How to Cite:
Abraham, A. T., & Fredrik, E. J. T. (2022). Ensuring the security and balancing the load in the cloud computing by DCRI-RI hybrid method. *International Journal of Health Sciences*, *6*(S2), 9776–9793. https://doi.org/10.53730/ijhs.v6nS2.7559

Ensuring the security and balancing the load in the cloud computing by DCRI-RI hybrid method

Abin T Abraham
Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India
Corresponding author email: abysid@gmail.com

E. J. Thomson Fredrik
Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India
Email: thomson500@gmail.com

***Abstract*---**In the cloud environment, the confidentiality of data is improved by protecting the cloud data from unauthorized user access. During data communication, the balancing of load across cloud servers helps to maintain the cloud service's reliability. Through intrusion detection, the performance of secured data communication is enhanced in a significant way. Some techniques were developed in the field of cloud computing to provide secure communication between the cloud server and cloud user. These developed techniques failed to improve the security and load balancing efficiency simultaneously during the data transmission on a cloud. There is no sufficient algorithm in the present situation to detect the intrusions and to provide improved results in the load balancing. In this research work we propose a novel "Dynamic Certificateless Random Identity (DCRI)" algorithm for ensuring cloud security and a "Rank-Indexing (RI)" algorithm based on weightage for load balancing. Our proposed DCRI-RI hybrid method will ensure a better rate of intrusion detection with higher load balancing efficiency. The DCRI algorithm is relied on a cryptographic concept based on advanced encryption and decryption signature authentication process performed on both cloud server and user end to detect and remove the unauthorized users in a significant way. The RI algorithm is implemented to successfully improve the load balancing efficiency by balancing the load across multiple servers in a rank/weight-based indexing way. Through this, the data communication is attained with a better confidentiality level and load balancing efficiency through the proposed DCRI-RI algorithms. The performance metrics of Intrusion-Detection-Rate (IDR), Load-Balancing-Efficiency (LBE), and Data-Accessing-Time (DAT) were better in DCRI-RI when compared with the existing work "Binomial

Protection based Authentication with a Stochastic Agent-based Load Balancing (BPA-SAB)" technique.

***Keywords*---**cloud environment, security, load balancing, cryptography.

Introduction

Cloud Computing (CC) is a combination of services and databases which are accessible through the web or any private network. In addition, the CC is also enabled to deal with physical infrastructures by virtualization [1]. The service load in CC is dynamically altered concerning users' service requests. Many organizations namely, research centers and enterprises employ cloud computing for performing the respective applications. In CC the security, confidentiality, and privacy problems are extensively considered for protecting the cloud storage from unauthorized users [2].

The users lacking accession to physical infrastructure in CC causes security and privacy restrictions. The Cloud-Users (CU) stores the data in public Cloud-Servers (CS) which gets exposed by intrusion attacks or unauthenticated users leading to confidentiality violations [3]. Encryption of data is performed before storage at cloud provider to resolve confidentiality issues. Authentication is to be ensured as it influences the reliability of the CC environment. Secure data storage is attained through the identification of malicious attacks [4].

Authentication is the method for authorizing the identity by enabling the system to recognize the user through a username and legalize their identity through a password. Certificates, One-Time Passwords (OTP), and Fingerprinting are some of the efficient approaches of user authority with enhanced integration of authentication aspects. The identity of users is essential during communication with the cloud for maintaining security, visibility, and control [5]. In a distributed environment, there is a requirement for applications to validate the user's identity, recognize the authority of the user for producing, updating an account, and assessing their actions. Both validation and authorization are significant for the cloud identity approach to increase portability and extensibility. The users are requested to complete the user authentication procedure during the accessing of cloud service in CC.

The cloud resources for registered people, software practices, or other systems are provided with Identity-Administration by the "Identity and Access Control Service" [6]. For attaining an appropriate level of access, the identity of the user is legalized and an authentication procedure is performed for initiating the authorization process. In addition, an audit logging method is employed for the detection of successful and misleading functions concerning authentication. Various encryption mechanisms are also used for encoding data with the aid of cryptographic algorithms for increasing confidentiality. This increases the privacy of sensitive and private data by enabling only authorized users to decode it [7].

In CC, cryptography utilizes encryption methods for securing the stored data in the cloud. Cryptography enables the users to suitably and securely access the allocated cloud services through the preservation of data with encryption by cloud providers. In addition, Cryptography also protects sensitive data without causing communication delay and helps in securing sensitive data. Signcryption schemes are employed to ensure confidentiality and authentication through the integration of public-key encryption and digital signatures for superior performance and security [8]. In Cryptography, the original message is applied with an encryption technique that transferred it into cipher-text by performing certain conversions and replacements with the aid of a secret key. Then, the ciphertext is converted plain-text which by a decryption algorithm through a secret key. The accurate replacements and transformations executed by the respective algorithm are based on the key [9].

Load-Balancing (LB) is a method that allocates the workload on the resources of a node to the corresponding resources on the other node without the restriction of any running functions. The balancing of load among different nodes is a demanding task in the CC scenario. The loads are of different categories namely, network load, memory load, CPU load, and delay load. The LB is also essential for allocating workload across various system nodes to achieve superior performance and efficient resources consumption.

The main objective of LB is to guarantee user's requirements through the allocation of workload between various system nodes and increase resource consumption efficiency with increased system performance. This in turn also enhances the system consistency and throughput with reduced response time. In addition, the LB helps in organizing dynamic resources in cloud systems using virtualization technology. This increases the power efficiency through the allocation of various virtual machines to a single physical server. Accordingly, power utilization is also reduced by switching off certain servers or turning to sleep mode [10].

The problem statement of this research deals with security and LB problems in the cloud environment. In CC, the provision of security to the data is the essential factor to improve the confidentiality level of data. Due to the occurrence of unauthorized users (intrusions), security is the major concern while performing communication in the cloud. The LB also needs to be attained simultaneously to detect the intruders who make attacks and modifications on the cloud data. In existing many Energy-aware operation models have been implemented to successfully balance the load as well as used for application scaling on a cloud. It failed to provide better results for identifying the intrusions on cloud environment. Thereby, the efficiency in the LB had not improved at the essential level. Besides, numerous techniques have been developed with the implementation of a hidden access control approach for operating the encrypted data from the cloud environment. But LB issues remain unaddressed. Thus the security and LB are the significant challenging entities to perform efficient data communication on the cloud.

