INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

ENSEMBLE OF RANDOM DECISION TREES WITH BOOTSTRAP AGGREGATING FOR IMPROVING CONFIDENTIALITY OF CLOUD DATA SERVICES

Computer Science

K.PALANISAMY Ph.D Research Scholar, Dravidian University, Kuppam , AP.

DR.C.CHANDRA SEKAR Professor, Department of Computer Science, Periyar University, Salem, TN.

ABSTRACT

Cloud computing is computing resources to deliver services using local servers or private devices in order to maintain the cloud applications. The cloud service provider is responsible for maintaining the cloud data on cloud database against the unauthorized access. Thus, cloud data security is one of main issue in a cloud computing environment with higher response time of cloud service provisioning. In order to overcome the above issues, Ensemble of Random Decision Trees with Bootstrap Aggregating (ERDT-BA) Technique is proposed. Thus, the proposed technique enhancing the security and confidentiality rate of cloud data service provisioning. In addition, Bagging Ensemble Classifier is used to improve the authentication performance of cloud users with minimum time. In Bagging Ensemble Classifier, Random Decision Trees is combined with Bootstrap Aggregating to attain higher classification accuracy for user authentication. With the aid Ensemble Classifier, cloud data is classified as legitimate or illegitimate users and verified cloud users only access the data. After cloud user verification, required data services are provided only to legitimate cloud users in cloud computing environment. This helps to attain secure cloud data service provisioning with higher integrity and confidentiality rate of cloud data services. The performance analysis of proposed ERDT-BA technique is conducted on parameters such as classification accuracy, false positive rate, and data confidentiality rate. The experimental result shows that the ERDT-BA technique achieves higher security and data confidentiality rate of cloud service provisioning than other methods.

KEYWORDS

Cloud service provisioning, Bagging Ensemble Classifier, Random Decision Trees, Bootstrap Aggregating technique

INTRODUCTION

Cloud computing provides a data sharing which is an essential possessions due to the enormous improvement of data in cloud data services. Data confidentiality is one of main provision to maintain the data outsourcing on cloud with secured manner. Here, Secure Cloud Storage System was considered to enhance the security and confidentiality of user authentication. Thus, it protects the data's of organizations from cloud environment.

Secure Data sharing (SeDaSC) methodology was presented in [1] to encrypt the data by using single encryption key. During data encryption, inner threats and cryptographic servers are prevented with the support of different key shares. It enhances data security but reduces confidentiality rate. In [2], Shared Authority based Privacy-preserving Authentication protocol (SAPA) was designed to attain shared access authority. Data sharing is achieved among multiple users but failed to report the response time of data sharing.

An adaptive multilevel security framework was planned in [3] using cryptography techniques to organize the data in an effective manner. It manages various business and commercial situations but authentication time is unaddressed. A secure multi-owner data sharing scheme named as Mona was developed in [4] to achieve dynamic collection of data from users. Thus, it contains better storage overhead and encryption cost but remains minimum security.

In [5], confidentiality technique named as Word Magical Rolling Alpha Digits Obfuscation (WMRADO) was designed. Due to minimum data size, data storage in minimized and security is improved. Fragmentation technique was applied in [6] to accomplish higher data confidentiality in cloud servicer. By using fragmentation and distribution approach, confidentiality is improved. Though, data stored with minimum security and response time.

A secure partitioning approach was considered in [7] to provide trust and secure data in cloud computing. With this approach, images are divided and attributes are removed to improve security and privacy of data in public cloud. In [8], Cloud Computing Adoption Framework (CCAF) was considered to improve the security of cloud data with encryption decryption process. Though, it attains reduced data confidentiality rate with higher authentication time. A secured confidentiality technique named as AROcrypt was developed in [9] for improving the data storage in cloud computing. It converts the plaintext to cipher text to improve security but data confidentiality rate was not sufficiently improved.

A classification technique was presented in [10] on the basis of data confidentiality. Based on encryption, authentication and authorization, stored data in cloud is improved. Though, the authentication time was improved by using classification technique based on data confidentiality. The issues presented in the existing methods are reduced data security and confidentiality level. In order to overcome such issues, Ensemble of Random Decision Trees with Bootstrap Aggregating (ERDT-BA) technique is developed in cloud service provisioning.

