ISSN: 0974-5823 Vol. 6 No. 3 December, 2021

International Journal of Mechanical Engineering

FAST AND FRUGAL RANDOM FOREST DECISION TREE CLASSIFIER BASED CLOUD USER AUTHENTICATION FOR SECURE CLOUD IOT SERVICES

[1]S.Sivakamasundari, [2]Dr.K.Dharmarajan

[1]Research Scholar, School of Computing Sciences, VISTAS, Chennai, India

[1]Assistant Professor

New Prince Shri Bhavani Arts and Science College

[2]Associate Professor, Dept.of Information Technology, VISTAS

ABSTRACT

Authentication is essential to increase the cloud security through validating the identity of user. A Fast and Frugal Random Forest Decision Tree Classifier based Cloud User Authentication (FFRFDTC-CUA) method is proposed in this paper for secured cloud service provisioning with higher data secrecy and decrease time consumption which comprises of three phases, namely registration phase, authentication phase and data access phase. FRFDTC-CUA method authenticates that cloud user is an authorized or unauthorized by using fast and Frugal Random Forest Decision Tree Classifier (FFRFDTC). Experimental evaluation of FFRFDTC-CUA method is carried out on factors such as validating accurate authentication, error rate, response time and data secrecy rate with respect to number of cloud user request and data.

Keywords: Authentication, Fast and Frugal Decision Trees, Majority Vote, Random Forest, Strong Classifier, User Requests

1. INTRODUCTION

With the rapid increase of connected objects, IoT has played a vital place. But, the restriction of objects limits the development of IoT which become the key barrier for wide range implementation of objects. Cloud computing is a method for the analysis and repository of a huge volume of information. But, the combination of Internet of things and cloud computing provides guarantee and secrecy confront. As a result, an authentication mechanism is required.

Lightweight IoT-based authentication scheme [1] was used for Internet of things-based framework with cloud host. But, the authentication accuracy was not enhanced. An Attribute-based Encryption (ABE) scheme [2] was used for IoT cloud to govern the data user credentials. Still, the time taken to respond was not reduced during access control.

A Chinese Remainder Theorem (CRT) was used [3] for performing data storage process in cloud databank. However, this scheme was not succeed to reduce the computational complication over the cloud and IoT-based applications. Lightweight mechanism was employed [4] to validate users at runtime. But, user authentication accuracy was lower.

A new light-weight authentication and authorization architecture for distributed IoT environment with help of Elliptical Curve Cryptography (ECC) was implemented in [5]. However, time complexity involved during the authentication was higher. A design of secure fine-grain access control system was in [6] for protecting an outsourced cloud information in IoT environments. But, the inaccurate authentication of cloud user requests was higher.

A machine Learning-based authentication structure was used in [7] to authorize user devices with more accuracy and less overhead. However, higher was not obtained during the cloud IoT service provisioning process. Another light weight authentication protocol was developed in [8] to access private information securely in distributed cloud environment. But, the access of authorized user ratio of cloud data was poor.

A secure lightweight mutual authentication was intended in [9] for IoT smart home environment. However, authentication performance was not sufficient. For discovering, authenticating and authorizing smart objects and thereby managing access of end users in IoT services a novel method was presented in [10]. But, computational complexity involved during the secure access of users was not reduced. FFRFDTC-CUA method is proposed with help of random forest concepts and fast and frugal decision tree (FFDT).

2. FAST AND FRUGAL RANDOM FOREST DECISION TREE CLASSIFIER BASED CLOUD USER AUTHENTICATION METHOD

Several user authentication techniques are designed in conventional works to avoid unauthorized access to cloud information. Still, validation performance of conventional classification algorithm was not adequate to attain higher data confidentiality level in cloud. In order to get higher authentication accuracy through classifying a cloud users , a Fast and Frugal Random Forest Decision Tree Classifier based Cloud User Authentication (FFRFDTC-CUA) method is designed in this work.