The main contribution of this research work is to propose a DCRI-RI hybrid technique for performing intrusion detection with higher LBE.

- At first, the CU's need to register their identity on a cloud server to obtain the cloud services. Based on the registration, the "user-id" and "password" are generated by the CS for CU. The proposed DCRI-RI technique employs the DCRI process to detect and remove intrusions (unauthorized users) by the generation of dynamic random public-key and private-key. Through the generated keys, the encryption and signature processes are performed at the CS side and then decryption and signature verification processes are carried out at the CU side. By the signature verification process, the unauthorized users (intruders) are detected and removed in a significant manner.
- Secondly, the RI process is carried out to successfully improve the LBE by balancing the load across multiple servers in an effective manner. From that, the data communication is attained with a better confidentiality level and LBE through the proposed DCRI-RI technique.

The remainder of this article is categorized as follows: Section 2 lists out some published articles regarding this research problem statement, Section 3 briefs about the methodologies module by module deeply for the proposed system, Section 4 discusses the results obtained both for an existing and proposed model with its comparative analysis, and Finally, Section 5 concludes this article with future scope.

Related Works

The researchers in [11] proposed a model called "Attribute-based Keyboard Search Scheme with User Revocation (ABKS-UR)". A comprehensive search permit for the encryption and diffusion of cloud data has been given. The users may generate their search capability without utilizing online trustworthy authorities. A policy on access imposed by the owner was then used to allow a search permit. Proxy re-encryption and lazy re-encoding strategies for carrying out deep device upgrade workloads have since been integrated. By utilizing a verification scheme to increase protection and authorizations standards, the efficiency of ABKS-UR has been enhanced. By utilizing ABKS-UR, the extent of data protection was not increased.

The researchers in [12] have built a "Privacy-Preserving Model (PPM)" to provide safe cloud storage. In CSPs and "Third Party Auditors (TPAs)", "Quality Of Service (QoS)" was improved and it was found malicious. A framework for auditing a TPA to reduce malicious threats has then been created. This helped TPA increase the degree of data integrity. Malicious insider attacks have been detected effectively. PPM refused to take into consideration the reliability of task scheduling.

The researchers in [13] created a "Remote Data Auditing (RDA)" strategy for improving cloud storage device credibility. For File-Authentication, the algebraic properties of the diffused data blocks were used. For preserving complex data functions, a "Divide and Conquer Table (DCT)" data structure was used. This system framework was able to have tremendous data storage and computing costs. A strong standard of confidentiality was reached, and server and auditor communications expenses were also lowered. By utilizing RDA methods, intrusion prevention has not been done successfully.

The researchers in [14] intend to consider various energy-efficient cloud procedures that employ resource allocation and compaction to achieve the very same. In contrast, the researchers aim to alter the existing protocol by adding a new variable. The researcher's main goal is to develop viable models and techniques for virtualization warehouses. Additionally, consider an effort to decrease energy demand while increasing resource utilization. The researchers suggest that, in comparison to the price, an extra variable, period, be added, which could result in improved resource use and a decline in the number of active servers. Before general adoption, the proposed proposal must be carried out and evaluated under multiple persistent or montage environments.

The researchers in [15] suggest a cloud-fog-dependent requirement for efficient energy storage in their article. Load balancing techniques such as "Weighted-Round-Robin (WRR)", "Round-Robin (RR)", and "Throttled", and is simulated in Cloud Analyst to examine and evaluate their implementation. The Throttled load balancing method outperforms the WRR and RR algorithms in terms of response time.

Methodologies

BPA-SAB (Existing Model)

In existing, the "Binomial Protection based Authentication with a Stochastic Agent-based Load Balancing (BPA-SAB)" was implemented to this research problem. The BPA-SAB model which has been performed to attain privacy preserved load balancing while accessing the data on the cloud. At first, the requests from the CU are forwarded to the CS. After that, the proposed BPA-SAB technique performs the BPA for effectively identifying the intrusion attacks to provide better results in the IDR. From the performance of this authentication, the authorized users are only permitted to operate on the server's data in the cloud which results in improved data privacy preservation. Thereby, the confidentiality level of data stored on the cloud is enhanced. Followed by, the SAB is deployed to perform the LB for accessing the data in the cloud. From that, the data accessing on the cloud is effectively performed by the proposed BPA-SAB technique with the improved data privacy perseveration and LB [16].

DCRI-RI (Proposed Model)

The proposed DCRI-RI technique performs the secured data communication in the cloud by effectively detecting unauthorized users (i.e. intruders) with improved load balancing efficiency. At first, the CUs need to register the "Identity (ID)" on the CU side to access the data from cloud storage. After the registration process, the CS creates the CU "user-id" and "password". Through the DCRI process, the Dynamic-Random key is generated for performing the encryption. Due to the performance of encryption, the original data is converted into cipher-text and then transmitted to the CUs. After that, the CU performs the decryption to obtain the plain-text from the cipher-text. Followed by, the signature-key verification being carried out to enhance the data confidentiality level through the detection of unauthorized users. Then, the RI process based on weightage indexing LB is performed to increase the LBE by effectively balancing the load on

the cloud. The process involved in the proposed DCRI-RI technique is elaborated and discussed in the following sections. The workflow of the proposed DCRI-RI methodology is given in Figure 1.