The main contribution of the research work is described as follows,

- To achieve confidential cloud service provisioning, Ensemble of Random Decision Trees with Bootstrap Aggregating (ERDT-BA) technique is used with the aid of bagging ensemble classifier. Then, Random Decision Trees is combined with Bootstrap Aggregating technique to attain higher classification accuracy. Therefore, it effectively authenticates the cloud users request to cloud server and verifies either it is legitimate or illegitimate cloud data.
- After verifying the cloud data, Authentication Based Data Access Algorithm is used to provide confidential cloud services. When there is a legitimate cloud user in cloud computing environment, secure cloud data service provisioning is achieved. As s result, the integrity and confidentiality rate of cloud data service provisio ning is improved in a significant manner.

The rest paper is organized as follows: In Section 2, Ensemble of Random Decision Trees with Bootstrap Aggregating (ERDT-BA) technique is described with neat diagram. In Section 3, experimental settings are provided with the analysis of results explained in Section 4. In Section 5, introduces the related works. The conclusion of the research work is presented in section 6.

2. ENSEMBLE OF RANDOM DECISION TREES WITH BOOTSTRAP AGGREGATING TECHNIQUE

Cloud computing is an encouraging information technology that is designed for both organizations and individuals. They provide more advantages for example minimum costs, data reliability, unlimited storage and so on. There are three types of services such as software as a service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Cloud Service Provider in cloud architecture presents required services to the users. The general architecture of cloud service provisioning with computing resources to their users are demonstrated in figure 1.

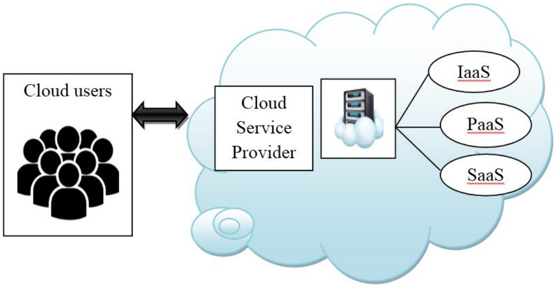

Figure 1 General Architecture of Cloud Service Provisioning

As shown in the figure 1, both the users and developers are controlled that are involved in on-line businesses. Here, cloud server permits the authorized users to contact the cloud storage and helps a user to access the data after achieving a proper authentication. At last, authentication technique is used for improving the security of cloud service provisioning. Therefore, ERDT-BA Technique is proposed using bagging ensemble classifier and improves user authentication performance. It responsible authentication is obtained between cloud user and cloud service provider. The overall architecture for Ensemble of Random Decision Trees with Bootstrap Aggregating (ERDT-BA) Technique is shown in below figure 2.

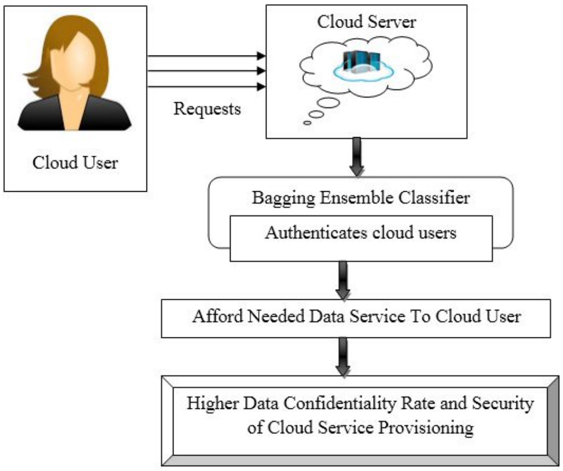
Cloud User
Requests
Cloud Server
Bagging Ensemble Classifier
Authenticates cloud users
Afford Needed Data Service To Cloud User
Higher Data Confidentiality Rate and Security of Cloud Service Provisioning

Figure 2 Architecture Diagram of Ensemble of Random Decision Trees with Bootstrap Aggregating Technique

Above figure 2 describes the architecture diagram of ERDT-BA Technique. Initially, cloud user request is transmitted to cloud server to access cloud data. After receiving the user request, Bagging Ensemble Classifier is used to verify the cloud user as legitimate or illegitimate cloud data. During cloud user verification, cloud service provider contributes essential data services to cloud users in cloud computing environment when the user is legitimate. Hence, unnecessary persons cannot get the data stored in cloud. Therefore, ERDT-BA technique enhances security of cloud service provisioning with higher data confidentiality rate. The proposed ERDT-BA Technique includes of three phases for achieving confidential cloud services such as Setup phase, Verification phase and Data access phase.

