Original Research Paper Computer Science

CONFIDENTIAL CLOUD SERVICE PROVISIONING USING BOOSTING ENSEMBLE CLASSIFICATION BASED AUTHENTICATION

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

Dr.C.Chandrasekar Professor, Department of Computer Science, Periyar University, Salem, TN.

ABSTRACT A cloud computing is a promising computing equipment that allows the cloud user to manage the cloud information from wherever at every time. The cloud computing and storage resources based on meter basis are utilized by presenting a computing capability. Due to the presence of storage resources, security is not provided for cloud system to achieve data confidentiality and authenticity. Though, a client is not able to belief the cloud service provider to accumulate its data more securely within the cloud. In order to overcome the data security problem, a Boosting Ensemble Classification based Authentication (BECA) technique is introduced. The data confidentiality and security is enhanced for cloud service provisioning with minimum time in BECA Technique. Initially, BECA Technique performs Boosting Ensemble Classifier to attain higher security level in cloud computing. In addition to that, Bayes Optimal Classifier (i.e. Boosting Ensemble classifier) is combined with AdaBoost to classify the user request during the authentication of users in cloud computing. Then, the user request to cloud server is provided as authorized or unauthorized data for securing the cloud services. After the classification of user request, user authentication process is carried out to present user data required services to the subsequent cloud user. Thus, it resulted with improved cloud data security in a significant manner. According to the authentication process, when the cloud user is authorized then the data services is provided and unauthorized users are not able to store the data in cloud system. This in turns helps for attaining the improved data security and confidentiality rate of cloud service provider in an optimized manner. The performance analysis of proposed BECA Technique is conducted on parameters such as classification accuracy, authentication time, false positive rate, data security rate and data confidentiality rate. The experimental result shows that the BECA Technique achieves higher security and confidentiality rate of cloud service provisioning when compared to the state-of-the-art works.

KEYWORDS : Cloud service provisioning, Boosting Ensemble classifier, cloud users, AdaBoost algorithm and Bayes Optimal Classifier

1. INTRODUCTION

The cloud computing is the process of large scale distributed computing model to enhances the cost-effective and on-demand services. Thus it leads to improve the consideration in academic research and industry technology. Cloud computing is mostly used for distributing the applications as services over the Internet and those services are ensured by the hardware and systems software in the data centers. The combination of hardware and software system is utilized by cloud computing resources in network services. Therefore, the various cloud computing techniques were developed for attaining higher security.

Secure Data sharing (SeDaSC) method was introduced in [1] to encrypt the data using single encryption key. It prevents insider threats and other key was saved with the help of cryptographic server. But, data security and confidentiality rate with fine-grained access was decreased. A secure cloud storage system was presented in [2] with two authentication techniques namely Time-based One Time Password and Automatic Blocker Protocol. This authentication technique improves the data security but reduces data integrity level.

The layered model was constructed in [3] for confidentiality and security to the stored data in cloud computing. Here, confidentiality of sensitive data is maintained using cryptography algorithms. But classification accuracy was not considered. A confidentiality technique named as MONcryptto [4] was developed for securing the stored data in cloud computing. It performs higher data security but failed to improve data integrity. In [5], data in cloud computing was provided with high confidentiality. Though, data response time was increased.

A secure storage system was developed in [6] for providing security to the cloud. Here, the data was encrypted using RSA algorithm and digital fingerprint. Though, the data integrity rate was not improved. Neural Data Security Model (NDSM) [7] improves the confidentiality and security in cloud computing. But, NDSM fails data security rate. The secure user authentication framework [8] was designed with the application of two-factor authentication technology. Though, it provides minimum data integrity rate.