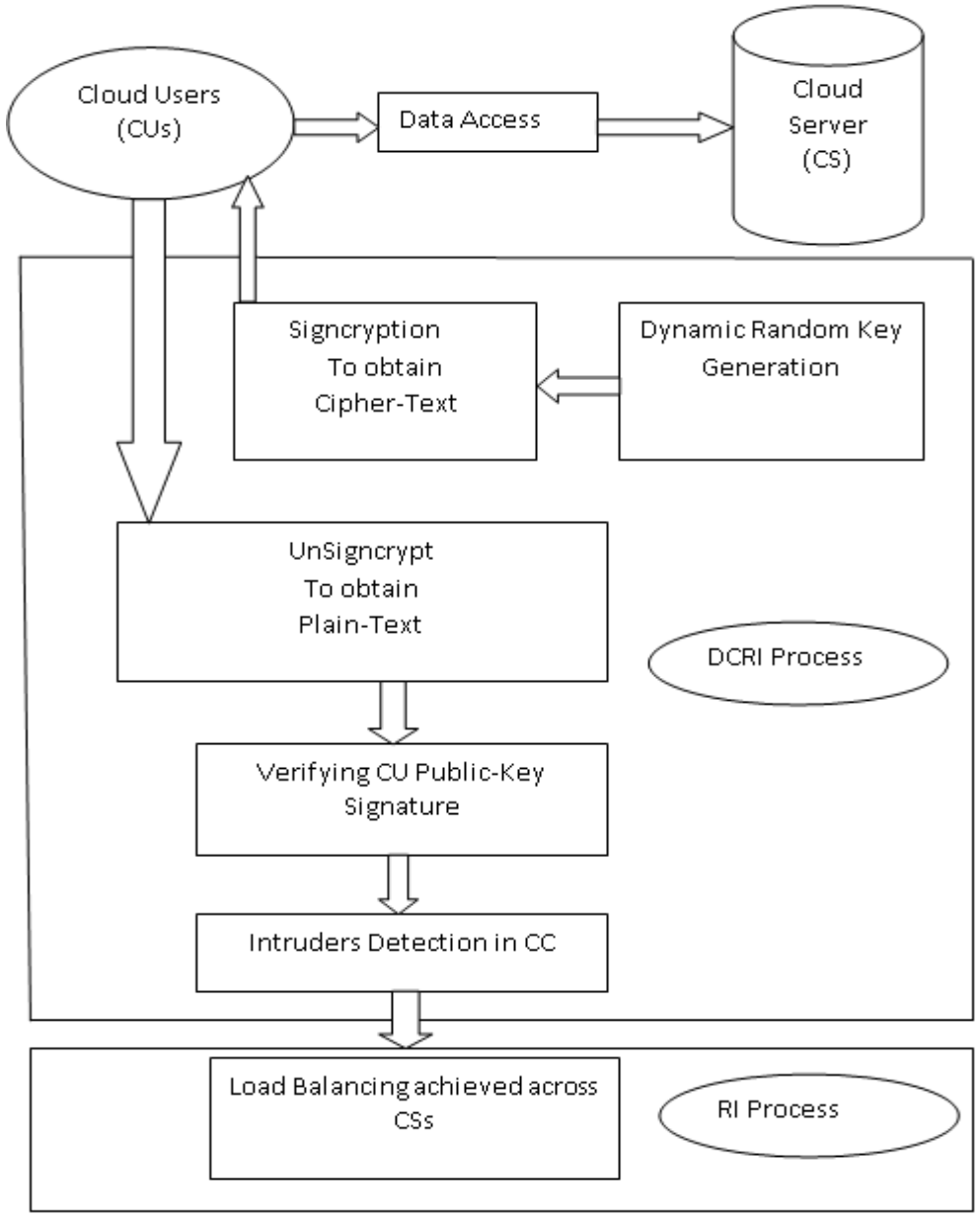

Figure 1: Proposed DCRI-RI Methodology Work Flow

Dynamic Certificateless Random Identity (DCRI) Based Intrusion Detection

The Dynamic Certificateless-Keygeneration is an identity-based cryptography technique that is used to protect the data by detecting and removing unauthorized users on the cloud. Through the development of Certificateless-

Keygeneration, the data confidentiality level is enhanced by performing the public-key encryption and digital signatures simultaneously. If the CU wants to access the data, then send the request to the CS. The CS performs the encryption and then transmits the data in encrypted form i.e. cipher-text as well as signatures to the respective CUs. After getting the cipher-text from CS, the CU performs the decryption to obtain original data i.e. plain-text as well as verify the CS signature. From that, the confidentiality level on cloud data is enhanced with the help of Certificateless-Keygeneration. According to the data classification, the secure CC model has been introduced to improve the confidentiality level of data by reducing the overhead and processing time while performing the secured data communication in the cloud. It had not an adequate model to effectively detect and remove unauthorized access within the service providers. With this intend, the proposed DCRI-RI technique carries outs the DCRI cryptographic system within the four essential steps to identify and discard unauthorized users. There are "Private-Key and Dynamic-Random-Key Generation", "Signcryption", "Unsigncryption" and "Digital-Signature Verification" which are elaborately explained as following subsections.

Generation of Private-Key and Dynamic-Random-Key

During the implementation of the proposed DCRI-RI technique, the DCRI cryptographic system carries outs the key generation process as a first step. Through the key generation process, the pair of keys is generated to carry out the encryption to enhance data security. With the help of generated key pair, the DCRI cryptographic system performs the encryption and decryption whenever the CU wants to access the data from the CS. By using DCRI cryptographic system, the encryption and decryption are performed with minimum time by using Private-Key and Dynamic-Random Public-Key. The setup phase of the DCRI cryptographic system comprises security-parameter 'S' and returns global system-parameters 'P_G'. The global-parameter is contained with dynamic-random public-key 'RK', data-space 'D', cipher-text space 'C' which is formularized as given below.

$$P_G \rightarrow \{RK, D, C\} \quad (1)$$

As shown in above Equation (1), 'P_G' represents the global parameter. Through the DCRI cryptographic system, the Dynamic-Random Public-Key 'RK' of the CU is generated to carry out the encryption and verification. In general, the Certificateless-Signcryption generates pair of keys to effectively perform the encryption and decryption. Due to the employment of a similar key in the encryption process, there is a chance for unauthorized users (intruders) to hack the data which leads to reducing the confidentiality level of data. The framework to provide security to the data has been designed in the cloud environment.

In the existing model, it provides multi-layered security, the data in real-time has been preserved from unauthorized users by the deployment of three layers of security such as firewall and access control, identity management and intrusion prevention, convergent encryption. But it did not enhance the confidentiality level. For that reason, the proposed DCRI-RI technique creates the Dynamic-Random Public-Key for each session with the help of the DCRI cryptographic system to

improve the confidentiality level. After the completion of one session, the Dynamic-Random Public-Key is disabled by DCRI cryptographic system. Followed by, the new Dynamic-Random Public-Key is created for the next session. From that, the unauthorized access is removed from the cloud which leads to enhancing the data confidentiality level. Figure 2 shows the Dynamic-Random Public-Key generation process.