A random forest applied in FFRFDTC-CUA method is an ensemble learning algorithm where it employs the bagging technique. By using random forest algorithmic concepts, FFRFDTC-CUA method constructs many FFDT result for the subset of the user requests made on cloud server and unites the output of all the trees. Thus, FFRFDTC-CUA method decreases overfitting problem in base fast and frugal decision trees and also reduces the variance and therefore improves the authentication accuracy of users in cloud environment with minimal time complexity. The construction diagram of FFRFDTC-CUA model is presented in below Figure 1.

The architecture diagram of FFRFDTC-CUA method to get better user validation action in cloud through classification. In the above demonstration figure, FFRFDTC-CUA method contains three key phases namely registration phase, authentication phase, and data access phase. In the registration phase, the FFRFDTC-CUA method registers user's personal details and consequently gives unique ID and password to each cloud users.

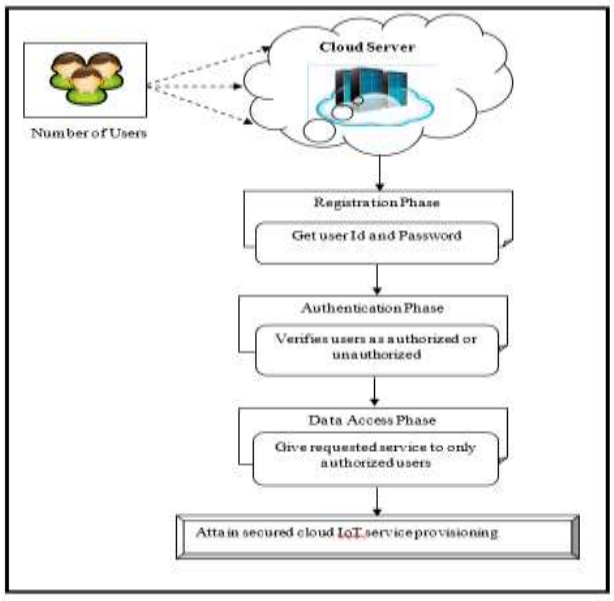

Figure 1 Architecture Diagram of FFRFDTC-CUA method

In the authentication phase, the FFRFDTC-CUA method verifies the user as authorized or not. During the data access phase, finally FFRFDTC-CUA method provides the user desired data services when the person is an authorized. From that, FFRFDTC-CUA method increases the security level of cloud IoT service provisioning with higher data confidentiality. The procedure of FFRFDTC-CUA model are explained in the lower subsections.

2.1 Registration Phase

Initially, users in a cloud register their individual details to the cloud server. For registration, each user sends his/her private details to cloud server. Then, cloud server stores details of users in its database and constructs a user ID, password. In FFRFDTC-CUA method, password comprises of the numeric values and special characters. The registered cloud user only provides the user ID and password using below,

$$CS \rightarrow (U_{id}, PWD) \quad (1)$$

From equation (1), 'CS' is a cloud server where 'U_{id}' points out user ID and 'PWD' is a password. For each registered users, the cloud server produces a unique user ID, password and to securely accessing data from cloud. The generated user ID 'U_{id}', password 'PWD' is stored in cloud server database for authentication purpose.

2.2. Authentication Phase

In FFRFDTC, final strong classifier result is obtained by training each base classifier (i.e. FFDT) on a training set sampled with replacement from the original training set. The FFRFDTC aggregates the individual FFDT predictions results to combine into a final prediction based on a majority votes and thereby design strong classifier for user authentication in cloud.