Message Digest-based Authentication (MDA) was introduced in [9] to presents the security issues in mobile cloud computing. It stores the data from various security attacks. However, false positive rate is increased. Authentication scheme using Chebyshev chaotic maps [10] improves certain security factors to identify the user links in cloud. But, data confidentiality level is reduced against various attacks. The issues presented in the existing literature such as reduced data security and data integrity level. In order to overcome such issues, Boosting Ensemble Classification based Authentication (BECA) technique is developed in cloud service provisioning. The main contribution of the research work is described as follows,

- Boosting Ensemble Classification based Authentication (BECA) technique is designed in cloud service provisioning. Based on Boosting Ensemble Classifier, the confidentiality and security of data of increased. Additionally, it performs user verification in a secured manner by classifying the user request to cloud server for accessing cloud data.
- With the application of Boosting Ensemble Classifier, the cloud users are authenticated to achieve higher classification accuracy by combining together with Adaboost. They protect the cloud data against unintended or unauthorized access. This helps for attaining the enhanced data security and confidentiality rate of cloud with better effectiveness.

The rest of the paper is structured as follows: In Section 2, Boosting Ensemble Classification based Authentication (BECA) 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. BOOSTING ENSEMBLE CLASSIFICATION BASED AUTHENTICATION TECHNIQUE

Cloud service provisioning system provides clouds storage system for grouping the data and individuals are stored with their data everywhere at anytime without any difficulty. The cloud users are reassured from the difficulty by contract out the data with local data storage and maintenance. The data security and confidentiality is main issue in cloud data storage. In order to improve the cloud data

security and confidentiality, cloud user authentication technique is needed. There are many research work were designed to authenticate the cloud users but they are not achieve higher confidential rate for cloud service provisioning.

Therefore, Boosting Ensemble Classification based Authentication (BECA) Technique is developed to overcome the above issues. Here, Bayes Optimal Classifier is grouped with Adaboost (i.e. Boosting Ensemble classifier). The cloud users are classified using Boosting Ensemble classifier when the request is transmitted to the cloud servers as authorized or unauthorized for securing the cloud services. Thus, it considerably authenticates cloud users for providing a confidential cloud services. The general architecture diagram of Boosting Ensemble Classification based Authentication (BECA) Technique is exposed in below figure 1.

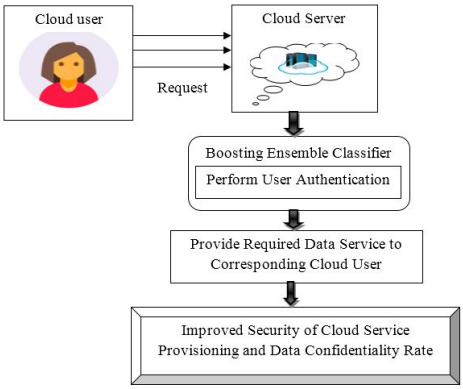

Figure 1 Architecture Diagram of Boosting Ensemble Classification Based Authentication Technique for Improving Data Confidentiality

Above figure 1 describes the structure of BECA Technique to achieve higher data confidentiality rate. At first, cloud user request is send to cloud server and then, Boosting Ensemble Classifier is used to authenticate the cloud users. During data authentication, when the user is authorized it provides a data to cloud users and if it is unauthorized, the data cannot be attained in cloud. Thus, the security of cloud service provisioning is improved with high data confidentiality rate. Initially, cloud user has to register his/her details to attain the data from cloud servers by sending a request. After receiving the request, user's ID and password is transmitted to cloud servers. After sending the client's ID, the authentication server checks whether the client is authenticated user or not. If it is authenticated user, cloud service provider provides the required data services. Thus, the process of proposed BECA Technique divided into three phases for confidential cloud service provisioning as follows.

1) Registration phase
2) Authentication phase
3) Service Provisioning phase

2.1 Registration Phase

In the beginning registration phase is used to register the user's details with cloud server. When user requests to cloud data, users are registered to the cloud server for authentication. The below figure explains the process involved in registration phases on the cloud.