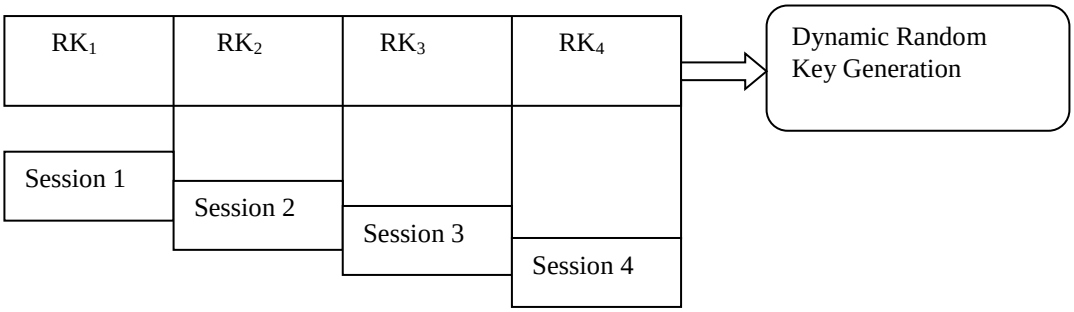

Figure 2: Dynamic-Random Public-Key Generation Process

As shown in Figure 2, the generation of Dynamic-Random Public-Key successfully performs the encryption and decryption to enhance the data security. For each session, the Dynamic-Random Public-Keys 'RK_1, RK_2, RK_3, RK_4' are created with the aid of the DCRI cryptographic system. The DCRI cryptographic system creates the Dynamic-Random Public-Key 'RK_1' for session 1 which the generated key helps to encrypt and decrypt the data at a particular session. The session is the sequence of interactions is carried out between two communication endpoints namely cloud server and users. After the completion of this process for one session, the DCRI cryptographic system eliminates the dynamic-random public-key 'RK_1' and then creates a new Dynamic-Random Public-Key 'RK_2' for the next session (session 2). The generation of Dynamic-Random Public-Keys for four sessions is formularized as given below.

$$\begin{aligned} \text{cs} \rightarrow Rand\ (RK_1, \text{RK}_2, \text{RK}_3, \text{RK}_4) \quad (2)\\ session_1 \rightarrow \text{RK}_1\\ session_2 \rightarrow \text{RK}_2\\ session_3 \rightarrow \text{RK}_3\\ session_4 \rightarrow \text{RK}_4 \end{aligned}$$

From Equation (2), 'cs' represents the CS, and 'RK_1, RK_2, RK_3, RK_4' represents the generated Dynamic-Random Public-Keys. These generated keys are distributed without any certification. Followed by, the Partial-Private-Key is generated where the cloud user in the certificateless environment submits their identity 'ID', global parameters 'R', and secret key 'SK'. The generation of a Partial-Private-Key is expressed as given below.

$$PP_K \rightarrow \{ID, P_G, SK\} \quad (3)$$

As shown in Equation (3), 'PP_K' represents the extracted Partial Private Key. Here, the user identity 'ID' takes a random value '0' and '1'. When the user identity 'ID' is '1', then it returns a partial private key. Otherwise, the unauthorized user is

identified if the user identity is '0'. The DCRI cryptographic system provides dissimilar partial private keys at different times for each user. After the extraction of Partial-Private-Key of the users, the full private key is constructed. The user secret value 'α_s' is created by considering the user identity 'ID' and global parameters 'P_G'. From that, the full private key is generated by taking the partial private key 'PP_K' and a secret value 'α_s' as an input. The generation of a Full-Private-Kkey is expressed as given below.

$$FP_K \rightarrow \{\alpha_S, PP_K\} \quad (4)$$

As shown in Equation (4), 'FP_K' signifies the Full-Private-Key. While performing the encryption process, the DCRI cryptographic system distributes the dynamic random public key and secretly keeps the private decryption key. From that, the proposed DCRI-RI successfully generates the private-key and public-key with minimum time with the help of the DCRI cryptographic system. According to the private-key and public-key, the proposed DCRI-RI carries out the signcryption and unsigncryption which is explained in the below subsection.

Signcryption Process

Once the private-key and public-key are generated, the proposed DCRI-RI technique carry-outs signcryption as a second step for performing both encryption and digital signature together to enhance confidentiality. Let us assume the number of CSs as 'u_1, u_2, u_3...u_n' and the Cloud-Data as 'D_1, D_2, D_3...D_n' from the CS. Then, the proposed DCRI-RI technique executes the encryption process through the identity. Figure 3 shows the block diagram of the signcryption process. As shown in Figure 3, the signcryption process successfully generates the cipher text and the signature. When the user needs to access the data, the cloud server forwards the cipher-text to the user by performing the encryption process with the aid of randomly selected receiver (i.e. user) Dynamic-Random Public-Key 'RK' and their identity 'ID_r'. Then, the encryption process on data is expressed as given below.

