the necessity of providing strong prevent measures against security breaches by developing Persuasive encryption security schemes to protect from invaders. There are many encryption models are already available but implementing them increases the computation complexity, time complexity and resource utilization is also very high. To overcome this issue, in this paper a Persuasive Rabbit algorithm enhanced by MapReduce based Encryption is developed to preserve the ECG data stored in cloud. This proposed model is a light weight cryptographic model which uses very limited resources, shares very less memory and the computation as well as time taken is also very less compared to the other conventional encryption scheme. Thus, the proposed MapReduce + Rabbit algorithm provides security at high level against any kind of security breaches. The ECG Big data is effectively handled by the MapReduce and it performs the encryption in parallel manner to assure the shortest processing time. The simulation results evidence the performance of the proposed algorithm is superior in time consuming, accurate validation and provide better performance than the traditional algorithms.

Keywords: ECG, Security, Big data, MapReduce, Rabbit Algorithm, Encryption, Cryptography

I. Introduction

In this modern era, the advancement in IT field have exponentially increased the production rate of data. Most of the organizations highly demand efficient solutions to store and analyze its big volume of data which are generated from various other resources like sensors, instruments or other devices connected to the system. The big data can use the benefits offered by cloud computing like virtual resource utilization, connect, store in cloudlets and assemble tools automatically. These factors make the organization to meet their goal easily by developing the services of cloud. These advancements are also extended as a great helpful for the health informatics field to collect, manage and use patient's biomedical information to improve the efficiency and quality of medical care. But, transmission of increasing volume of health information results in ethical safety anxieties associated to privacy of patient's health details [1].

Monitoring heart rate continuously and detection of heartbeat immediately are the primary anxieties in modern health care system. Many of the arrhythmia can be better controlled, diagnosed and preventing by monitoring continuously and analyzing ECG signals. The shift in storage paradigm which adapts the cloud computing is increasingly giving rise to security and privacy factors associated to facets of cloud storage and computing in terms of trust, accountability and loss of control. The health information is very sensitive, so strong preventive measureshas to be taken while storing ECG data in cloud to avoid breakdowns in data protection and security breaches.

For security communication over the internet, the encryption algorithms are used to protect the confidentiality of the sensitive information [2]. The encryption algorithms are either heavy or light weighted. The heavy weight algorithms like RSA, AES, and Blowfish will take more computing time and more resource utilization. So, this paper aims to develop a light weighted encryption algorithm which takes less time for encryption and offers better security compared to the existing heavy weighted algorithms RSA, AES and Blowfish. This research concentrates on constructing MapReduce based security mechanism to improve the ECG data security in cloud computing.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 8882 - 8893
Received 25 April 2021; Accepted 08 May 2021.

The ECG Data is a big data, while using conventional cryptographic algorithms it will increase the computation complexity and the time taken, to overcome this issue we have integrated the light weighed cryptography with MapReduce for effective security mechanism.

II. Related Work

Smita Sharma et al [3] in their work constructed a novel symmetric algorithm with different file size and any type of file stored in cloud. It works in bit level of data with different keys are used for each encryption but for decryption only option is used for secure cloud storage.

Arivazhagan and Kirubakaramoorthi[4] this work focuses on the implementation of cloud security and limitation relevant to cloud based secured schemes. The authors performed a deep investigation on anonymity, protecting confidential data from unauthenticated persons. Need for secure cloud data handling, abandon the strains of applying cryptographic procedures in cloud with the accepted expectation of the cloud users.

Fursanet al [5] designed a lightweight method for reducing the time complexity and maintaining the sensitivity of key using image histogram, statistical analysis and change in entropy for providing strong and secured cloud storage.

Ahmad and Garko[6] performed a deep study about hybrid cryptography models by considering the user friendly and in-depth survey to understand the merits and demerits of symmetric and asymmetric cryptographic models by providing clear guidelines to the new researches about the security mechanism.

Nooh[7] in this work thee main factors are considered to provide security and privacy of data stored in cloud paradigm. This work states that storing the data in cloud storage platforms like Amazon, Cloudsim, and Google Drive as encrypted format will help to maintain the confidentiality, integrity and availability of the sensitive data more effectively. This work used symmetric key cryptography with Amazon S3 space for securing confidential data in cloud.

Thirupalu et al [8] in their work discussed conducted a wide survey on symmetric and asymmetric cryptographic algorithm used to assure the confidently of the cloud data. The proposed a novel public key-based cryptography to maintain the security of the data stored in cloud paradigm.

Pansotraet al [9] reported in their work about the importance of security while storing data in cloud computing or other open sources. The flexibility of storing confidential data in cloud can be accomplished by cryptographic models, thus in this work they discussed about the various symmetric and asymmetric algorithms are explained in detail.

Gangireddyet al [10] they introduced a clustering-based security mechanism for the data stored in cloud. The different types of data such as messages, pictures and texts are stored in cloud but they cannot provide complete trusty to the authorized services. So, to enhance the security of cloud data, a novel cyber security based on k-medoids clustering is developed to cluster the confidential data using data distance measure along with dragonfly algorithm to improve its clustering performance.

Alabdulatif et al [11] designed a fully homomorphic encryption scheme to protect the sensitive data and reduce the computation complexity. The data is partitioned into subsets and encrypted using homomorphic encryption and maintained in cloud to improve the security of data. They used fuzzy clustering and hard clustering to group the similar data and finally fully homomorphic encryption is applied on each subgroup.