2.1 Setup Phase

In the beginning, setup phase is used in ERDT-BA Technique to schedule the user's information's request with cloud server for authentication. The details about the cloud users are registered in setup phase to cloud server and store in the database. Then, the User-ID (User Identity, password) is produced in cloud server and transmitted towards the user's personal device or personal mail account. Thus, the cloud user enters the login page for obtaining the cloud data. The process of setup phase for registering user on cloud is shown in figure 3.

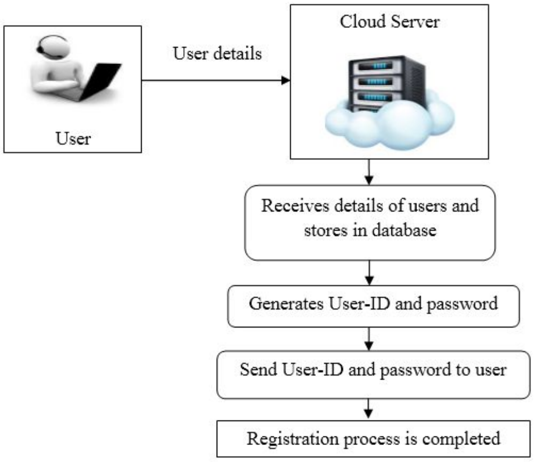
User
User details
Cloud Server
Receives details of users and stores in database
Generates User-ID and password
Send User-ID and password to user
Registration process is completed

Figure 3 Processes of Setup Phase for Registering User on Cloud

The process of setup phase is described in figure 3. At first, cloud user information's such as First Name, Middle Name, Last Name, Date of birth, Gender, Mobile No, Mail-ID are transmitted to cloud server for registration. Then, cloud server stores all information in database and generates id and password to each user requests. At last, user id and password is transmitted to cloud user for achieving secured and confidential cloud services. After that, verification process is carried out to ensure the user as an authorized or unauthorized person.

2.2 Verification Phase

Next, Verification phase utilized in ERDT-BA technique which verifies the authority of cloud users stored in database. With the application of Bagging Ensemble Classifier, verification is carried out on the data stored in cloud. The Bagging Ensemble Classifier increases the analysis of user verification in cloud with higher classification accuracy. It classifies the cloud users as legitimate or illegitimate with the help of information stored in database. Here, only the legitimate cloud users are permitted to attain the cloud data. Thus, the security and confidentiality of cloud service provisioning is improved. Below diagram 4 shows process of Bagging Ensemble Classifier for confidential cloud service provisioning.

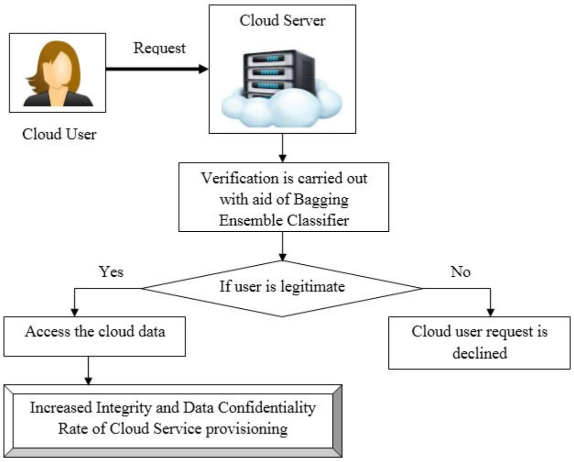
Cloud User
Request
Cloud Server
Verification is carried out with aid of Bagging Ensemble Classifier
Yes
No
If user is legitimate
Access the cloud data
Cloud user request is declined
Increased Integrity and Data Confidentiality Rate of Cloud Service provisioning

Figure 4 Process of Bagging Ensemble Classification for Confidential Cloud Service

The process of bagging ensemble classifier is shown in figure 4 for providing confidential cloud service. At first, cloud user request is send to cloud server to attain cloud data. After that, verification process is performed on cloud server to determine legitimate or illegitimate cloud users. When there is a legitimate user, cloud data is access, else it is declined. Therefore, ERDT-BA technique achieves higher integrity and confidentiality data on cloud service provisioning in an effectual manner.