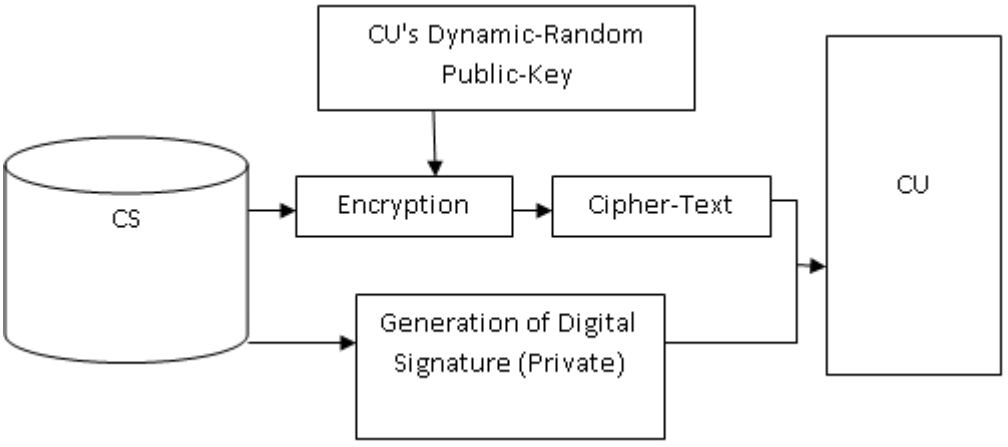

Figure 3: Block Diagram of Signcryption

$$C(D) \leftarrow E\ (RK_r, ID_U, D) \qquad (5)$$

From Equation (5), 'C(D)' signifies the cipher-text of original data. Here, 'E' denotes the encryption, 'RK_r' denotes the Dynamic-Random Public-Key of a receiver, 'ID_U' denotes an identity of receiver and 'D' denotes an original data (i.e. plain-text). After the completion of encryption, the cipher-text, as well as signature, is generated by the CS. By using the Digital-Signature, the authenticity of original data is established. The valid Digital-Signature assures that whether the data has been produced by a recognized sender (i.e. CS), and the data is not modified by intruders. From that, the generation of Digital-Signature of the data is carried out with the aid of the secret private-key of the sender. In a cloud environment, the proposed DCRI-RI technique gives the additional assurances of original data while accessing the data from the cloud. The Digital-Signature is attained in the form of hash-value. For any function, the hash-value is generated which helps to map data of random size into data of fixed length. Figure 4 shows the block diagram of the Digital-Signature generation process.

Figure 4. Digital Signature Generation

As shown in Figure 4, the fixed size of hash-value is obtained by the generation of Digital-Signature. The CS (i.e. sender) utilizes their full private-key for to create the signatures of the original data (plain-text). Then, the signature generation is expressed as given below.

$$S(D) \leftarrow \left(CS_{FPK}, D\right) \qquad (6)$$

As shown in Equation (6), 'S(D)' represents a signature of data. Here, 'CS_{FPK}' represents a CS (i.e. sender) full private-key and 'D' represents original data i.e. plain-text. From that, through the creation of hash-value, the proposed DCRI-RI technique obtains the Digital-Signature. After getting the encrypted data (i.e. cipher-text) and Digital-Signature, the CS forwards it to the CU (i.e. receiver).

Unsigncryption and Digital Signature Verification

After the encryption process, the decryption process is performed for producing the plain-text from the cipher-text to enhance the security in cloud data communication. The private-key (i.e. secret key) of CU on the CU side is helped for forwarding the encrypted data (cipher-text) back into the original readable form (plain-text). Through the proposed DCRI-RI technique, the decryption process is successfully carried out without the involvement of randomness for providing the output results. Thus, the proposed DCRI-RI technique performs encryption and decryption as a deterministic process for providing the original text from the cipher-text with an improved security level. Figure 5 shows the block diagram of unsigncryption and Digital-Signature verification.

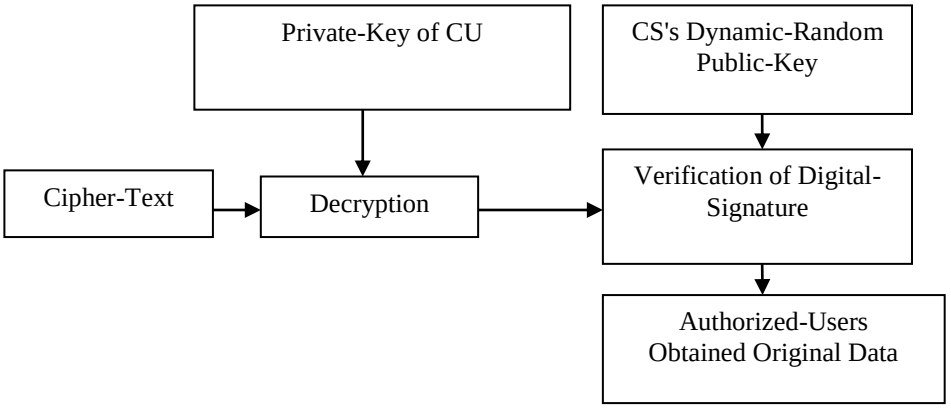

Figure 5: Block Diagram of Unsigncryption and Verification of Digital-Signature

As shown in Figure 5, the unsigncryption and Digital-Signature verification produce the plain-text from the cipher-text in a significant manner. The cipher-text is received by the CU from the CS. After that, the plain-text is obtained with the help of private-key and their Identity 'ID_{CS}'. The performance of the decryption process is expressed as given below.

$$P(D) \leftarrow D\ (\ PK_r, ID_{CS}, C(D)) \qquad (7)$$

From Equation (7), 'P(D)' represents the plain-text. Here, the private-key of a receiver (i.e CU) is signified as 'PK_r', and the identity of the sender (i.e. CS) is signified as 'ID_{CS}'. After getting the plain-text from the cipher-text through the decryption, the signature verification is carried out for identifying the unauthorized users on the cloud. The signature verification is performed at the CU side with the help of the Dynamic-Random Public-Key of the server. If the user recognizes the public-key of the sender, then the signature is verified. According to the signature verification, the CS detects whether the CU is authorized or not. When the signature of CU and CS are matched, then the user is identified as an authorized user. Otherwise, the user is said to be an unauthorized user (intruder) if the signature is mismatched. Through the above DCRI-RI processes it is possible to avoid intruders attacks and the data on the cloud server is protected by identifying the unauthorized users.

Rank-Indexing (RI) Based Load Balancing

After the detection of intruders on the cloud, the LB needs to be performed to enhance the data accessing from the CS. In the CC environment, the workloads among the multiple CSs are minimized by the performance of LB on the cloud. With this intend, the proposed DCRI-RI technique introduces the weighted-based indexing search to balance the load across the multiple CSs in an effective manner. Figure 6 shows the flow process of RI-based LB.