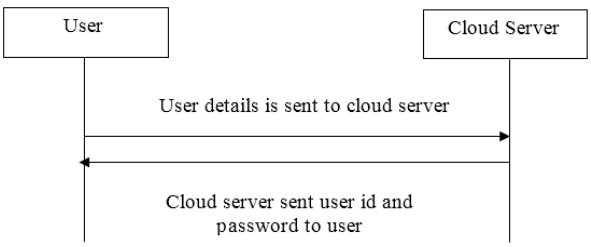

Figure 2 Processes Involved in Registration Phase

From the figure 2, initially the cloud server receives the user information such as user name, mail-id, and phone number etc after user request registration. Then, user information's are stored with the aid of user id and password in hashing table for authentication and attains higher data security in cloud service provisioning as shown in below table 1.

Table 1 Hash Table

User	Client-id	Password
User A	10011	*****
User B	10012	*****
User C	10013	*****

With the help of information stored in Hash table in table 1 about the users, BECA Technique proficiently authenticates the cloud user as authorized or unauthorized.

2.2 Authentication Phase

Next, Authentication phase is designed for authenticating the cloud users before providing the cloud services. In addition, Boosting Ensemble Classifier is developed to access the data stored on cloud and thus it improves the user authentication with higher classification accuracy. It efficiently classifies the cloud users as authorized or unauthorized by using information stored in hash table. After data classification, only the legal cloud users are allowed to access the data in an efficient manner. Below figure 3 describes the process of Boosting Ensemble classification for confidential cloud service provisioning.

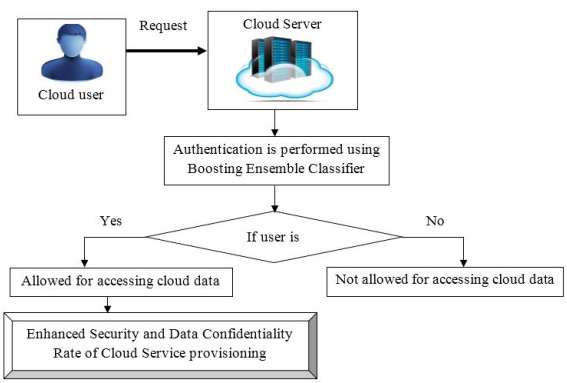

Figure 3 Process of Boosting Ensemble Classification for Confidential Cloud Service Provisioning

From above figure, cloud user sends a request to server and performs the boosting ensemble for data authentication. If the user is authorized, it permits cloud data accessing. After verifying the cloud user, it provides desired data services in cloud computing environment. As a result, the security and confidentiality rate of cloud service provisioning is improved.

2.2.1 Boosting Ensemble Classifier

Boosting Ensemble Classifier (Bayes Optimal Classifier) is combined with Adaboost for obtaining higher classification accuracy. When the true probabilistic distribution of data is known, Bayes Optimal Classifier is used which is the combination of all hypotheses in hypothesis space. The training dataset (i.e. user login information's) is sampled for each hypothesis with vote proportional likelihood. To assist training data of finite size, the product of each hypothesis and prior probability of that hypothesis (i.e. user information stored in hash table) is provided. The expression of Bayes Optimal Classifier for authenticating cloud user is given below.

$$y = \underset{c_j \epsilon C}{\operatorname{argmax}} \sum_{h_i \epsilon H} P(c_j/h_i) P(T/h_i) P(h_i) \quad (1)$$

From (1), the predicted class y is given with the set of all possible classes C along with hypothesis space H, a probability P and training

data T. In (1), the training data (i.e. user login information) is compared with user's information stored in hash table. Thus, it classifies the user as authorized or unauthorized person and the output is either '0' or '1' i.e. y∈{0,1}. From the output of Bayes Optimal Classifier, the authorized person is denoted as '1' whereas '0' specifies unauthorized person. This Classifier predicts the cloud users efficiently whereas misclassification error is occurred due to lack of classification accuracy of user authentication. Therefore, Ensemble of Bayes Optimal Classifier with Ad boost is designed for obtaining higher classification accuracy for cloud user verification.