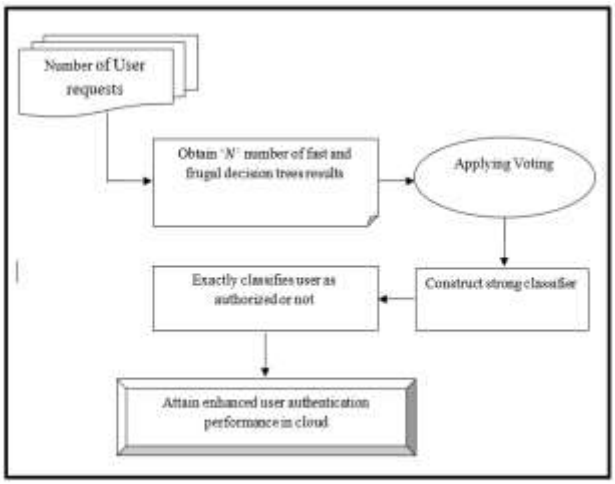

Figure 2 Authentication process using FFRFDTC

The authentication process using FFRFDTC is depicted in above Figure 2 . As demonstrated in the above figure, FFRFDTC initially obtains 'N' number of fast and frugal decision trees results for all user requests. In FFRFDTC, FFDT is a type of classification decision tree with sequentially ordered nodes. Here, every node includes two branches and one branch is an exit point. The final node in FFDT contains a two exit points to ensure that a decision is always made. The simplicity and transparency of FFDT make them useful where decision rules need to be quickly understood, implemented, communicated, or taught to decision makers. From that, FFDT carry out user authentication process through classifying an each user who gives request to the cloud server as authentic or not. Thus, FFDT classification result for each user request is mathematically obtained using below,

$$FT(\gamma_i) = \begin{cases} \text{If } ((U_{id} = {U_{id}}^*) \;\&\&\; (PWD = PWD^*)), & \textit{then user is authentic} \\ otherwise, & \textit{user is unauthentic} \end{cases} \quad (2)$$

From equation (2), 'U_{id}' and 'PWD' represents the user entered ID and passwords whereas '${U_{id}}^*$', 'PWD^*' indicates the user ID and passwords that are stored in cloud server

database. Whenever user ID and passwords is valid, then FFDT classifies the user as an authentic person. Otherwise, FFDT classifies the user as an unauthentic person in cloud. The classification performance of FFDT was lower to attain higher authentication accuracy. Hence, a random forest concept is applied in FFRFDTC-CUA method.

In FFRFDTC, Random forest is a supervised learning algorithm. By using the random forest algorithm, FFRFDTC generates 'N' number of fast and frugal decision trees results for each user request given to the cloud server using below,

$$FT(\gamma_i) = FT_1(\gamma_i) + FT(\gamma_i) + , \dots , + FT_N(\gamma_i) \qquad (3)$$

Consequently, FFRFDTC apply vote '$\$_i$' for all '$N$' fast and frugal decision trees results '$FT(\gamma_i)$' of each user request using below,

$$\$_i \rightarrow \sum_{i=1}^{N} FT(\gamma_i) \qquad (4)$$

Followed by, FFRFDTC finds majority votes of 'N' fast and frugal decision trees results for each cloud user request is discovered in order to design a strong classifier. Accordingly, strong classifier result for accurate user authentication in cloud environment is acquired using below,

$$\alpha_{\gamma_i} = arg \max_{N} \$(FT(\gamma_i)) \qquad (5)$$

From (5), 'α_{γ_i}' represents the strong classifier result obtained for cloud user request 'γ_i'. Here, '$arg \max_{N} \$$' helps for FFRFDTC to determine the majority votes of 'N' fast and frugal decision trees results. By using designed strong classifier, FFRFDTC exactly classifies each request sent by users in cloud environment as authorized or unauthorized with lower amount of time.

2.3 Data Access Phase

After completing the authentication process, data access phase is used in FFRFDTC-CUA method for providing the required services to users. The FFRFDTC-CUA method gives the needed cloud data services when the person is authorized in cloud environment.