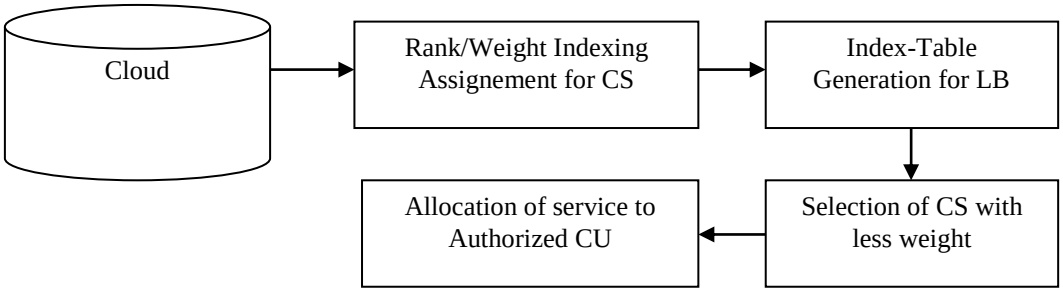

Figure 6: Processing of RI Based Load Balancing

As shown in Figure 6, the loads between multiple CSs are balanced by performing the weighted index search on the cloud. At first, according to the request sends from the CUs, the weights are allocated to each server which is expressed as given below.

$$w_t \rightarrow \{CS_1, CS_2, CS_3, CS_4\} \qquad (8)$$

As shown in Equation (8), weight 'w_t' is assigned to each CS. Followed by, the search is carried out by LB to obtain the possible solution of LB issues from the initial state. Through the heuristic function, the CSs are ranked in search algorithms according to the weight to access the data. The heuristic ranking model is expressed as given below.

$$LB \rightarrow R\{w_t CS_i\} \; i = 1, 2, 3 \ldots n \qquad (9)$$

From Equation (9), 'LB' represents a load balancer. Here, 'R' represents a rank assigned to cloud-server 'CS' depending on the weight 'w_t'. In the index-table, the rank allocated to CS is loaded.

Table 1: Rank-based Index Table

Cloud Servers	Ranks
CS1	2
CS2	1
CS3	3
CS4	4

The index-table is comprised of the information related to the CS. Then, the CS with less weight has a high rank to provide services. Table 1 illustrates the ranking model depending on the weight. According to the heuristic ranking model, the LBr chooses the cloud server with less weight and high rank 'CS_3' from the index table. The selection of CS with high rank is helped for offering the services to the Authorized CUs. Thereby, the overload across the servers is minimized in the cloud. The process involved in the RI is: At first, the weight of the CS is determined according to the number of CS requested data. Followed by, the weighted heuristics search is carried out by LB to balance the load across the multiple CSs. Through the weighted heuristics search, the CS is ranked based on the less weighted (i.e. the server has minimum user request). Then, the CS is

selected to provide services for Authorized CUs. In this way, unauthorized CUs are detected and avoided. Thereby, the proposed DCRI-RI technique balances the load with higher efficiency for detecting intrusions to provide secure data communication in the cloud environment.

Results and Discussions

An experimental evaluation for the proposed DCRI-RI hybrid technique is implemented in Java Environment utilizing Cloudsim simulator. The Cloudsim simulator uses the dataset from Amazon's ECC during the experiment's conduction. Through the use of Amazon's ECC dataset, the proposed DCRI-RI technique improves privacy preservation with effective load balancing by successfully performing intrusion attack detection processes. For experiment setup, the number of cloud users and the number of cloud user data is considered to range from 100 to 500 and 200 to 1000 within 20 iterations. The performance verification on the proposed DCRI-RI technique is recognized by making the comparative analysis of the existing BPA-SAB Model. The experimental evaluation is conducted based on the following factor as Load balancing efficiency (LBE), Intrusion detection rate (IDR), and Data accessing time (DAT).

Performance Analysis of LBE

The users who are authorized are correctly discovered from overall users in the cloud to attain the required services to the users is defined as LBE. The LBE is determined as per the given Equation (10).

$$LBE = \frac{Numberofauthorizedusersaredetected}{Totalnumberofcloudusersincloud} * 100 \quad (10)$$

In Equation (10), LBE is measured in terms of percentage (%). By detecting the authorized users, the load across the multiple cloud servers is balanced effectively. When the LBE is high then the technique provides better results on cloud communication.

Table 2: Numerical Comparision of LBE

CLOUD USERS	BPA-SAB	DCRI-RI
100	96	98
200	94	96
300	92	95
400	90	94
500	88	92

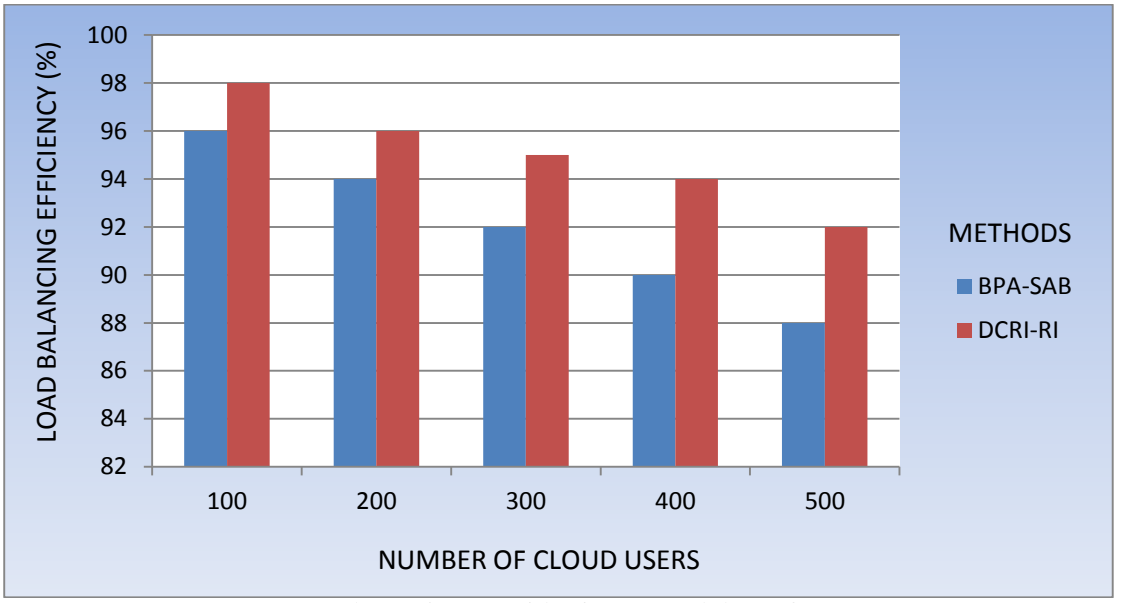

Figure 7: Graphical Comparision of LBE

Table 2 and Figure 7 illustrate that the experimental results of LBE concerning the number of cloud users. For simulation purposes, the number of cloud users is considered the range from 100 to 500 which is taken as input. The performance analysis of LBE of the proposed DCRI-RI technique is compared with the existing method BPA-SAB. The LBE is gradually varied in both methods based on the different number of cloud users. The proposed DCRI-RI technique effectively enhances the LBE than the existing method BPA-SAB for the higher number of cloud users.