2.2.1 Bagging Ensemble Classifier

The verification phase in ERDT-BA technique uses the Bagging Ensemble Classifier for ensuring the cloud users to cloud server. With the classification process, legitimate or illegitimate cloud users are classified. Here, Random Decision Trees is combined with Bootstrap Aggregating technique (i.e. bagging) to achieve classification performance for authenticating cloud users with minimum time. At first, input of the Bagging Ensemble Classifier is user login information to cloud server. Next, bootstrap random sampling technique is used where it consists of 'n' decision trees and every decision tree is trained by random approach. The data's are randomly selected from the user login information. Then, collected data's are classified with higher classification accuracy and minimum time. The process of Bagging Ensemble Classifier for cloud user verification is shown in below figure 5.

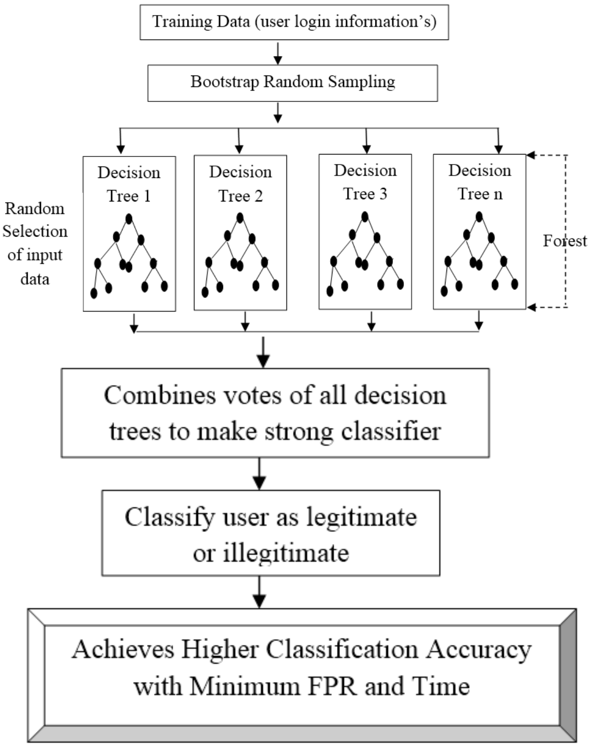
Training Data (user login information's)
Bootstrap Random Sampling
Random Selection of input data
Decision Tree 1
Decision Tree 2
Decision Tree 3
Decision Tree n
Forest
Combines votes of all decision trees to make strong classifier
Classify user as legitimate or illegitimate
Achieves Higher Classification Accuracy with Minimum FPR and Time

Figure 5 Process of Bagging Ensemble Classifier for User Verification

From the figure 5, a Bagging Ensemble Classifier consists of *'n'* decision trees and each decision tree is trained through a random approach. For each decision tree '**t**$_n$' features (i.e. user id, password, etc) are selected randomly from user login information and verified with pre-stored information that stored in database. At last, Bagging Ensemble Classifier combines votes of all decision trees to make the strong classifier for classifying the user as genuine or not. Thus, it significantly enhances the classification accuracy of cloud user verification with minimum false positive rate and time. In order to classify features in decision tree, each node establishes the Gini index. For each node in a decision tree, features are randomly selected from user login information and the node is divided with the help of binary split. Here, parent node 'node$_p$, is divided into child nodes ***'node'****l* and ***'node$_r$'*** using Gini index. The mathematically representation of Gini index is as follows.

$$I_G(node) = 1 - \sum_{c=1}^{2} p_c^2 \qquad (1)$$

From (1),'p$_c$' represents the relative proportion of features and presents class in node. The best Gini index is determined by using below mathematical formula.

$$\Delta I_G(node_p) = I_G(node_p) - p_l I_G(node_l) - p_r I_G(node_r) \qquad (2)$$

From (2), 'pl' and 'p_r' signifies the proportions of features in user login information of parent node ***' nodep'*** that are assigned to child nodes ***'nodel'*** and ***'noder'*** respectively. With the aid of Gini index, the relative importances of features are attained for classification.