Next, AdaBoost a machine learning meta-algorithm is used with the combination of other learning algorithms to improve classification performance. The AdaBoost algorithm is strong classifier for user authentication whereas other learning algorithm provides weak classifier output. Both outputs are combined by using AdaBoost technique. Here, Bayes Optimal Classifier classifies the cloud user as authorized or unauthorized and efficiently predicts the unauthorized cloud users with higher classification accuracy. Thus, the process of Boosting Ensemble classifier for efficient user authentication is shown below.

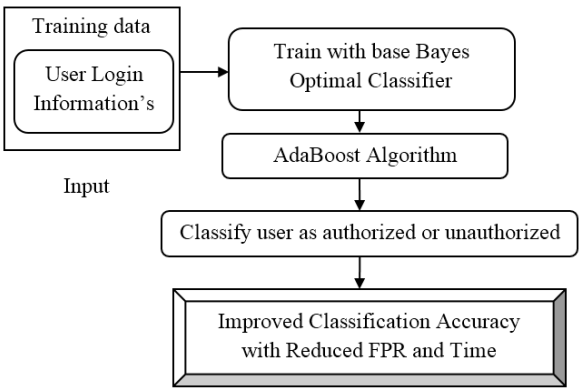

Figure 4 Process of Boosting Ensemble Classifier for Effectual User Authentication

The process of boosting ensemble classifier from figure 4 improves the classification performance of cloud user. Initially, training data (i.e. user login information) is provided as input with aid of ensemble learning algorithm as AdaBoost. Bayes optimal classifier classifies the users for obtaining the strong classifier with higher classification accuracy and reducing the authentication time.

Let us considered $\{(X_1, Y_1), (X_2, Y_2), \ldots (X_n, Y_n)\}$ is a collection of training data where X_i represents user's login information and Y_i denotes the target output class i.e $Y_i \in \{0, 1\}$. Here, the output $Y_i = 1$ is said to be an authorized cloud user and the output $Y_i = 0$ is said to be an unauthorized cloud user. Thus, the classifier determines probability with user's information stored in hash table to categorize the user as legitimate or illegitimate person. The weight (*wt*) of the training sample *x* is initialize as (*1/N*) which is mathematically formulated as below.

$$\sum_{i=1}^{N} wt_{x_i} = \frac{1}{N} \tag{2}$$

From (2), weight values is measured based on base classifier error. Using below formulation, the error rate is calculated.

$$ERR_r = \sum_{i=1}^{n} wt_{x_i}\ (x) \tag{3}$$

Then, the error value (β_x) of optimal classifier is mathematically expressed as follows.

$$\beta_x = \frac{1}{2}\ln\left(\frac{1-ERR_r}{ERR_r}\right) \tag{4}$$

From (4), β_x is adjustment coefficient that ensure cloud user authentication. Then, the weight of the each sample is restructured to achieve the maximum iteration which formulated as,

$$wt_i(x+1) = \frac{wt_i(x)\exp(-\beta_x Y_i h_x(X_i))}{N_f} \tag{5}$$

From (5), the new weight of sample is *wti* (x+1) and initial weight of sample is wt_i (*x*). Here, h_x denotes the prediction label of the *ith* component classifier and target output is Y_i with normalization factor N_f. Then, updated weight value is assigned as 1 and given as below.

$$\sum_{i=1}^{n} wt_i\ (x+1) = 1 \tag{6}$$

The weight function is compared with predetermined threshold(wt_{TH}) using (6). The strong classifier classifies the cloud users with the help of weight threshold value and classified as either legitimate or illegitimate. To improve classification performance, an ensemble of Bayes Optimal Classifier with AdaBoost is utilized. Adaboost algorithm is a strong classifier and it is mathematically formulated as below equation.

$$Y_i = sign\ (\sum_{x=1}^{T} \beta_x\ h_x(X_i)\ ) \tag{7}$$

By using (7), Bayes Optimal Classifier with AdaBoost is utilized to assemble base classifiers and generating the accurate user authentication technique. From expression, Y_i indicates the target strong classifier outputs. The output of strong classifier is as follows.

$$Y_i = \begin{cases} 1 & legitimate\ cloud\ user \\ 0 & ilegitimate\ cloud\ user \end{cases} \tag{8}$$

The algorithmic process included in Boosting Ensemble Classifier for authorizing the cloud user is described in below algorithm.

