Chi-Square Detective Ensembled Cardinal Gradient Bootstrap Aggregating Classifier for Secured Big Data Communication

S.L. Swapna
Research Scholar, Department of Computer Science, Hindusthan College of Arts and Science (Autonomous), Coimbatore, India

V. Saravanan
Professor and Head, Department of Information Technology, Hindusthan College of Arts and Science (Autonomous), Coimbatore, India

ABSTRACT
The application of big data analytics and related technologies like the Internet of Things (IoT) facilitates user intentions and behaviours as well as operational decision-making. Security is the major concern in the application of big data analytics to protect the system and secure the information as well as the data being handled. Conventional security techniques have become inefficient in terms of processing and identifying network threats in a reasonable amount of time. To deal with this problem, a unique Chi-Square Detective Ensembled Cardinal Gradient Bootstrap Aggregating Classifier based Secured Data Communication (CSDECGBAC-SDC) model with improved accuracy and lower time complexity is introduced. The CSDECGBAC-SDC model's core functions for enhancing security include user registration, data collection, and data communication. During the registration process, the user's information is initially registered. Following that, the CSDECGBAC-SDC model collects data from the enrolled user. The Chi-Square Detective Ensembled Cardinal Gradient Bootstrap Aggregating Classifier is used in the CSDECGBAC-SDC Model to accomplish user authentication for anyone who want to access the data. For detecting the authorized user, the ensemble technique uses a group of weak learners as a Tversky Indexive Chi-square automatic interaction detection decision tree. The weak learner results are combined. Finally, cardinal voting is applied to find the majority vote in data classification by using the gradient ascent function. This in turn helps to improve secured data communication. Experimental evaluation is carried out on factors such as classification accuracy, error rate, and classification time with respect to a number of users. The results indicate that the CSDECGBAC-SDC model effectively improves the classification accuracy with minimum error rate and classification time than the conventional approaches.

General Terms
Big Data, Communication, Data Security

Keywords
Secured Big data Communication, Tversky Indexive Chi-Square Automatic Interaction Detection, Ensembled Cardinal Gradient Bootstrap Aggregating Classifier, Cardinal Voting, Gradient Ascent Function

1. INTRODUCTION
IoT enables devices in a smart environment to communicate with each other. The extensive usage of IoT technology is employed for data acquisition. In addition, these devices are used in a variety of applications that are connected to the IoT network controlled remotely. Different factors need to be taken for IoT security solutions. Due to the large capability made available by big data technologies that enable user information transmitted securely through all communications. When the information is transmitted without authentication, adversaries are given the chance to break the privacy of the owner. Therefore, big data technologies consist of secure transmission of data by using machine learning techniques [1].

Homomorphic Block-Ring Security System (HBRSS) was designed in [2] for the security of data communication. But the access control method was not applied to improve the security level. A lightweight multi-factor authentication and authorization scheme in IoT cloud-based environment (LMAAS-IoT) was developed [3]. However, the IoT-based promising security solutions were not obtained.

A deep learning model was introduced in [4] for enhancing IoT security. But it failed to solve the challenges of improving the secure transmission of a big volume of data. A novel security risk analysis method was introduced in [5] for Big Data environments. However, it failed to apply the learning system in the cloud environment for security risk analysis.

Information Security Monitoring and Management scheme was developed in [6] with large Data for IoT Environment. But the access control algorithm was not applied for improving the security level by implementing the large volume of data. The network security and protection approach was introduced in [7] for big data. But it failed to design a network security system that accomplishes all big data requirements.

A Secure Authentication and Data Sharing in Cloud (SADS-Cloud) enabled Big Data Environment was introduced in [8]. But, the complexity of data sharing was not reduced by applying SADS-Cloud architecture. A hybrid unauthorized data handling (HUDH) method was introduced in [9] for big data in cloud computing. But the effective learning technique was not applied to further improve the security of big data handling. A data transmission technique was designed in [10] to provide secure communication of IoT infrastructure. The designed technique failed to increase the complexity of device-to-device communication in IoT infrastructure.

A flexible and efficient authentication method was introduced in [11] for heterogeneous IoT devices to provide security and privacy with better storage and computational ability. But the designed authentication method failed to provide better security to a system with communications between the IoT devices to further increase the transmission efficiency.