Performance Analysis of IDR

The IDR is defined as the ratio of the number of users who are appropriately discovered as intrusions (i.e. users who are unauthorized) by overall cloud users. The IDR is determined as per the given Equation (11).

$$IDR = \frac{No.ofusers - No.ofintrusionscorrectlydiscovered}{No.ofusers} * 100 \quad (11)$$

In Equation (11) the IDR is measured in terms of percentage (%). When the performance of IDR is high then the technique provides improved results for secured data communication in the cloud.

Table 3: Numerical Comparision of IDR

CLOUD USERS	BPA-SAB	DCRI-RI
100	96	98
200	93	95

300	91	93
400	88	91
500	85	89

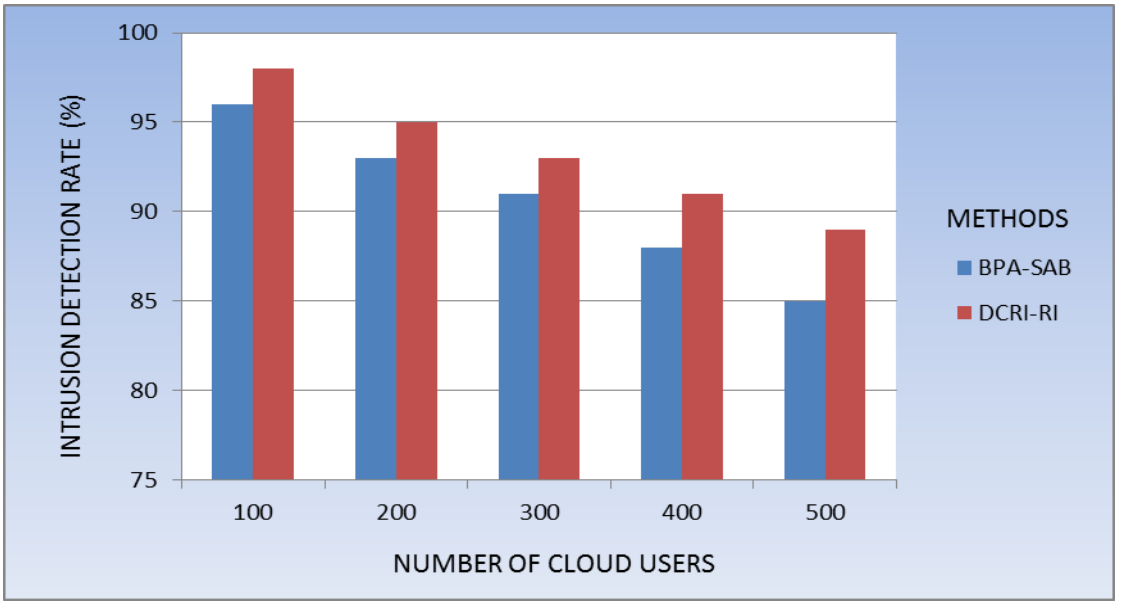

Figure 8: Graphical Comparision of IDR

Table 3 and Figure 8 illustrate the experimental results of IDR concerning the number of cloud users. For simulation purposes, the number of cloud users is considered the range from 100 to 500 which is taken as input. The performance analysis of IDR of the proposed DCRI-RI technique is compared with the existing method BPA-SAB. The IDR is gradually varied in both methods based on the different number of cloud users. The DCRI-RI technique effectively enhances the IDR than the existing method BPA-SAB for the higher number of cloud users.

Performance Analysis of DAT

The DAT is determined as the total taken time in the cloud for data accessing. This DAT is evaluated as per the given Equation (12).

$$DAT = Number\ of\ \ data * time\ (accessingdatafromcloudserver) \quad (12)$$

In Equation (12) the DAT is measured in terms of milliseconds (ms). When the accessing time of data is less, then the technique provides better performance in cloud data communication.

Table 4: Numerical Comparision of DAT

USER DATA	BPA-SAB	DCRI-RI
200	20	10
400	35	18
600	50	31
800	65	43
1000	80	66

Table 4 and Figure 9 illustrate the experimental results of DAT concerning the number of user data. For simulation purposes, the number of user data is considered as the range from 200 to 1000 which is taken as input. The performance analysis of the DAT of the proposed DCRI-RI technique is compared with the existing method BPA-SAB. The DAT is gradually varied in both methods based on the different numbers of user data. The DCRI-RI technique effectively takes less time to access the data than the other existing method BPA-SAB for large number cloud user data.