// Boosting Ensemble Classification based authentication Algorithm
Input : $\{(X_1, Y_1), (X_2, Y_2), \ldots (X_n, Y_n)\}$ is a set of training sample i.e. contains the multiple users login information's to cloud server
Output : Improved Classification Accuracy with Minimum Time and Reduced FPR
Step 1: **Begin**
Step 2: Initialize the weight of training sample (1/N) using (2)
Step 3: **For** each user login information
Step 4: Compute error to obtain optimal weight using (3)
Step 5: Assign the weight of the sample (i.e. user login information) after evaluating the error using (4)
Step 6: Update the weight value using (5)
Step 7 : **If** $(wt_x > \delta)$ (then
Step 8: Train a Boosting Ensemble Classifier for discovering the authorized user
Step 9: Constructs strong classifier
Step 10: **If** strong classifier output is $Y_i = 1$ **then**
Step 11: The user is legitimate
Step 12: **else**
Step 13: The user is illegitimate
Step 14: **End if**
Step 15: **End if**
Step 16: **End for**
Step 17: **End**

Algorithm 1 Boosting Ensemble Classification based Authentication

Algorithm 1 explains the Bayes optimal classifier with Adaboost to classify the cloud user as legitimate or not with minimum time. At first, error value for training data is measured for each user using login information through weighted sample. Then, weighted sample and threshold value is compared. When it is higher value, authorized user is determined using boosting ensemble classifier. As a result, it significantly classifies the users as either legitimate or illegitimate during cloud service provisioning. Hence, false positive rate of user authentication is reduced and improves the classification accuracy with minimum authentication time.

2.3 Service Provisioning phase

At last, service provisioning phase is used for presenting the required services to cloud user. The algorithmic process of authentication based service provisioning is explained below.

// Authentication Based Service Provisioning Algorithm
Input: User Request UR_i
Output: Improved Security and Data Confidentiality Rate
Step 1: Begin
Step 2: For each user request
Step 3: Authentication is performed using boosting ensemble classifier
Step 4: If user is authorized**, then**
Step 5: cloud user is allowed for accessing cloud data from cloud server
Step 6: else
Step 7: cloud user is not allowed for accessing cloud data from cloud server
Step 8: End if
Step 9: End for
Step 10: End

Algorithm 2 Authentication Based Service Provisioning Algorithm

Authentication Based Service Provisioning Algorithm in algorithm 2 initially verifies the each user for accessing cloud data with use of boosting ensemble classifier. If the cloud user is an authorized, then required data service is provided. Else, the cloud users are not allowed to access the cloud data. Thus, only authorized cloud users are able to access the cloud data stored in cloud server. Therefore, BECA Technique significantly enhances the security and confidentiality rate of cloud data service provisioning.

3. EXPERIMENTAL EVALUATION

A Boosting Ensemble Classification based Authentication (BECA) Technique is implemented in Java language using Amazon EC2 Dataset. The simulation is performed for many instances with respect to different number of cloud users, cloud data size. The performance evaluation of BECA Technique compared with existing approach Secure Data Sharing in Clouds (SeDaSC) [1] and Secure Cloud Storage System [2]. The following metrics such as Classification accuracy, false positive rate and Data Confidentiality rate are evaluated to improve the performance of BECA Technique.