Raju et al [12] devised a group key-based encryption to provide better encryption using Fibonacci-Lucas which generates the quantum signature for verifying the confidentially of the data. They improved the security mechanism by improving the process of signature verification and information verification of the users with minimal delay in processing.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 8882 - 8893
Received 25 April 2021; Accepted 08 May 2021.

III. Methodology: APersuasiveRabbit algorithm enhanced with MapReducesecurity mechanism to improve the ECG data security in cloud computing

The proposed model provides a secure storage of ECG big data in cloud by developing Persuasive Rabbit Algorithm enhanced by adapting MapReduce scheme (MapReduce + Rabbit). The security of ECG data is ensured by developing a light weight encryption model which integrates Rabbit Algorithm and MapReduce to effectively reduce the computation complexity and time taken. The detailed description of the proposed MapReduce + Rabbit encryption scheme is discussed in the following section to preserve the confidentially of ECG dataset [15, 16]. Rabbit algorithm is a light weighted encryption scheme comprised of steps of processing which is explained in the paper detailed. In this paper the conventional rabbit algorithm is enhanced by integrating the knowledge of MapReduce.Before uploading the ECG data it encrypted using MapReduce and Rabbit encryption scheme and using Google Cloud Console, the bucket is created to store the encrypted files in cloud.

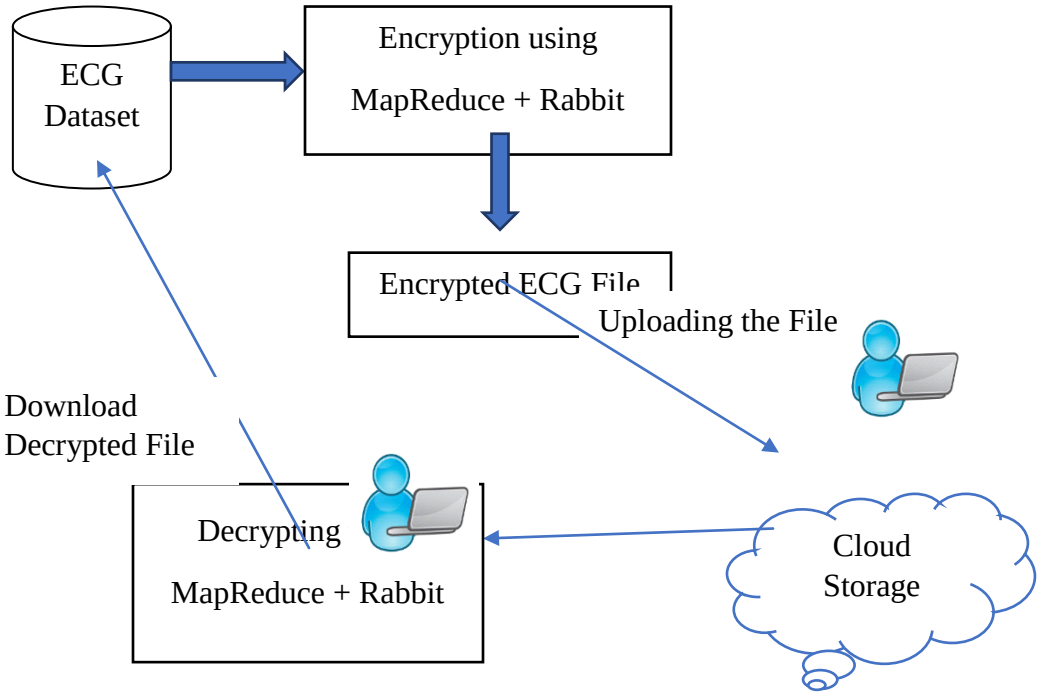

Figure1:Framework of Rabbit algorithm enhanced with MapReduce mechanism to improve cloud data security

Rabbit Algorithm

The rabbit algorithm is very compact for encryption and decryption of confidential messages which offers a strong non-linear mixing of the inner state among two iterations [13]. It uses 128 bit as secret key is used for encryption along with the original message as shown in the figure 1.The keys are used for encrypting and decrypting the files which will be shared among the authenticated users. The output block is generated during each iteration with 128

random bits of the internal state bits. By applying XOR's peration for both encryption and decryption to convert plain text to cipher text and vice versa respectively. The internal state size is divided into 513 bits portioned as state variable with 32 bit, eight counters with 32 bit and a single carry bit for counter. The eight coupled non-linear function is used for updating state variables. The state variables length of period secured at its lower bound by counters. The main part of this algorithm is to generate cipher as a big stream by encrypting 128 message bits for each iteration. Depending on the strong mixing in inner states among two successive iteration which incrases the cipher strenght. The mixing function uses the g-function related to arithmatical squarings, XOR, bit wise rotation and modulo 2 addition.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 8882 - 8893
Received 25 April 2021; Accepted 08 May 2021.