After constructing 'n' decision trees, the vote is allocated for each tree by verifying user login information stored in database. Finally, Bagging Ensemble Classifier combines all the outputs from the individual decision tree (***t1,t2 …tn***) by considering the average of all ***n*** outputs using voting results. The Bagging Ensemble Classifier combines the results of each weak classifier to a strong classifier and it is expressed as follows.

$$\hat{\boldsymbol{F}}(\boldsymbol{A}) = \boldsymbol{arg} \ \max_{c} \boldsymbol{p}_{c}(\boldsymbol{A}) \qquad (3)$$

$$= \mathbf{arg\,max} \left(\frac{1}{N}\right) \sum_{n=1,2\ldots n} \boldsymbol{p}_{n,p} (\boldsymbol{f}(\boldsymbol{A}) = \boldsymbol{c}) \qquad (4)$$

From (3) and (4), number of random decision tree is denoted as ***'n'*** and ***'A'*** is the selected feature of user login information to classify and c represents the label of class. The probability classified by the nth binary tree is given as ***'pn,p'*** where the features are belonged to the legitimate class. From the class value, ***'0'*** and ***'1'*** effectively distinguishes the legitimate cloud users and illegitimate cloud users. In ERDT-BA Technique, ***c*=1** indicates the user is legitimate whereas ***c*=0** signifies the illegitimate cloud user. The algorithmic process of Bagging Ensemble Classifier for cloud user authentication is shown in below algorithm 1.

```
// Bagging Ensemble Classifier based Authentication Algorithm
Input: Training data $D = D_1 D_2 D_3 ... D_n$", i.e. contains multiple users login information's to the cloud server, Feature ", Number of trees in forest
Output: Increased Classification Accuracy with Reduced FPR and time
Step 1: Begin
Step 2:   For features in users login information's
Step 3:     Constructs n decision tree
Step 4:       For decision tree
Step 5:         Features are chosen randomly from the users login information's
Step 6:         Parent node is splits into child nodes based on Gini index using (1) and (2)
Step 7:           If ( number of trees are constructed) then
Step 8:             Bagging Ensemble Classifier combines votes of all weak classifier and makes a strong classifier by using (3) and (4) for user authentication
Step 9:             Strong classifier classifies the user as legitimate or illegitimate
Step 10:          End if
Step 11:      End for
Step 12:  End for
Step 13: End
```

Algorithm 1 Bagging Ensemble Classifier based Authentication

Algorithm 1 illustrates the process of bagging ensemble classifier. Initially, user's login information's is considered as input and multiple binary trees are constructed by using available features in user's login information's. Then, Gini index is used to separate the nodes and obtains varies result. After that, bagging ensemble classifier combines the results of all weak classifier in order to make a strong classifier by using voting results. Finally, the legitimate or illegitimate cloud users are classified with the aid of strong classifier. As s result, proposed technique improves the classification accuracy and reduces the false positive rate of user authentication.

2.3 Data Access Phase

At last, data access phase is used in ERDT-BA technique after the verification of the cloud user. It presents the advantageous services to cloud user. The algorithmic process of authentication based data access is shown in below algorithm 2.

```
// Authentication Based Data Access Algorithm
Input: User Request
Output: Enhanced Data Confidentiality and Integrity Rate
Step 1: Begin
Step 2:   For each user request
Step 3:     Verification is performed with aid of bagging
```

```
ensemble classifier
Step 4:     If user is genuine, then
Step 5:       Permitted for accessing cloud data
Step 6:     else
Step 7:       The user request is declined
Step 8:       End if
Step 9:       End for
Step 10:      End
```

Algorithm 2 Authentication Based Data Access

Algorithm 2 explains the Authentication Based Data Access Algorithm. Initially, bagging ensemble classifier verifies the each user to provide confidential cloud services. If the cloud user is a legitimate, then cloud service provider gives requested data service to user. Otherwise, the user request is declined. Thus, the legitimate cloud users are permitted to obtain the cloud data stored in cloud server. This helps to maintain consistency, accuracy and trustworthiness of data on cloud. As a result, ERDT-BA Technique enhances the integrity and confidentiality rate of cloud data service provisioning in an effective manner