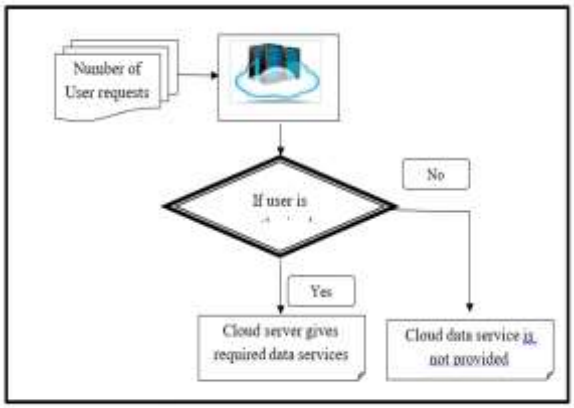

Figure 3 Flow Process in Data Access Phase

As presented in the above figure 3, FFRFDTC-CUA method does not allow the users to get the cloud services whenever user is an unauthorized. As a result, FFRFDTC-CUA method increases the authentication accuracy of user in cloud with a lower time. From that, FFRFDTC-CUA method get enhanced security level for cloud IoT services with minimal response time.

3. EXPERIMENTAL SETUP

For measuring the performance of proposed FFRFDTC-CUA and conventional two works [1] and [2], both methods are implememted in Java Launguage with CloudSim simulator by considering Amazon EC2 Dataset as input. To carry out an experimental evaluation, different numbers of cloud data and user requests from Amazon EC2 Dataset are taken. The experimental performance of FFRFDTC-CUA method is estimated in terms of authentication accuracy, error rate, response time and data confidential rate. The perfomance of FFRFDTC-CUA method is compared with two conventional methods namely Lightweight IoT-based authentication scheme and Attribute-based Encryption (ABE) scheme . The experimental evaluation of both proposed and existing methods are conducted for many instances with respect to varied number of cloud data and user requests and averagely ten results are depicted in below table and graph.

4. PERFORMANCE RESULT

In this section, the experimental perfomance result of FFRFDTC-CUA method is presented. The experimental result of FFRFDTC-CUA method is compared with Lightweight IoT-based authentication scheme and Attribute-based Encryption (ABE) scheme respectively using below parameters with the assist of tables and graphs.

4.1 Case 1: Authentication Accuracy

In FFRFDTC-CUA method, Authentication Accuracy '(AA)' estimates the ratio of number of user requests correctly verified as authorized or unauthorized to the total number of users requests. The authentication accuracy is determined as below,

$$AA = \frac{M_{EA}}{n} * 100 \qquad (6)$$

From equation (6), 'M_{EA}' shows the number of user requests exactly authenticated whereas 'n' refers to the total number of user requests. The authentication accuracy is calculated in terms of percentages (%). The experimental measure of authentication accuracy along with varied number of user requests using three methods is shown in below Table 1.

Table 1 Tabulation for Authentication Accuracy

Number of user requests (n)	Authentication Accuracy (%)		
	FFRFDTC-CUA method	Lightweight IoT-based authentication scheme	ABE scheme
25	92	80	76

50	94	82	74
75	96	83	72
100	95	83	75
125	97	84	73
150	96	81	75
175	98	85	79
200	94	83	78
225	97	88	80
250	98	89	82

Let us consider a 25 to 250 user requests from an input dataset with same experimental setup for implementing both the proposed FFRFDTC-CUA method and conventional Lightweight IoT-based authentication scheme [1] and Attribute-based Encryption (ABE) scheme [2]. The performance result of authentication accuracy in cloud using proposed FFRFDTC-CUA method is very higher while increasing the number of input user requests. Thus, it is considerable that the proposed FFRFDTC-CUA method achieves enhanced user authentication accuracy.

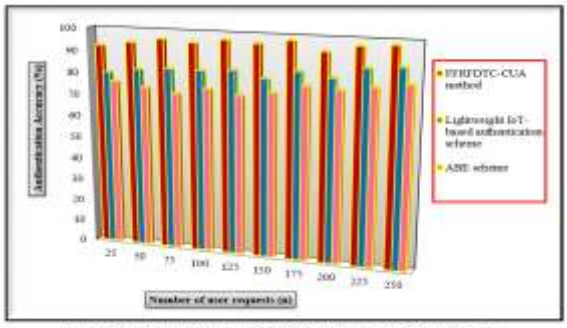

Figure 4 Graphical result of authentication accuracy versus number of user requests