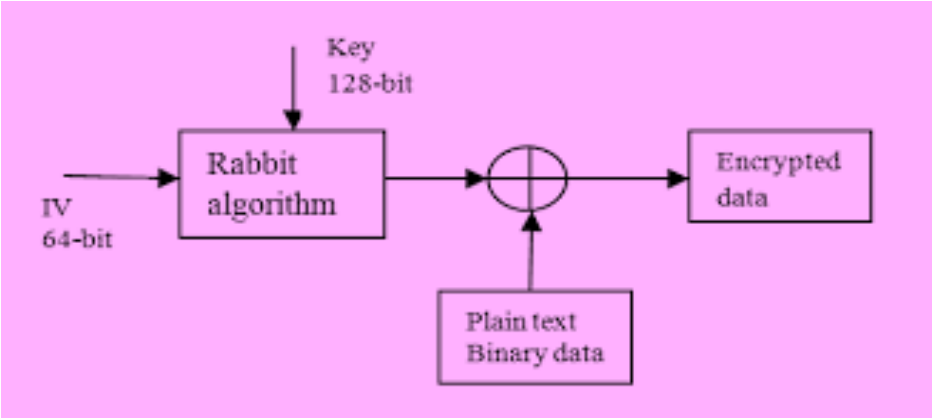

Figure 2: Basic Function of Rabbit Algorithm

In Rabbit Cryptography it is comprised of four main tasks they are key setup scheme, IV setup scheme, nest state funtion and Extract scheme.

- In key setup it uses 128-bit key which is partitioned into eight chunk of sub keys each of 12-bit length. These sub keys are used for state and counter variables using permutation operation. In order to reduce the correlation among bits in the key as well as state variable, the system is iterated four times.
- IV setup involves in updating the counter state function by applying XOR in 64 bits IV on all the counter variable of 256 bits
- Next state function is the core of the rabbit cryptography as it verifies the correct mixture of bits of IV using the state and counter register values.
- Counter System: This function updates the values of the counter register by summing the all the counter register's current state with a constant and carry bit value.
- Extraction: It is the final function which uses XOR operation is applied on various state registers to construct eight 16-bit key stream register. These key bits are XORed with plain text to generate the cipher text.

Algorithm:
Input: Plaint Text PT
Output: Encrypted Data
Procedure

- Generate key 128 bit
  The key is loaded in C_i and X_i registers
- Generate Initialization vector (IV) 64 bit
  CKS = IV XOR C_i
  The operation performs left rotation CKS <<< CKS on state values
- Generate Cipher Text by XOR plaint text PT with CKS (key 128 bit + IV 64 bit)
  CT = PT XOR CKS

The detailed workflow of Rabbit cryptography is depicted in the figure 2.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 8882 - 8893
Received 25 April 2021; Accepted 08 May 2021.