3. EXPERIMENTAL EVALUATION

An Ensemble of Random Decision Trees with Bootstrap Aggregating (ERDT-BA) technique is implemented in Java language using CloudSim simulator. The CloudSim simulator employs Amazon EC2 Dataset for performing experimental process. The performance evaluation of BECA Technique compared with existing approach Secure Data Sharing in Clouds (SeDaSC) [1] and Shared Authority based Privacy-preserving Authentication Protocol (SAPA) [2]. The following metrics such as Classification accuracy, false positive rate and Data Confidentiality rate are evaluated to improve the performance of ERDT-BA technique.

4. RESULT ANALYSIS

The result analysis of proposed ERDT-BA technique is performed with existing SeDaSC [1] and SAPA [2]. Experimental analysis is carried out with different parameter such as Classification accuracy, false positive rate and Data Confidentiality rate. Performance is evaluated along with the following metrics with help of tables and graph values.

4.1 Measurement of Classification Accuracy

The measure of correctly classified cloud user's as legitimate or illegitimate according to the total cloud users are termed as classification accuracy. It is measured in percentage (%).

$$Classification\ Accuracy = \frac{Correctly\ classified\ cloud\ user's}{Number\ of\ cloud\ users} * 100 \qquad (5)$$

Table 1 Tabulation for Classification Accuracy

Number of Cloud Users	Classification Accuracy (%)		
	SeDaSC	SAPA	ERDT-BA Technique
10	72.15	66.45	87.95
20	73.26	67.87	88.56
30	74.62	69.12	89.02
40	75.84	70.56	89.95
50	76.35	71.16	91.03
60	76.92	71.55	91.28
70	79.98	74.72	94.15
80	81.73	76.16	95.91
90	83.16	77.27	96.62
100	84.39	78.52	97.94

Above table 1 describes the tabulation result of classification accuracy for classifying the cloud user as legitimate or illegitimate users. For experimental purpose, 100 cloud users are considered for both proposed and existing methods.

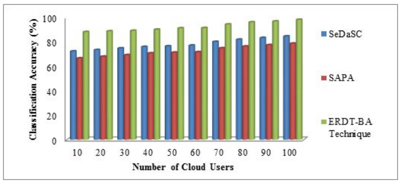

Figure 6 Measurement of Classification Accuracy

Figure 6 shows the result of classification accuracy for cloud user verification using existing methods namely SeDaSC and SAPA with proposed ERDT-BA Technique. With the aid of bagging ensemble classifier, proposed ERDT-BA technique gives better classification accuracy. At first, user login features are used to generate binary tree. Then, weak classifier is combined with strong classifier and effectively users are classified as legitimate or illegitimate cloud users. Therefore, classification accuracy is increased in ERDT-BA technique by 19 % and 28% when compared to existing SeDaSC [1] and SAPA [2] respectively.

4.2 Measurement of False Positive Rate

The ratio of incorrectly classified cloud user's as legitimate or illegitimate to total number of cloud users is defined as false positive rate. It is expressed in percentages (%).

$$False\ Positive\ Rate = \frac{incorrectly\ classified\ cloud\ user's}{Number\ of\ cloud\ users} * 100 \qquad (7)$$

Table 2 Tabulation for False Positive Rate

Number of Cloud Users	False Positive Rate (%)		
	SeDaSC	SAPA	ERDT-BA Technique
10	39.65	43.87	28.56
20	40.9	44.99	29.23
30	42.12	46.21	30.48
40	44.59	48.17	32.55
50	46.65	51.02	34.9
60	49.06	53.26	37.15
70	51.35	55.06	39.87
80	54.16	57.98	42.54
90	55.98	60.12	45.36
100	58.23	61.95	47.12

The tabulation result of false positive rate is illustrated in above table 2 based on number of cloud users in the range of 10-100 users. Above table shows the comparison results of proposed ERDT-BA technique with existing SeDaSC [1] and SAPA [2] methods.