1.1 Major Contributions
In order to overcome the existing issues, a novel CSDECGBAC-SDC model is developed with the following contribution,

- A novel CSDECGBAC-SDC model is introduced to increase secure big data communication with minimum time consumption.
- First, the CSDECGBAC-SDC model is applied to accurately classify the authorized user and unauthorized during big data communication for enhancing security. The CSDECGBAC-SDC model uses the Chi-Square Detective Ensembled Cardinal Gradient Bootstrap Aggregating technique to categorize the authorized and unauthorized users based on the Tversky similarity index. After the classification using weak learners, the strong results are obtained by applying the cardinal voting scheme. Then apply the gradient ascent function to find the majority votes of classification results. In this way, authorized users are identified for secure data communication.
- An extensive experiment is carried out to estimate the performance of the CSDECGBAC-SDC model and other related works. The obtained result reveals that our proposed, CSDECGBAC-SDC model provides improved performance in terms of accuracy, error rate, and time.

1.2 Organization of the Paper

The rest of the paper is arranged into different sections as follows. Section 2 discusses the related works. Section 3 describes the process of the proposed CSDECGBAC-SDC technique with a neat architecture diagram. Section 4 presents the experimentation with the dataset description. In section 5, the performance results of the proposed technique and conventional methods are discussed. At last, Section 6 concludes the paper.

2. RELATED WORKS

A lightweight smartcard-based secure authentication (LS-BSA) method was developed in [12] for proving the security and minimizing the computation and communication costs. However, the IoT-based big data forensic system was not designed. A trusted collaborative framework was developed in [13] for AI-enabled IoTs, computation security, and transmission security. But the security level was not improved by the big data security access control algorithm.

A novel lightweight authentication method was introduced in [14] for a cloud-based IoT environment. But the accurate authentication was not performed with minimum time consumption. A new authentication method was designed in [15] for IoT Environments to achieve a high-security level and minimum computation cost. However, the method was not improved the security level with big data applications.

A three-factor authentication framework was developed in [16] for IoT-driven security analysis. But it failed to investigate a more refined approach for improving IoT security by applying the learning techniques. Secure lightweight authentication and key agreement protocol were designed in [17] for healthcare applications. But the optimal experimental designs, evaluation, big data handling were not considered.

A smart healthcare system was designed in [18] based on edge computing architecture for maintaining the privacy of patient data. But, the time complexity of authorized and unauthorized detection was not minimized. A secure and lightweight mechanism was designed in [19] for ensuring the security of device-to-device message transmission for the IoT-cloud system. The designed mechanism failed to preserve the message authentication.

A share generation model was introduced in [20] for enhancing the privacy of healthcare data among individuals. However, the designed model was not used for various applications in cloud data security. Efficient data distribution and secure data transmission were performed in [21] based on IoT. However, an effective learning system was not implemented to improve secure data transmission.

3. PROPOSED WORK

The Internet of Things (IoT) has become a significant technology that connects a large number of sensor devices to collect data based on the applications. Communications in IoT environments are carried out on wireless channels that are susceptible to various unauthorized access [22]. IoT devices generated enormous data stored that are accumulated into a storage server and shared between the users. The processing of secure data communication is a significant problem for the development of real-time analysis. Therefore, an efficient technique called the CSDECGBAC-SDC model is introduced to perform secure big data communication based on the ensemble learning technique.