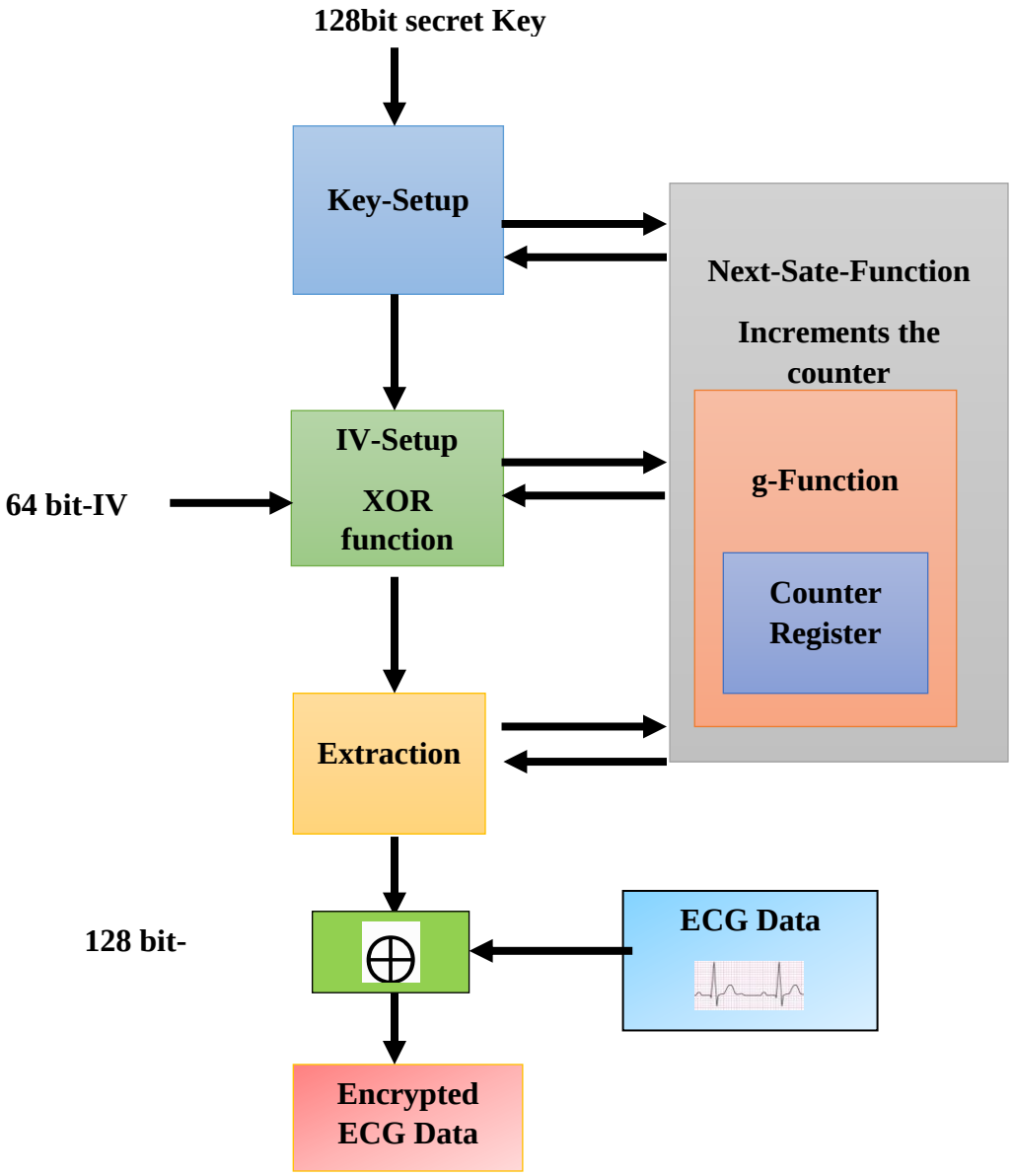

Figure 3: Workflow of Rabbit Encryption Algorithm

IV. **ECG Data Security usingMapReduce**

MapReduce is a kind of programming approach used in distributed process of big data in an effective and fault tolerance manner either in private or public cloud [14]. It is inherently parallel, so that it can handle any volume of big data. MapReduce comprised of two functions they are mapping and reducing. These two functions take input as set of key value pair and generates the output as another key-value pairs. The map receives input key-value pair and generates a pair of intermediate key-value pairs which are in the binary format. In Reduce function it groups all the intermediate values together with their corresponding keys and passed as output. The simple operation of the MapReduce is shown in the figure 3.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 8882 - 8893
Received 25 April 2021; Accepted 08 May 2021.

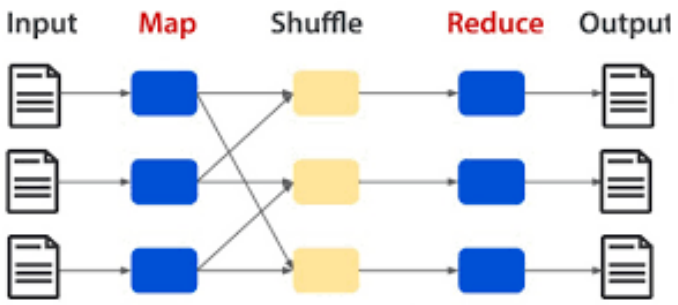

Figure 4: Simple Framework of MapReduce

In detail the frame work of the MapReduce with map, shuffle and reduce fucntion is depicted in the figure 4.

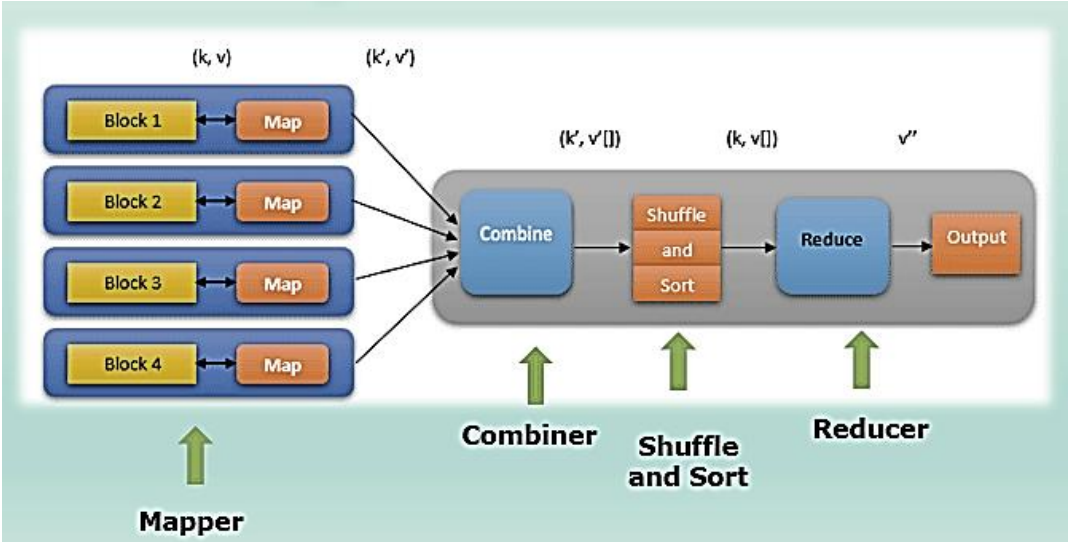

Figure 5: MapReduce Working Principle with Mapper, Shuffle and Reducer Function

The function Map(k',v') is the intermediate value of input k key and v value which works in a parallel manner on each input dataset. The shuffle function, redistribtues the data depending on the output keys by combining all the data which belongs to a single key is passed to the reducer. The Hashing based key distribution alogrithm is applied for performing this. Finally, in reduce funciton (k,v[]) is applied to each valur for a specific key and generates a group of vlaues v'' for each key as output.