Depends on the above acquired tabulation result of authentication accuracy, the graph is designed above in Figure 4. Figure 4 depicts performance result of authentication accuracy result based on diverse number of user requests in the range of 25-250 using three methods namely proposed FFRFDTC-CUA method and state-of-the-art Lightweight IoT-based authentication scheme and Attribute-based Encryption (ABE) scheme. As demonstrated in the above graphical figure, proposed FFRFDTC-CUA method attains enhanced authentication accuracy when compared to existing Lightweight IoT-based authentication scheme and Attribute-based Encryption (ABE) scheme . Thus, FFRFDTC-CUA method enhances the ratio of number of user requests precisely verified as authorized or unauthorized as compared to other two existing works. As a result, proposed FFRFDTC-CUA method improves the authentication accuracy of cloud IoT service provisioning by 14 % and 25 % when compared to Lightweight IoT-based authentication scheme and Attribute-based Encryption (ABE) scheme respectively.

4.2 Case 2: Error Rate

In FFRFDTC-CUA method, Error Rate '(ER)' determines the ratio of number of cloud user requests erroneously verified as authorized or unauthorized to the total number of cloud user requests. The error rate is measured using below,

$$ER = \frac{M_{WA}}{n} * 100 \qquad (7)$$

From equation (7), 'M_{WA}' denotes the number of cloud user requests wrongly authenticated whereas 'n' denotes to the total number of cloud user requests designed for experimental process. The error rate is computed in terms of percentages (%). The statistical result analysis of error rate is obtained during the user authentication process with respect to diverse number of user requests using three methods is depicted in below Table 2.

Table 2 Tabulation for Error Rate

Number of user requests (n)	Error Rate (%)		
	FFRFDTC-CUA method	**Lightweight IoT-based authentication scheme**	**ABE scheme**
25	8	20	24
50	6	18	26
75	4	17	28
100	5	17	25
125	3	16	27
150	4	19	25
175	2	15	21
200	6	17	22
225	3	12	20
250	2	11	18

In order to determine the performance of both the proposed FFRFDTC-CUA method and traditional Lightweight IoT-based authentication scheme and Attribute-based Encryption (ABE) scheme, different number of user requests in the range of 25 to 250 from an input dataset with similar experimental setting is considered. The error rate involved during the authentication process in cloud environment using proposed FFRFDTC-CUA method is very lower with increasing number of input user requests. Accordingly, it is clear that the proposed FFRFDTC-CUA method gets minimal error rate to effectively verify each user who access the data services from cloud when compared to other existing works. By using the above determine experimental result of error rate, the graph is intended in below Figure 5.

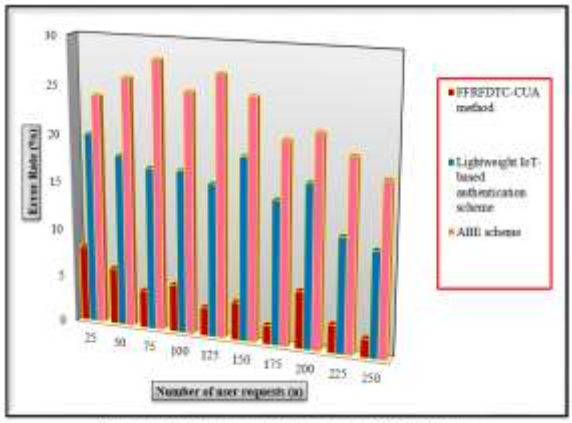

Figure 5 Graphical result of Error Rate versus number of user requests

Figure 5 shows comparative result of error rate according to varied number of user requests in the range of 25-250 using three methods namely proposed FFRFDTC-CUA method and state-of-the-art Lightweight IoT-based authentication

scheme and Attribute-based Encryption (ABE) scheme. As depicted in the above graphical design, proposed FFRFDTC-CUA method achieves lower error rate in order to accurately authenticate cloud users . Hence, proposed FFRFDTC-CUA method decreases the ratio of number of user requests incorrectly authenticated as authorized or unauthorized . Therefore, proposed FFRFDTC-CUA method reduces the error rate of cloud user authentication accuracy by 74 % and 82 % when compared to Lightweight IoT-based authentication scheme [1] and Attribute-based Encryption (ABE) scheme [2] respectively.