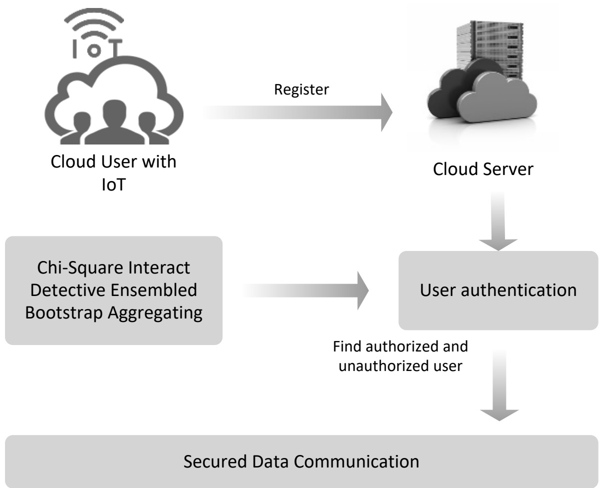

Fig.1: Architecture of the Proposed Cloud-Enabled CSDECGBAC-SDC Technique

Figure 1 illustrates the cloud-enabled CSDECGBAC-SDC technique used for secured big data communication. The architecture model comprises a number of cloud users '$CU = CU_1, CU_2, \dots, CU_n$' wants to store their big data '$D = D_1, D_2, \dots., D_n$' to a cloud server. First, the cloud user registers their details to the cloud server. The user wants to store their data on the cloud server. Whenever the user wants to access the data, they first verify their authenticity. Based on the user authentication, the cloud server finds the authorized or unauthorized user using the Chi-Square Interact Detective Ensembled Bootstrap Aggregating technique. The server permits the data to the authorized user and denied access to unauthorized users. The different process of the proposed CSDECGBAC-SDC technique is explained in the following subsections.

3.1 Registration

The proposed CSDECGBAC-SDC technique starts to perform the registration process before storing the big data into the cloud server. When the users want to store their data on the server, they first need to perform the registration. During the registration step, the user enters their personal information like the name, date of birth, age, gender, mobile number, and so on. The user's information's collected from the corresponding IoT is stored in the cloud server.

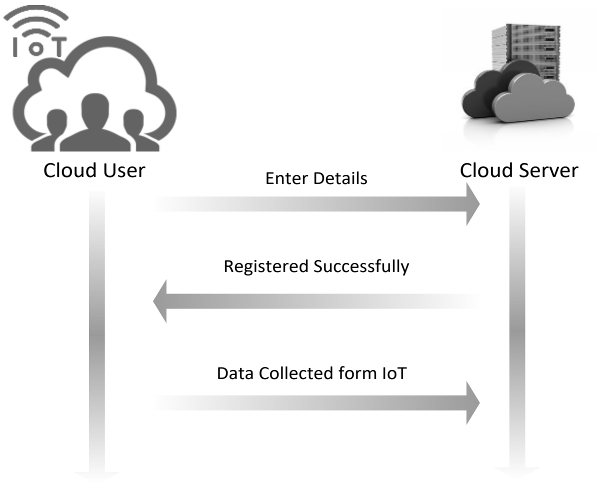

Fig. 2: Registration Process Flow

Figure 2 exhibits the registration process. First, the users enter their personal information and the data collected from the IoT. Let us consider the MHEALTH (Mobile HEALTH) dataset consisting of body motion and vital indications recordings for ten subjects while performing varieties of physical activities. Sensors (i.e. IoT) devices placed on the subject's chest, right wrist, and left ankle are employed to determine the activity experienced by various body parts of the subjects, namely, acceleration, rate of turn, and magnetic field orientation. The collected data are sent to the cloud server for further processing.

3.2 Chi-Square Interact Detective Ensembled Bootstrap Aggregating technique based user authentication

After the registration, the proposed CSDECGBAC-SDC technique performs the data collection at the cloud server by verifying the user authenticity. The authenticity of the user is identified by applying a Chi-Square Interact Detective Ensembled Bootstrap Aggregating technique. Bootstrap aggregating also termed bagging is a machine learning ensemble technique designed to improve the stability and accuracy of machine learning algorithms in statistical classification. The main aim of weak learners is combined to make a strong learner that attains better performance than a single one.

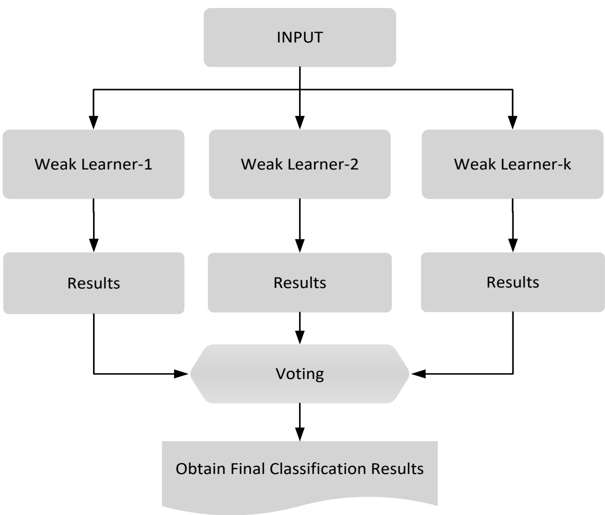

Fig. 3: Structure of the Chi-Square Interact Detective Ensembled Bootstrap Aggregating Technique