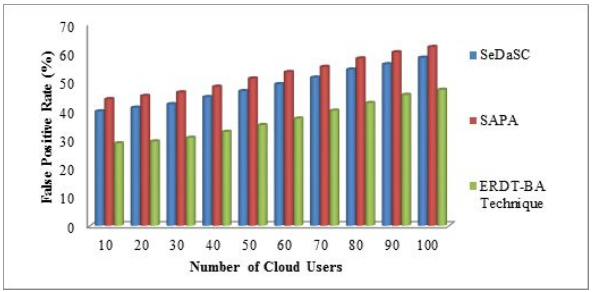

Figure 7 Measurement of False Positive Rate

The result analysis of false positive rate is shown in figure 7 for user verification versus with different number of cloud users. From figure, false positive rate of user verification using proposed ERDT-BA Technique is lower. With the application of bagging ensemble classifier, the cloud users are effectively classified as legitimate or illegitimate users. It is achieved by combining weak classifier to prepare a strong classifier. Thus, proposed ERDT-BA Technique minimizes the false positive rate of user verification by 24% and 30% when compared to existing SeDaSC [1] and SAPA [2] respectively.

4.3 Measurement of Data Confidential Rate

Data Confidentiality Rate is determined to protect the data stored in cloud and can only the accessed by the legitimate cloud user. It is measured in percentage (%).

Table 3 Tabulation for Data Confidential Rate

Size of Data (MB)	Data Confidential Rate (%)		
	SeDaSC	SAPA	ERDT-BA Technique
50	65.41	60.89	82.26
100	67.36	62.56	83.98
150	69.35	64.45	85.15
200	70.53	66.16	86.65

250	72.99	68.55	89.21
300	75.47	70.98	91.65
350	77.44	72.46	93.35
400	79.38	73.82	94.78
450	81.23	75.75	96.05
500	82.67	76.64	97.3

Table 3 represents the tabulation of data confidentiality rate with respect to cloud data size in the range of 50-500 MB using three methods. The table shows the comparative analysis of proposed ERDT-BA Technique with existing SeDaSC [1] and SAPA [2] methods. The data confidentiality rate using proposed ERDT-BA technique is higher than the existing methods.

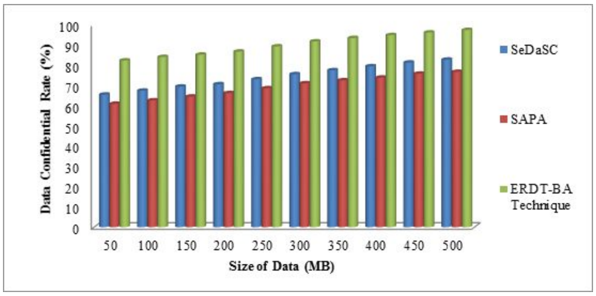

Figure 8 Measures of Data Confidential Rate

Figure 8 shows the performance analysis of data confidentiality rate with different size of cloud user data. The result shows that the proposed ERDT-BA technique provides better confidentiality rate when compared to existing methods. By the combination of random decision tree with bootstrap aggregating in ERDT-BA technique, classification accuracy of user authorization is improved. Thus, it protects the cloud data from unwanted or unauthorized cloud users. Therefore, proposed ERDT-BA Technique increases the confidentiality rate of cloud data by 22% and 30% when compared to existing SeDaSC [1] and SAPA [2] respectively.

5. RELATED WORKS

A secure data classification model was designed in [11] by using Bayesian supervised machine learning approach. Based on this approach, confident and highly confidential data is differentiated to improve confidentiality rate and efficient data storage in cloud server. But, authentication time during data classification is higher. In [12], data classification technique was developed to enhance the security of data in cloud computing according to the level of protection required. Though, the data confidentiality level was reduced.

With the assist of anonymous authentication, security level of cloud storage is improved by utilizing a developed Decentralized Access Control scheme in [13]. Bloom filters and simple randomization techniques were implemented in [14] using pre-filtering operator. With the help of pre-filtering operator, minimizes the encrypted subscriptions and improved security level of the stored information that restored by the bloom filters. But, response time is high due to reduced authentication level. Patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMA) was designed in [15] to access the personal health information with higher security. But, it fails to enhance the data confidentiality.