4. RESULT ANALYSIS

The result analysis of proposed BECA Technique is performed with existing SeDaSC [1] and Secure Cloud Storage System [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 Impact of Classification Accuracy

Classification Accuracy is defined as the ratio of number of correctly classified cloud user's as authorized or unauthorized to the total number of cloud users taken as input. It is measured in terms of percentages (%) and formulated as follows,

$$Classification\ Accuracy = \frac{number\ of\ correctly\ classified\ cloud\ user's}{total\ number\ of\ cloud\ users} * 100 \quad (9)$$

Table 1 Tabulation for Classification Accuracy

Number of Cloud Users	Classification Accuracy (%)		
	SeDaSC	Secure Cloud Storage System	BECA Technique
10	72.15	78.68	83.56
20	73.26	79.56	84.85
30	74.62	80.91	85.72
40	75.84	81.98	86.86
50	76.35	82.32	87.23
60	76.92	83.24	87.98
70	79.98	86.65	91.35
80	81.73	87.98	92.02
90	83.16	89.13	93.12
100	84.39	90.55	94.18

Table 1 describes the classification accuracy with respect to number of cloud users based on proposed BECA Technique with existing SeDaSC [1] and Secure Cloud Storage System [2]. The number of cloud user is varied from 10 to 100. The BECA Technique improves the classification accuracy than the existing methods.

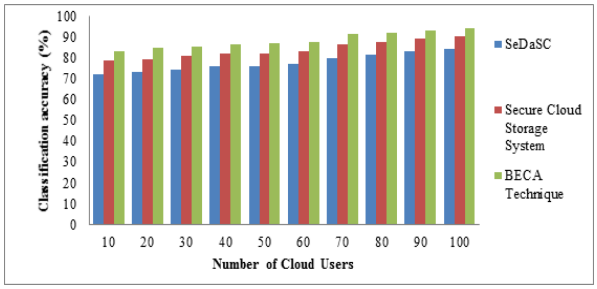

Figure 5 Measurement of Classification Accuracy

Figure 5 illustrates the performance analysis of classification accuracy with the number of cloud users in cloud environment. As shown in figure, proposed BECA Technique provides better classification accuracy for authenticating the cloud users than other existing methods. This is because of Boosting Ensemble Classifier application in BECA Technique for ensuring the cloud user as authorized or unauthorized. By combining weak Bayes optimal classifiers, accurately predict the authorized cloud users and enhances the classification accuracy. Therefore, the classification accuracy is significantly increased by 14% and 5% when compared to existing SeDaSC [1] and Secure Cloud Storage System [2] respectively.

4.2 Impact of False Positive Rate

The fraction of number of incorrectly classified cloud user's as authorized or unauthorized to the total number of cloud users is defined as false positive rate. It is measured in terms of percentages (%).

$$False\ Positive\ Rate = \frac{incorrectly\ classified\ cloud\ user's}{total\ number\ of\ cloud\ users} * 100 \quad (11)$$

Table 2 Tabulation for False Positive Rate

Number of Cloud Users	False Positive Rate (%)		
	SeDaSC	Secure Cloud Storage System	BECA Technique
10	39.65	35.89	31.92
20	40.9	37.12	32.89
30	42.12	38.38	34.41
40	44.59	40.21	35.98
50	46.65	42.9	38.54
60	49.06	45.26	39.99
70	51.35	47.8	43.02
80	54.16	49.68	45.25
90	55.98	52.56	48.16
100	58.23	54.26	50.18

Table 2 clearly describes the false positive rate with the number of cloud users in cloud environment. The false positive rate is significantly reduced using BECA Technique than the existing SeDaSC [1] and Secure Cloud Storage System [2]. A performance result of false positive rate is shown in below figure 6.