MapReduce Algorithm

Map(Key K, Plain Text PT)

For each word (wd) in PT

Emit-Intermediate (W, 1)

Reduce (key K, Iteration-val iv)

Int res = 0

For each I in iv

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 8882 - 8893
Received 25 April 2021; Accepted 08 May 2021.

res = res + ParseInt(iv)

Emit(asString(res))

V. Persuasive Rabbit Algorithm Enhanced using MapReduce Security Scheme

In this proposed work the light weight encryption model Rabbit Algorithm is enhanced by integrating the knowledge of MapReduce to provide security on ECG Data [15, 16] stored in Cloud. The big data of ECG is processed by converting them to blocks of 128 bits, it is accomplished by partitioning the block of data to two parts, then it partitions the first part into multiple blocks of 64 bit each and each block undergoes set of process like secret key, IV process, applying next state value and extraction operation. Finally, the extracted block is XOR with ECG data to generate cipher text or encrypted data as illustrated in the figure 5.

The MapReduce scheme ensures the parallel encryption which will be very effective for ECG big data which will greatly improve the performance with less time consumption and resource utilization, because the conventional encrypting models performs block by block process, while the MapReduce with its multiple mapper can certainly process different blocks encryption process at a time. Finally, the reducer will combine all the blocks and generate as a single encrypted data. To achieve strong results different keys can be involved for each individual block or else for simplicity same key can be used to encrypt entire blocks. But using more keys will reduce the performance of the decryption process so in this work only same key is used for encrypting all the blocks.

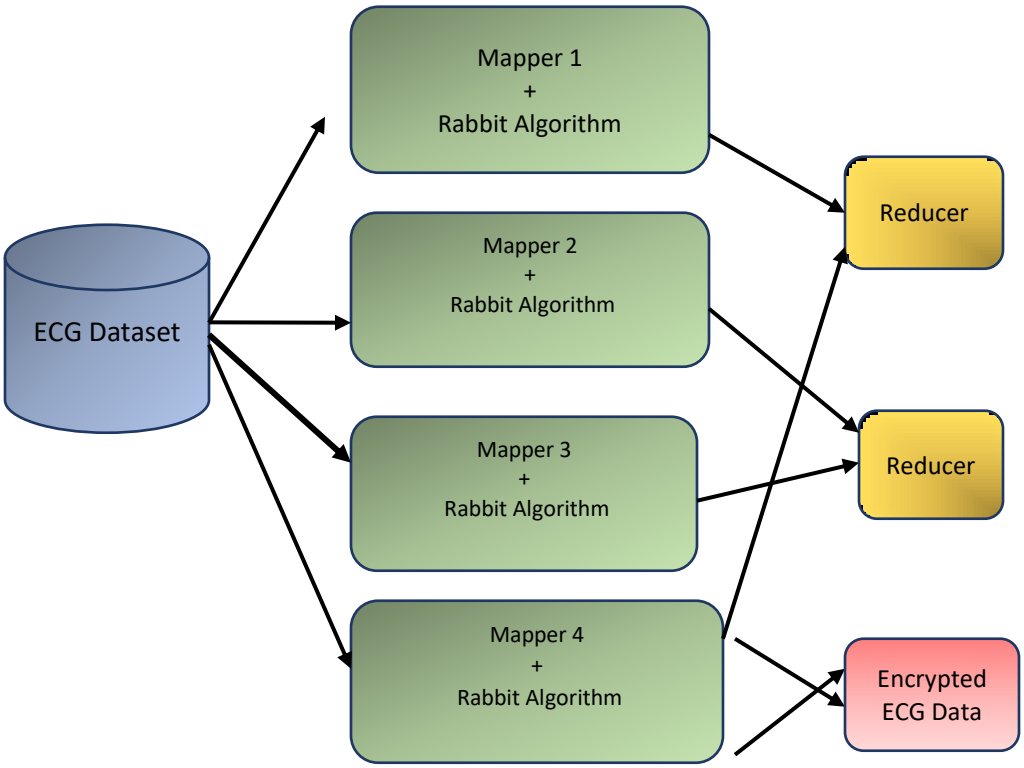

Figure 6: Persuasive Rabbit algorithm enhanced with MapReduce Security Scheme

The mapper takes key – value<blk-id, Edata> pair as input, whereEdata is considered as ECG data and block id is used as key to identify the block uniquely.

The mapper generate the output in the form of <blk-id,CEdta> where CEdata is the encrypted ECG data. While the reducer will receive the input and store them as a continuous block. The number of reducers used will related to the number of keys being used in encryption and data size.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 8882 - 8893
Received 25 April 2021; Accepted 08 May 2021.

Once the task of mapping process is completed, the output produced buy mapper will be copied in memory buffer of reducer. When the map output reaches its threshold value then it is combined and stored in the disk. In the reduce phase, it should retain the mapper output. The percentage of heal memory depends on the input and output accessing of the local disk. Depending on the length of the resource the number of reducers is assigned.

A Persuasive Rabbit algorithm enhanced with MapReducesecurityAlgorithm

- Input file IF
- Spilt the IF into chunks IF = ($f_{1,}$ f_2,…f_n)
- Apply Rabbit Algorithm on each data chunk to generate cipher text
    - CT(IF) = RBA(f_1), RBA(f_2),… RBA((f_n)
- Apply MapReduce on Each Encrypted file

  MP (key, value) = Mapper(CT(IF))
- Store the crypted file in cloud

VII. Results and Discussions

The efficiency of the proposed Enhanced Rabbit Cryptography with MapReduce to provide security on ECG dataset [15, 16] stored in cloud is developed using python code. Using the Python Google storage library to upload files and also download ECG files. The performance of the proposed MapReduce+ Rabbit security model is compared with other cryptographic models such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish. The evaluation metrics used for examining the performance are Processing Time, Encryption Time, Decryption Time and Accuracy of validation.