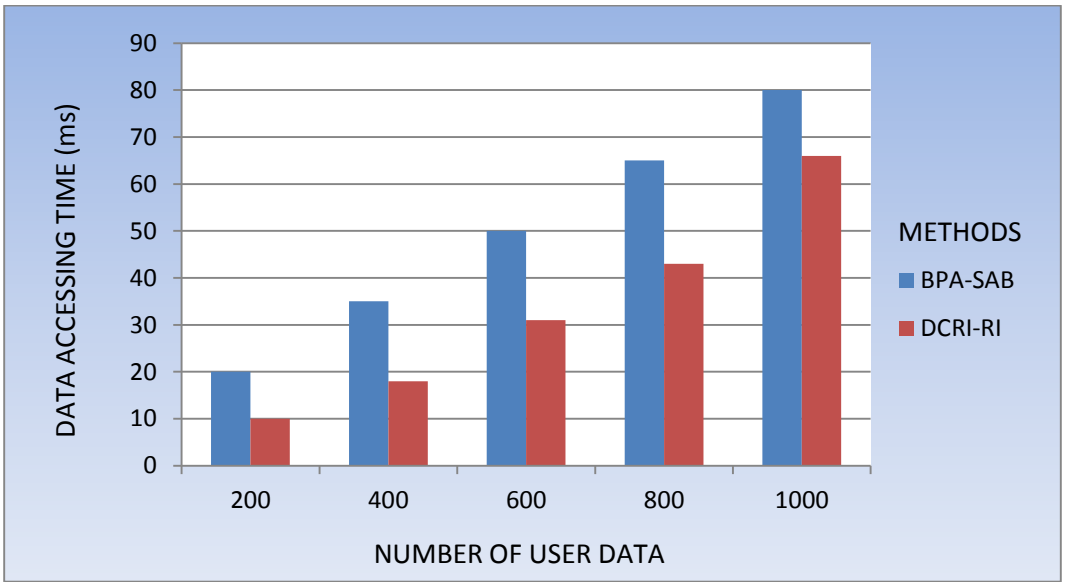

Figure 9: Graphical Comparision of DAT

Conclusion

In the cloud environment, we propose a DCRI-RI technique to perform the data communication in a secured manner. Through the involvement of the DCRI cryptographic system, the signcryption, unsigncryption, and Digital-Signature verification are carried out with the generation of Dynamic-Random Public-Key and Private-Key. The original data i.e. the plain-text is converted into cipher-text at the CS side and the obtained cipher-text is converted into plain-text with minimum time by performing the signcryption, unsigncryption respectively. Thereby, the confidentiality of the data gets improved. Through the performance of digital signature verification, the unauthorized intruders are identified with the

aid of a Dynamic-Random Public-Key which leads to enhance the security. Followed by, the Rank/Weight indexing based load balancing is performed to balance the load across the multiple cloud servers. From that, secure data communication is successfully performed by detecting intrusions and achieving load balancing in a significant manner. For examining the DCRI-RI method's performance, it was compared with the BPA-SAB. The comparison analysis, clearly described that the proposed DCRI-RI technique attains better improvement on the following parameters as LBE, IDR, and DAT than the BPA-SAB. Hence, the performance result of LBE and IDR in the DCRI-RI technique is improved up to 25% and 30% and DAT is improved by 20% when compared to BPA-SAB. In the future, we try to improve the load balancing with advanced bio-inspiring algorithms.

References

1. Yousif, M. (2017). The State of the Cloud. IEEE Cloud Computing, 4(1), 4-5. doi:10.1109/mcc.2017.4
2. Bhardwaj, A., & Goundar, S. (2020). Cloud Computing Security Services to Mitigate DDoS Attacks. Cloud Computing Security [Working Title]. doi:10.5772/intechopen.92683
3. N. Moustafa, B. Turnbull and K.-K.-R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things", IEEE Internet Things J., vol. 6, no. 3, pp. 4815-4830, Jun. 2019.
4. N. Moustafa, G. Creech, E. Sitnikova and M. Keshk, "Collaborative anomaly detection framework for handling big data of cloud computing", Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS), pp. 1-6, Nov. 2017.
5. N. Moustafa, G. Creech and J. Slay, "Anomaly detection system using beta mixture models and outlier detection", Progress in Computing Analytics and Networking, pp. 125-135, 2018.
6. M. Keshk, E. Sitnikova, N. Moustafa, J. Hu and I. Khalil, "An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems", IEEE Trans. Sustain. Comput., 2019.
7. M. Keshk, N. Moustafa, E. Sitnikova and B. Turnbull, "Privacy-preserving big data analytics for cyber-physical systems", Wireless Netw., vol. 24, pp. 1-9, Dec. 2018.
8. Herman, M., Iorga, M., Salim, A. M., Jackson, R. H., Hurst, M. R., Leo, R., Sardinas, R. (2020). NIST Cloud Computing Forensic Science Challenges. doi:10.6028/nist.ir.8006
9. Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018). Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. IEEE Access, 6, 18209-18237. doi:10.1109/access.2018.2820162
10. H. A. Alharbi, T. E. H. Elgorashi and J. M. H. Elmirghani, "Energy Efficient Virtual Machines Placement Over Cloud-Fog Network Architecture," in IEEE Access, vol. 8, pp. 94697-94718, 2020, doi: 10.1109/ACCESS.2020.2995393.
11. Wenhai Sun, Shucheng Yu, Wenjing Lou & Thomas Hou, Y, Hui Li 2016, 'Protecting Your Right: Verification Attribute-Based Keyboard Search with Fine-Grained Owner-Enforced Authorization in the Cloud', IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 4, pp. 1187-1198.

12. Abdul Razaque & Syed S Rizvi 2017, 'Privacy preserving model: a new scheme for auditing cloud stakeholders', Journal of Cloud Computing: Advances, Systems and Applications, Springer, vol. 6, no.7, pp. 1-17.
13. Mehdi Sookhak, Abdullah Gania, Muhammad Khurram Khan & Rajkumar Buyya 2017, 'Dynamic Remote Data Auditing For Securing Big Data Storage In Cloud Computing', Information Sciences, Elsevier, vol. 380, pp. 101-116.
14. Patel, K., Patel, N., & Patel, H. (2016, March). "Efficient Resource Allocation Strategy to Improve Energy Consumption in Cloud Data Centers." In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (p. 76). ACM.
15. Naeem, M., Javaid, N., Zahid, M., Abbas, A., Rasheed, S., & Rehman, S. (2018, September). "Cloud and Fog Based Smart Grid Environment for Efficient Energy Management." In International Conference on Intelligent Networking and Collaborative Systems (pp. 514-525). Springer, Cham.
16. Abraham, A.T., Thomson Fredrik, E.J. (2022). "Ensuring the Security and Load Balancing in the Cloud Environment by BPA-SAB Method". In: Hu, YC., Tiwari, S., Trivedi, M.C., Mishra, K.K. (eds) Ambient Communications and Computer Systems. Lecture Notes in Networks and Systems, vol 356. Springer, Singapore.