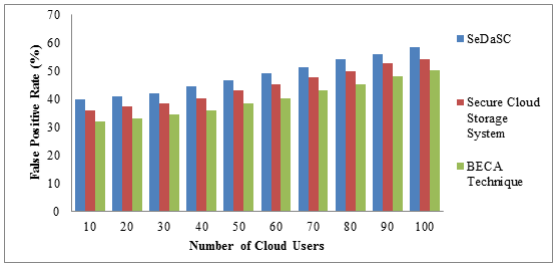

Figure 6 Measurement of False Positive Rate

As shown in figure 6, the false positive rate with respect to number of cloud users is illustrated. The false positive rate is considerably reduced than the existing methods. With the application of Boosting Ensemble Classifier in BECA Technique, false positive rate for authenticating cloud users is reduced. The Boosting Ensemble Classifier builds strong classifier for effective cloud user authentication. Thus, it helps to minimize false positive rate for classify the users in cloud. Therefore, the false positive rate is significantly minimized by 17% and 10% when compared to existing SeDaSC [1] and Secure Cloud Storage System [2] respectively.

4.3 Impact of Data Confidential Rate

The data confidentiality rate measures the capability of the system to transmit the secured data and only accessed by the authorized user. It is expressed in terms of percentage (%).

Table 3 Tabulation for Data Confidential Rate

Size of Data (MB)	Data Confidential Rate (%)		
	SeDaSC	Secure Cloud Storage System	BECA Technique
50	65.41	71.35	76.22
100	67.36	72.95	77.84
150	69.35	75.1	79.38
200	70.53	76.68	81.47
250	72.99	79.03	83.66
300	75.47	81.02	85.92
350	77.44	83.62	87.61
400	79.38	85.82	89.97
450	81.23	87.23	91.28
500	82.67	87.92	92.17

As listed in table 3, BECA Technique measures the data confidentiality rate on cloud infrastructure to provide the secured services. The confidentiality is measured based on varied number of cloud data size in the range of 50-500 using three methods.

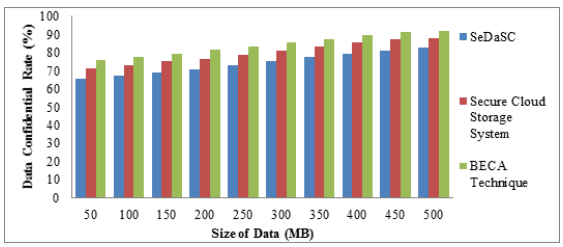

Figure 7 Measures of Data Confidential Rate

Figure 7 illustrates the experimental analysis of data confidentiality rate. It is measured with respect to number of cloud data with various sizes. From the figure, it is evident that the proposed BECA technique increases the data confidentiality rate than the existing methods. This is owing to usage of boosting ensemble classifier. With the aid of boosting ensemble classifier, only authorized cloud users are permitted for obtaining data stored in cloud. Therefore, BECA technique enhances the data confidentiality rate in cloud service provisioning. Thus, the data confidentiality rate is significantly increased by 14% and 6% when compared to existing SeDaSC [1] and Secure Cloud Storage System [2] respectively.

5. RELATED WORKS

A secure authentication scheme was presented in [11] to obtain session key security (SK-security) and avoid attacks in distributed mobile cloud computing services. But, it increases the authentication time. Security protocol data storage was explained in [12] to achieve efficient secure transmission in cloud environment. But, it failed to consider the data confidentiality rate

The boosting supervised machine learning approach [13] was used to attain secure data classification model. Here, multilevel authentication scheme was enclosed on the base of various users to enhance accuracy and reduces classification time. But, false positive rate was not considered. The structure of cloud-based and patient-centered personal health record (PHR) was developed in [14] to avoid the threats of information security. Though, confidentiality rate is reduced. In [15], convergent encryption technique was designed to enhance the confidentiality of sensitive data. But, it failed to achieve higher data security rate.

6. SUMMARY

Therefore, data security and confidentiality of cloud service provisioning with minimum time is attained by developing a Boosting Ensemble Classification based Authentication (BECA) technique. In the beginning, Boosting Ensemble Classifier is applied to enhance authentication result in cloud service provisioning. Then, Bayes Optimal Classifier is combined with AdaBoost for obtaining higher classification accuracy with reduced false positive rate. With the application of Boosting Ensemble Classifier, cloud data is protected from an unintended or unauthorized user. Experimental evaluation is carried out with the parameters such as Classification accuracy, false positive rate and Data Confidentiality rate. The result shows that the BECA Technique improves data confidentiality rate with minimum false positive rate. Similarly, the classification accuracy provides more accurate results for confidential cloud service provisioning than the state-of-the-art methods.