4.3 Case 3: Response Time

In FFRFDTC-CUA method, Response Time (RT) estimates the amount of time employed to give the required data services to cloud users from the cloud server. The response time is mathematically acquired using below,

$$RT = n * Time(RSUR) \quad (8)$$

From equation (8), the response time taken for securing cloud IoT services is evaluated. Here, 'n' denotes the total number of cloud user requests whereas '$Time(RSUR)$' indicates the time utilized for responding single user request data services. The response time is measured in terms of milliseconds (ms). The performance evaluation of response time is determined during the secured cloud service provisioning process based on varied number of user requests using three methods are described in below Table 3.

Table 3 Tabulation for Response Time

Number of user requests (n)	Response Time (ms)		
	FFRFDTC-CUA method	Lightweight IoT-based authentication scheme	ABE scheme
25	27	35	38
50	31	37	42
75	34	41	46
100	36	44	50
125	40	47	52
150	43	50	55
175	45	54	58
200	49	57	62
225	52	60	65
250	54	63	69

To measure the response time involved during the processes of secure cloud IoT service rendering, the proposed FFRFDTC-CUA method and Lightweight IoT-based authentication scheme and Attribute-based Encryption (ABE) scheme are implemented in Java language with similar experimental conditions. The response time in cloud using proposed FFRFDTC-CUA method is very minimal with increasing the number of input user requests. According to the above estimated experimental result, the graph is drawn in below Figure 6.

As represented in the above graphical depiction, proposed FFRFDTC-CUA method attains mininal response time to securely provide requested data services in cloud environment when compared to existing Lightweight IoT-based authentication scheme and Attribute-based Encryption (ABE) scheme .

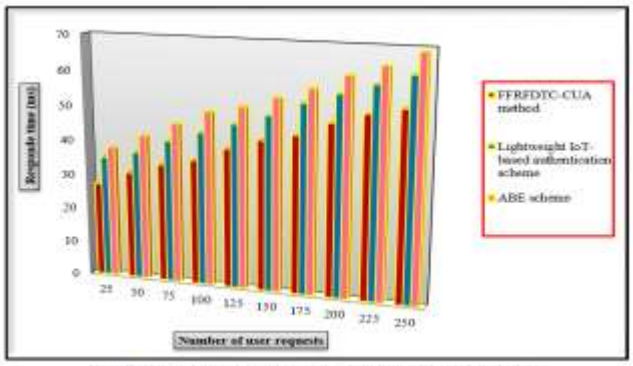

Figure 6 Graphical result of Response Time versus number of user requests

This is due to application of Fast and Frugal Random Forest Decision Tree Classifier in proposed FFRFDTC-CUA method on the contrary to conventional works. For this reason, proposed FFRFDTC-CUA method minimizes the amount of time utilized to provide the demanded data services to cloud users from the cloud server when compared to other two state-of-the-art works.Consequently, proposed FFRFDTC-CUA method decreases the response time of secure cloud IoT service provisioning by 16 % and 24 % when compared to Lightweight IoT-based authentication scheme and Attribute-based Encryption (ABE) scheme respectively.

4.4 Case 4: Data Confidential Rate

In FFRFDTC-CUA method, Data Confidential Rate '(DCR)' calculates ratio of the number of cloud data that are accessed only by authorized users to the total number of cloud data. The data confidential rate is mathematically determined as,

$$DCR = \frac{M_{CAAU}}{m} * 100 \quad (9)$$

From equation (9), 'M_{CAAU}' denotes the number of cloud data correctly obtained only by authorized users and 'm' denotes the total number of cloud data. The data confidential rate is determined in terms of percentages (%). The comparative measurement of data confidential rate in cloud environment according to diverse number of cloud data using three methods are portrayed in below Table 4.