Table1:Performance Comparison based on Security Models

Security Models	Processing Time	Encryption Time	Decryption Time	Accuracy
DES	262	60	58	52.62
AES	255	58	52	64.25
Blowfish	178	46	45	73.48
MapReduce + Rabbit	95	15	12	98.27

Table 1 depicts the detailed evaluation results of the four different security models to protect the confidentiality of the ECG data stored in cloud storage. The outcome of the result reveals that the proposed Enhanced Rabbit Cryptography with MapReduce (MapReduce + Rabbit) produce less processing, Encryption and Decryption time because they are light weight cryptographic model, which takes less computation with minimum arithmetic operators and the logic of mapping and reducing reduces the complexity of the model with limited usage of resources. The accuracy is also very high compared as it discovers the genuinity of the user more obviously. The DES model takes more processing time, encryption and decryption time. The accuracy of validating the authenticated users is also very less compared to all other security schemes.

Processing time = Time taken Complete execution of the algorithm

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 8882 - 8893
Received 25 April 2021; Accepted 08 May 2021.

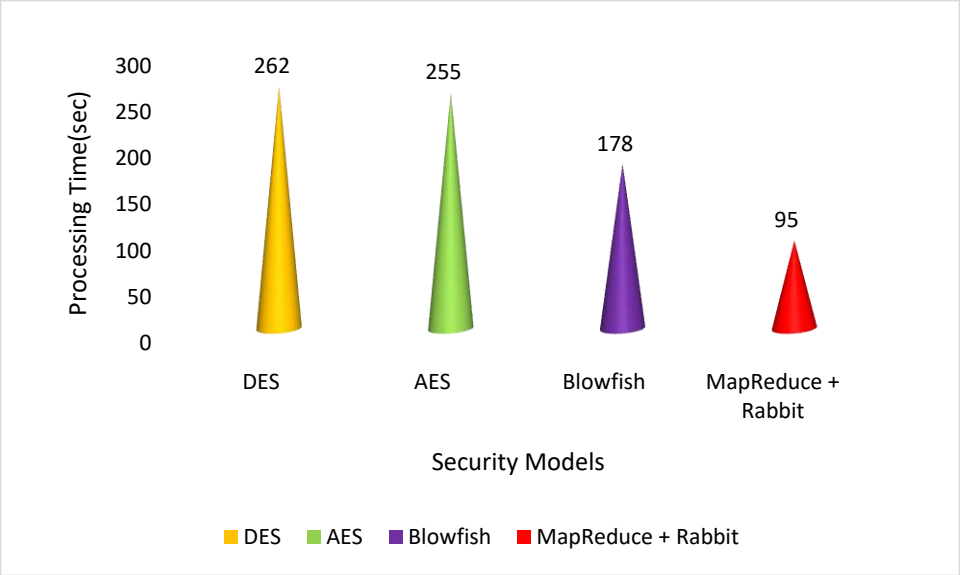

Figure 7:Performance Comparison based on Processing Time

The figure 6 illustrates the performance of the four different security models which provides security to the ECG Dataset. It is proved that the proposed MapReduce based Rabbit algorithm takes very less processing time while comparing with other three security models namely DES, AES and Blowfish. This is because the Rabbit algorithm itself is a light weight cryptography when it is passed to the mapping and reducing function then it consumes less resources and the time taken for processing the entire ECG dataset is very least with other standard security schemes.

Encryption time = Time taken for Encryption of the ECG Data

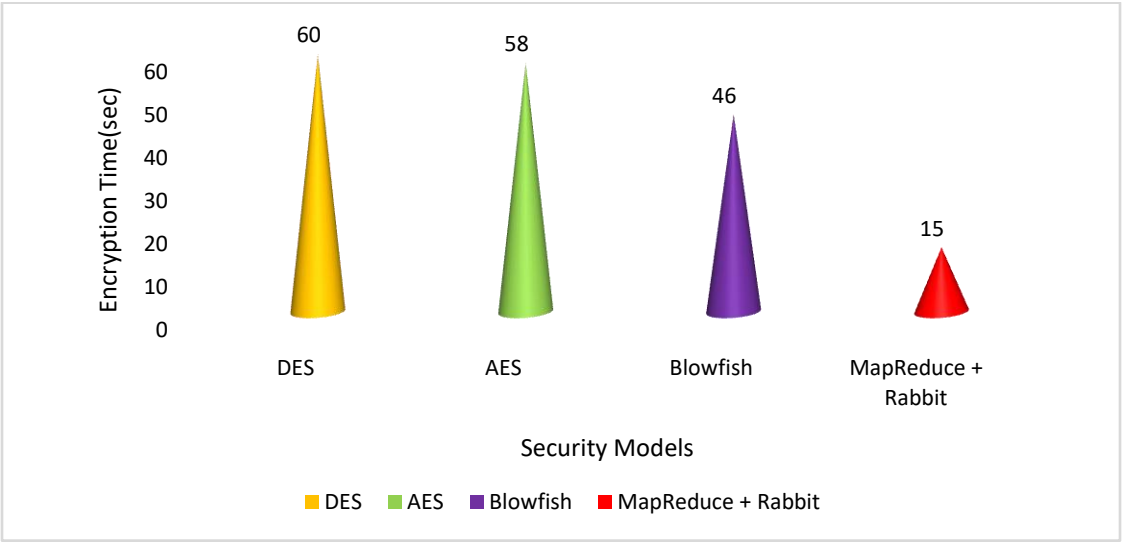

Figure8:Performance Comparison based on Encryption Time

The figure 7 depicts the time taken of encrypting the ECG dataset using four different encryption algorithms. The Enhanced Rabbit encryption model combined with MapReduce approach reduces the physical size, limitations of memory, less consuming of energy and overall processing is also reduced by just involved simple arithmetic operations to convert plain text to the cipher text. While using the conventional encryption models like DES, AES