REFERENCES:

[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] Sheren A. El-Booz, Gamal Attiya and Nawal El-Fishawy, "A secure cloud storage system combining time-based one-time password and automatic blocker protocol", EURASIP Journal on Information Security, Springer , June 2016, Pages 1-13.

[3] Khalid El Makkaoui, Abdellah Ezzati, Abderrahim Beni-Hssane and Cina Motamed, "Data Confidentiality in the World of Cloud", Journal of Theoretical and Applied Information Technology", Volume 84, Issue No.3, February 2016, Pages 305-314.

[4] S. Monikandan and L. Arockiam, " Confidentiality Technique to Enhance Security of Data in Public Cloud Storage using Data Obfuscation", Indian Journal of Science and Technology, Volume 8, Issue No.24, September 2015, Pages 88-97.

[5] Mr. Chandan B and Mr. Vinay Kumar K, "Cloud Computing Systems: Confidentiality Protection of Data", International Journal of Computer Science Trend s and Technology (IJCST), Volume 3, Issue No. 6, Nov-Dec 2015, Pages 105-108.

[6] Nithya Chidambaram, Pethuru Raj, K. Thenmozhi, and Rengarajan Amirtharajan, "Enhancing the Security of Customer Data in Cloud Environments Using a Novel Digital Fingerprinting Technique", Hindawi Publishing Corporation, International Journal of Digital Multimedia Broadcasting, Volume 2016, May 2016, Pages 1-6.

[7] S. Jegadeeswari, Dr. P. Dinadayalan and Dr.N.Gnanambigai, "Enhanced Data Security Using Neural Network in Cloud Environment", International Journal of Applied Engineering Research, Volume 11, Issue No.1, 2016, Pages 278-285.

[8] Rui Jiang, "Advanced Secure User Authentication Framework for Cloud Computing", International Journal on Smart Sensing and Intelligent Systems, Volume 6, Issue No. 4, September 2013, Pages 1700-1724.

[9] Saurabh Dey, Srinivas Sampalli and Qiang Ye, "MDA: message digest-based authentication for mobile cloud computing", Journal of Cloud Computing, Springer, Volume 5, Issue No.18, December 2016, Pages 1-13.

[10] Suye Namasudra and Pinki Roy, "A new secure authentication scheme for cloud computing environment", Willey, Concurrency and Computation: Practice and Experience, April 2016, Pages 1-20.

[11] Vanga Odelu, Ashok Kumar Das, Saru Kumari, Xinyi Huang and Mohammad Wazid, "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services", Future Generation Computer Systems, Elsevier, Volume 68, March 2017, Pages 74-88

[12] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou and Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, Volume 22, Issue No. 5, May 2011, Pages 847-859.

[13] Amanpreet Singh, Dr. Manju Bala and Supreet Kaur, "Classification Of Data Using Multi-Level Authentication In Cloud Computing", International Education and Research Journal (IERJ), Volume 3, Issue No.5, May 2017, Pages 114-117.

[14] Shyh-Wei Chen, Dai Lun Chiang,Chia-Hui Liu, Tzer-Shyong Chen,Feipei Lai,Huihui Wang and Wei Wei, "Confidentiality Protection of Digital Health Records in Cloud Computing", Journal of Medical Systems, Volume 40, Issue No.5, May 2016.
[15] Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P.C.Lee and Wenjing Lou, " A Hybrid Cloud Approach for Secure Authorized Deduplication", IEEE Transactions on Parallel and Distributed Systems, Volume 26, Issue No.5, May 2015, Pages 1206-1216.