6. SUMMARY

An efficient Ensemble of Random Decision Trees with Bootstrap Aggregating (ERDT-BA) technique is designed to enhance the user authentication to secure cloud service provisioning with minimum time. By using bagging ensemble classifier, confidential cloud service provisioning is achieved. Here, Random Decision Trees is combined with Bootstrap Aggregating technique for verifying the cloud user as legitimate or not with minimum false positive rate. After user verification, only legitimate users are permitted to access the data stored in cloud server. As a result, security of cloud data is increased and effectively improves the data confidentiality rate in a significant manner when compared to the other methods.

REFERNCES

[1] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li and Albert Y. Zomaya, "SeDaSC: Secure Data Sharing in Clouds", IEEE Systems Journal , Volume 11, Issue No.2, June 2017, Pages 395 – 404.

[2] Hong Liu, Huansheng Ning, Qingxu Xiong and Laurence T. Yang, "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, Volume 26, Issue No.1, January 2015, Pages 241 – 251.

[3] Sudha Devi Dorairaj and Thilagavathy Kaliannan, "An Adaptive Multilevel Security Framework for the Data Stored in Cloud Environment", Hindawi Publishing Corporation, Scientific World Journal, Volume 2015, 2015, Pages 1-11.

[4] Xuefeng Liu, Yuqing Zhang, Boyang Wang and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE Transactions on Parallel and Distributed Systems, Volume 24, Issue No.6, June 2013, Pages 1182-1191.

[5] D.I. George Amalarethinam and B. Fathima Mary, "Confidentiality Technique for Enhancing Data Security in Public Cloud Storage using Data Obfuscation", IJCTA, International Science Press, Volume 9, Issue No. 27, 2016, Pages 107-113.

[6] Aleksandar Hudic, Shareeful Islam, Peter Kieseberg and Edgar R. Weippl, "Data Confidentiality using Fragmentation in Cloud Computing", International Journal of Communication Networks and Distributed Systems, Volume 1, Issue No. 3/4, 2012, Pages 1-10.

[7] Shivali Munjal and Shelly Garg, "Enhancing Data Security and Storage in Cloud Computing Environment", (IJCSIT) International Journal of Computer Science and Information Technologies, Volume 6, Issue No.3, 2015, Pages 2623-2626.

[8] Victor Chang and Muthu Ramachandran "Towards achieving Data Security with the Cloud Computing Adoption Framework", IEEE transactions, 2015, Pages 1-14

[9] Dr. L. Arockiam and S. Monikandan, "A Security Service Algorithm to Ensure the Confidentiality of Data in Cloud Storage", International Journal of Engineering Research & Technology (IJERT), Volume 3 Issue No. 12, December 2014, Pages 1053-1058.

[10] Kulwinder Kaur and Vikas Zandu, "A Secure Data Classification Model for achieving Data Confidentiality and Integrity in Cloud Environment", International Journal on Computer Science and Engineering (IJCSE), Volume 8, Issue No.9, September 2016, Pages 362-369.

[11] Tamanna and Rajeev Kumar, "Secure Cloud Model using Classification and Cryptography", International Journal of Computer Applications, Volume 159, Issue No 6, February 2017, Pages 8-13.

[12] Rizwana Shaikha and Dr. M. Sasikumar, "Data Classification for achieving Security in cloud computing", Procedia Computer Science, Elsevier, Volume 45, 2015, Pages 493-498.

[13] Sushmita Ruj, Milos Stojmenovic and Amiya Nayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE Transactions on Parallel and Distributed Systems, Volume 25, Issue No. 2, February 2014, Pages 384-394.

[14] Raphael Barazzutti, Pascal Felber, Hugues Mercier, Emanuel Onica and Etienne Riviere, "Efficient and Confidentiality-Preserving Content-Based Publish/ Subscribe with Prefiltering", IEEE Transactions on Dependable and Secure Computing, Volume 14, Issue No.3, May-June 2017, Pages 308-325.

[15] Jun Zhou, Xiaodong Lin, Xiaolei Dong and Zhenfu Cao, "PSMPA: Patient Self-controllable and Multi-level Privacy-preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System", IEEE Transactions on Parallel and Distributed Systems , Volume 26, Issue No. 6, June 2015, Pages 1693 – 1703.