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 8882 - 8893
Received 25 April 2021; Accepted 08 May 2021.

and Blowfish, they consume more resources with low throughput, while handing big data such as ECG data in cloud storage.

Decryption Time = Time taken for Decryption of the ECG Data

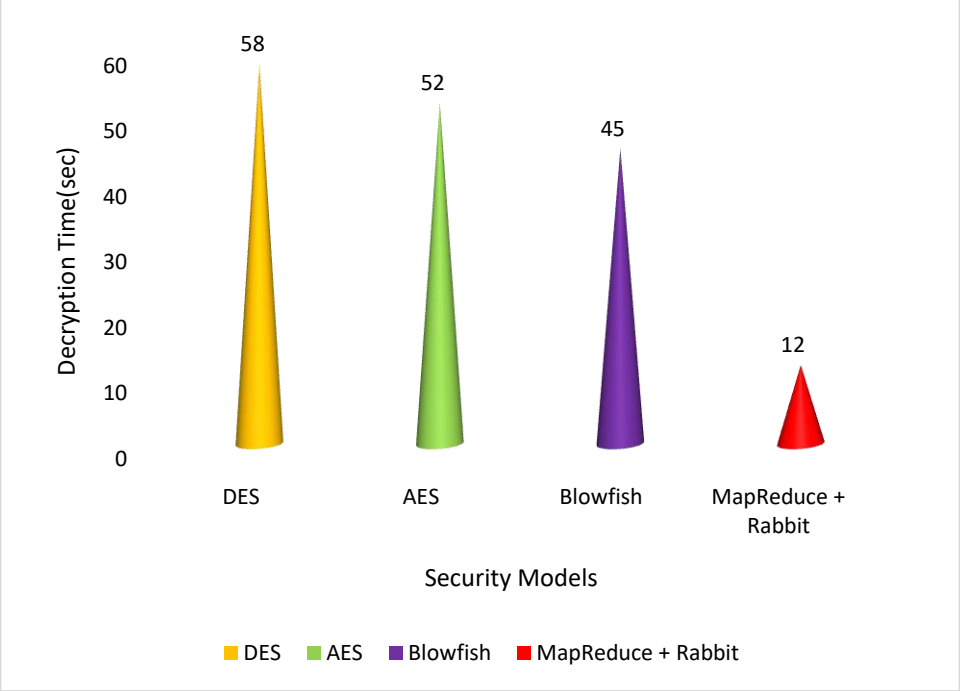

Figure 9: Performance Comparison based on Decryption Time

The figure 8 explores the decryption time taken by DES, AES, Blowfish and proposed Enhanced Rabbit cryptography with Map Reduce (MapReduce + Rabbit). The decryption process of MapReduce + Rabbit is done in a parallel manner, hence its decryption time taken is also very less compared to the other conventional models. Because AES, Blowfish and DES undergoes so many permutation processes with high computation complexity they take more decryption time while handling huge volume of ECG dataset.

Accuracy = No. of Correctly Authenticated/ Number of Attempts

The Accuracy of verifying the authentication of genuine and imposters are prominently detected by the proposed MapReduce+ Rabbit security scheme as shown in the figure. While comparing with the conventional symmetric key cryptography algorithms, the proposed model is light weighted and provide strong security by functioning in a parallel manner and generating key value pair during each iteration as intermediate values. Thus, the proposed model produces highest accuracy rate while comparing the other models.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 8882 - 8893
Received 25 April 2021; Accepted 08 May 2021.