Table 4 Tabulation for Data Confidential Rate

Number of cloud data (m)	Data Confidential Rate (%)		
	FFRFDTC-CUA method	Lightweight IoT-based authentication scheme	ABE scheme
20	90	80	75
40	93	85	80
60	92	87	83
80	94	88	85
100	95	82	80
120	93	83	79
140	94	85	82

160	96	88	85
180	95	88	86
200	97	90	88

With aim of evaluating the experimental result of data confidentiality rate in cloud, the proposed FFRFDTC-CUA method and existing Lightweight IoT-based authentication scheme [1] and Attribute-based Encryption (ABE) scheme [2] are implemented using same experimental situations by considering diverse number of cloud data. The performance of data confidentiality rate using proposed FFRFDTC-CUA method is higher while taking an increasing number of user requests as input. As a result, it is descriptive that the proposed FFRFDTC-CUA method acquires improved data confidentiality rate in cloud when compared to other conventional works. With the help of above obtained experimental result, the graph is plotted in below Figure 7.

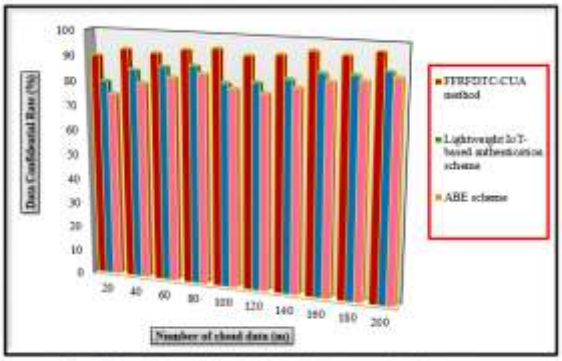

Figure 7 Graphical result of Data Confidential Rate versus number of user requests

Figure 7 explains statistical performance result measure of data confidentiality rate along with various number of cloud data in the range of 20-200 using three methods namely proposed FFRFDTC-CUA method and traditional Lightweight IoT-based authentication scheme [1] and Attribute-based Encryption (ABE) scheme [2]. As shown in the above graphical representation, proposed FFRFDTC-CUA method gets higher data confidentiality rate in cloud environment when compared to state-of-the-art Lightweight IoT-based authentication scheme [1] and Attribute-based Encryption (ABE) scheme [2]. This is because of Fast and Frugal Random Forest Decision Tree Classifier in proposed FFRFDTC-CUA method opposite to existing works [1] and [2]. Accordingly, proposed FFRFDTC-CUA method enhances proposition of the number of cloud data that are acquired only by authorized users when compared to other traditional works [1] and [2]. Thus, proposed FFRFDTC-CUA method increases the data confidentiality rate of cloud IoT services by 10 % and 14 % when compared to Lightweight IoT-based authentication scheme [1] and Attribute-based Encryption (ABE) scheme [2] respectively.

5. LITERATURE SURVEY

Anonymous Authentication method was implemented in [11] for improving performance of secure cloud computing services. But, authentication accuracy was not at required level. Data Access Control system was designed in [12] to get higher security for data access in the cloud with minimal computation overheads. However, time utilized for accurate user authentication was more.

A dynamic access control system was performed in [13] to get better privacy level in a cloud environment. Though, confidential level of data was lower. A Secure Data Sharing in Clouds (SeDaSC) method was designed in [14] with the objective of obtaining the cloud data confidentiality. But, the time required to secure the cloud data was higher

6. CONCLUSION

The FFRFDTC-CUA method is proposed with the objective of attaining improved security performance for cloud IoT services through user authentication. The goal of FFRFDTC-CUA method is obtained with help of Fast and Frugal Random Forest Decision Tree Classifier. The FFRFDTC-CUA method enhances classification accuracy of user authentication in cloud environment with minimal amount of time. The proposed FFRFDTC-CUA method increases the ratio of number of user requests perfectly verified as authorized or unauthorized as compared to other conventional works. In addition, proposed ADQBC-RHCDS Model lessens the amount of time taken to respond the required services to cloud users from the cloud server when compared to other traditional works.