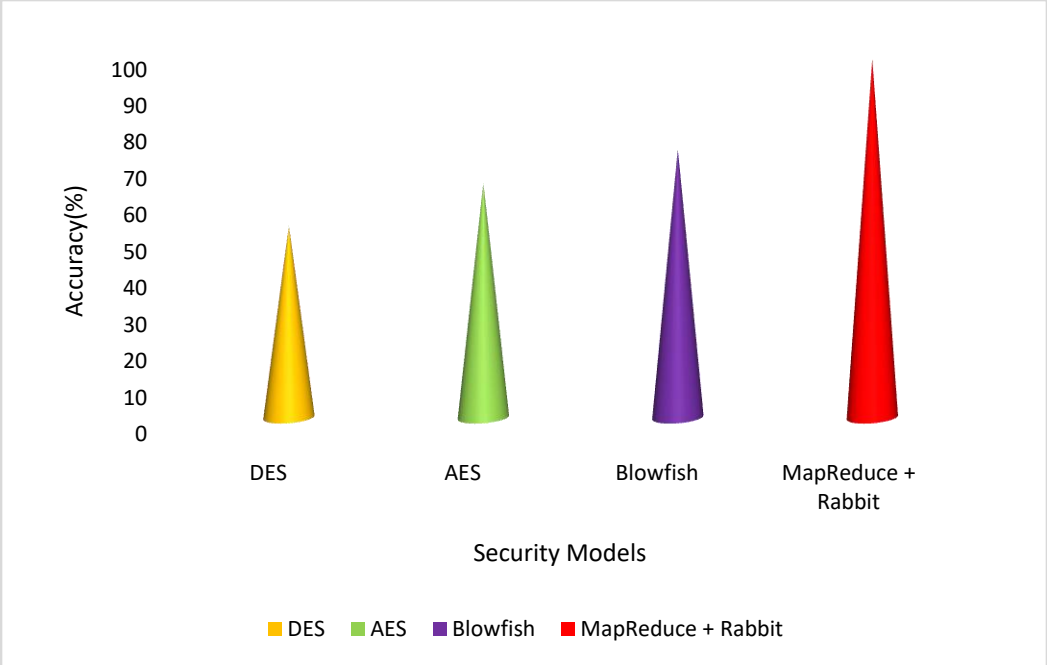

Figure 10:Performance Comparison based on Accuracy

VIII. Conclusion

In this work a Persuasive security model is constructed with the objective of reducing the computation complexity and time complexity along with improved security on ECG data stored in Cloud paradigm. The lightweight algorithm Rabbit cryptography is used for its simplicity and strength to provide strong security on sensitive data with its simple arithmetic operations such as XoR and counters. The Persuasiveness of the rabbit algorithm is enhanced by adapting the MapReduce scheme which works in a parallel manner to boost the encryption process of rabbit algorithm in terms of minimal execution time and resource utilization. Unlike the traditional cryptographic algorithm which consumes more time, computation is high, resource utilization like memory space is high when the key size and handling ECG big data, whereas the proposed model with its ability of parallel processing the strong security is provided to the sensitive information of ECG data more prominently, as ensured in the outcome of the comparison analysis.

References

1. Adluru, Pradeep, SrikariSindhooriDatla, Xiaowen Zhang. Hadoop eco system for big data security and privacy." In Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island, pp. 1-6. IEEE, 2015.
2. Gupta NK (2018) Advancements in cloud computing software testing research. In: 4th int'l conf. on recent advances in information technology, RAIT-2018
3. Smita Sharma, R.P. Singh, The Cryptography Based Security Algorithm for Protecting Sensitive Information in Cloud Environment, International Journal of Scientific & Technology Research, Volume 8, Issue 11, November 2019
4. D. Arivazhagan, R Kirubakaramoorthi, Develop Cloud Security in Cryptography Techniques Using DES-3L Algorithm Method in Cloud Computing, International Journal of Scientific & Technology Research, Volume 9, Issue 01, January 2020
5. FursanThabit,SharafAlhomdy,SudhirJagtap,Security Analysis and Performance Evaluation of a New Lightweight Cryptographic Algorithm for Cloud Computing Environment,GlobalTransitionsProceedings(2021)
6. S. A. Ahmad and A. B. Garko, "Hybrid Cryptography Algorithms in Cloud Computing: A Review," 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, Nigeria, 2019, pp. 1-6.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 8882 - 8893
Received 25 April 2021; Accepted 08 May 2021.

7. S. A. Nooh,Cloud Cryptography: User End Encryption,International Conference on Computing and Information Technology (ICCIT-1441), Tabuk, Saudi Arabia, 2020, pp. 1-4, 2020
8. U. Thirupalu, Dr. E. Kesavulu Reddy, E. Spandhana, Security Analysis of Cryptographic Algorithms in Cloud Computing, International Journal of Engineering Research & Technology (IJERT) Volume 07, Issue 10 (October – 2018),
9. Pansotra, Singh, Simar Preet, (2015). Cloud Security Algorithms. International Journal of Security and Its Applications. 9. 353-360. 10.14257/ijsia.2015.9.10.32.
10. Gangireddy, V.K.R Kannan, S. Subburathinam, K, Implementation of enhanced blowfish algorithm in cloud environment. J Ambient Intell Human Comput (2020).
11. Alabdulatif I, Khalil I, Yi X,Towards secure big data analytic for cloud-enabled applications with fully homomorphic encryption. J Parallel DistribComput 137:192–204, (2020)
12. Raju UN, Vivekanandam, E-commerce security by quantum digital signature-based group key management. In: Innovations in computer science and engineering, LNNS, vol 74. Springer, New York, pp 251–262, (2019)
13. Khaled Suwais, "Parallel Model for Rabbit Stream Cipher over Multi-core Processors" Volume 11, 2014 WSEAS Transactions on Information Science and Application
14. X. Zhang, C. Yang, S. Nepal, C. Liu, W. Dou, and J. Chen. A MapReduce based approachof scalable multidimensional anonymization for big data privacy preservation on cloud, International Conference on Cloud and Green Computing, Karlsruhe, Germany, September 30 -October 2, 2013, pages 105–112, 2013
15. Moody GB, Mark RG. The impact of the MIT-BIH Arrhythmia Database. IEEE Eng in Med and Biol 20(3):45-50 (May-June 2001). (PMID: 11446209)
16. http://archive.ics.uci.edu/ml/datasets/Arrhythmia