REFERENCES

[1] Lu Zhou, Xiong Li, Kuo-Hui Yeh, Chunhua Su and Wayne Chiu, “Lightweight IoT-based authentication scheme in cloud computing circumstance”, Future Generation Computer Systems, Elsevier, Volume 91, Pages 244-251, February 2019

[2] Qi Xia, Emmanuel Boateng Sifah, Kwame Opuni-Boachie Obour Agyekum, Hu Xia, Kingsley Nketia Acheampong, Abla Smahi, Jianbin Gao, Xiaojiang Du, Mohsen Guizani “Secured Fine-Grained Selective Access to Outsourced Cloud Data in IoT Environments”, IEEE Internet of Things Journal, Volume 6, Issue 6, Pages 10749 – 10762, 2019

[3] Shengmin Xu, Guomin Yang, Yi Mu and Ximeng Liu, “A Secure IoT Cloud Storage System with Fine-Grained Access Control and Decryption Key Exposure Resistance”, Future Generation Computer Systems, Elsevier, Volume 97, Pages 284-294, 2019

[4] Balasubramanian Prabhu Kavin and Sannasi Ganapathy, “A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications”, Computer Networks, Elsevier, Volume 151, Pages 181–190, 2019

[5] Muhammad Kazim, Lu Liu, Shao Ying Zhu, “A Framework for Orchestrating Secure and Dynamic Access of IoT Services in Multi-Cloud Environments”, IEEE Access, Volume 6, Pages 58619 – 58633, October 2018

[6] Ankur Lohacha, Karambir, “ECC based inter-device authentication and authorization scheme using MQTT for IoT networks”, Journal of Information Security and Applications, Elsevier, Volume 46, Pages 1-12, June 2019

[7] P.Punithavathi, S.Geetha, MarimuthuKaruppiah, SK Hafizul Islam, Mohammad Mehedi Hassan, Kim-

Kwang RaymondChoo, “A lightweight machine learning-based authentication framework for smart IoT devices”, Information Sciences, Elsevier, Volume 484, Pages 255-268, May 2019

[8] Ruhul Amin, Neeraj Kumar, G.P.Biswas, R.Iqbal, Victor Chang, “A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment”, Future Generation Computer Systems, Elsevier, Volume 78, Part 3, Pages 1005-1019, January 2018

[9] Mohammed Alshahrani, Issa Traore, “Secure mutual authentication and automated access control for IoT smart home using cumulative Keyed-hash chain”, Journal of Information Security and Applications, Volume 45, Elsevier, Pages 156-175, April 2019

[10] Marta Beltrán, “Identifying, authenticating and authorizing smart objects and end users to cloud services in Internet of Things”, Computers & Security, Elsevier, Volume 77, Pages 595-611, August 2018

[11] Jia-Lun Tsai and Nai-Wei Lo, “A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services”, IEEE Systems Journal, Volume 9, Issue 3, Pages 805-815, 2015

[12] Xianglong Wu, Rui Jiang, and Bharat Bhargava, “On the Security of Data Access Control for Multi-authority Cloud Storage Systems”, IEEE Transactions on Services Computing, Pages 1-14, 2015

[13] Mansura Habiba, Md. Rafiqul Islam, A. B. M. Shawkat Ali, Md. Zahidul Islam, “A New Approach to Access Control in Cloud”, Arabian Journal for Science and Engineering, Springer, Volume 41, Issue 3, Pages 1015–1030, March 2016

[14] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, Albert Y. Zomaya, “SeDaSC: Secure Data Sharing in Clouds”, IEEE Systems Journal, Volume PP, Issue 99, Pages 1 – 10, 2015