Figure 3 demonstrates the Chi-Square Interact Detective Ensembled Bootstrap Aggregating technique for accurate classification. The Ensemble technique consists of training sets $\{x_i, Y\}$ where x_i denotes an input sample (i.e. cloud users) and 'Y'represents an ensemble classification results. The Ensembled Bootstrap Aggregating classifier initially constructs a 'k' set of weak learners $\{w_1, w_2, w_3, \dots . w_k\}$. Here, the Chi-Square Interact Detective Decision Tree is used as a weak learner to categorize the cloud users as authorized or unauthorized. Tversky Indexive Chi-square automatic interaction detection decision tree is a classification tree is in which each internal (non-leaf) node is labeled with input. The arcs coming from a root node are connected to the leaf of the tree that the data set has been classified by the tree into either a specific class.

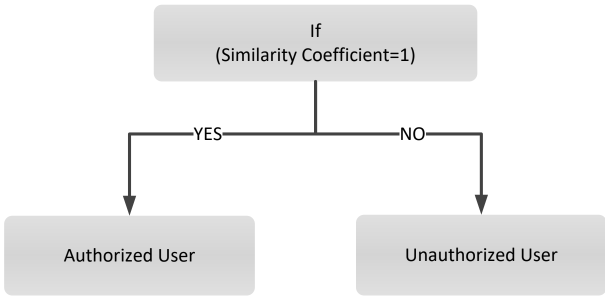

Fig. 4: Tversky Indexive Chi-square Automatic Interaction Detection Decision Tree

Figure 4 demonstrates the Chi-square automatic interaction detection decision tree that classifies the user into authorized or unauthorized. The proposed Chi-square automatic interaction detection decision tree uses a Tversky similarity index. The Tversky similarity index is used to measure the correlation between the two variables (i.e. receiver ID and registered ID) is measured as given below,

$$SI = \frac{RID \cap RegID}{P\,(RID \,\Delta\, RegID) + Q\,(RID \cap RegID)} \tag{1}$$

Where, SI indicates a Tversky similarity coefficient, RID denotes received ID, $RegID$ indicates a registered ID, $RID \cap RegID$ indicates a mutual dependence between the received ID and registered ID, $RID \,\Delta\, RegID$ indicates a variance between the received ID and registered ID. From (1), P and Q represent parameters of the Tversky index ($P, Q \geq 0$). The similarity coefficient (SI) provides the resultant value between [0, 1]. Based on the similarity, the Authorized and unauthorized users are correctly identified.

$$SI = \begin{cases} if[SI = 1] \;;\; Authorized\ user \\ if[SI = 0] \;;\; Unuthorized\ user \end{cases} \tag{2}$$

Where, if the two IDs get matched, the user is said to be authorized. Otherwise, the user is said to be an unauthorized user. In this way, the weak learner classifies the user into different classes.

The weak learner results have some training errors in the output. In order to get strong classification results, the classification results of weak learners are combined.

$$Y = \sum_{i=1}^{k} w_i \tag{3}$$

Where, Y designates the output of strong classification results, w_i indicates an output of the weak learners. For each weak learner, the training error is computed based on the squared difference between the actual classification results and observed classification results. The error rate is measured as given below,

$$Er = [R_A - R_o]^2 \tag{4}$$

Where, Er represents the error after the classification, R_A represents the actual output, R_o symbolizes the observed results. By applying the cardinal voting scheme, the weak learner results are rated based on the preference order according to the error value.

Table 1. Example of Cardinal Voting Based on Weak learner's Arrangement

Weak Learners	Preference Order
$\boldsymbol{w_1}$	First
$\boldsymbol{w_3}$	Second
$\boldsymbol{w_4}$	Third
$\boldsymbol{w_2}$	Fourth

Table 1 shows the order of the weak learners based on the error value. The weak learner 'w_1' rated in the order of the first position. It means that the weak learner 'w_1' has minimum error among the other weak learner. Likewise, the weak learners are ordered second, three, four according to the error value. After the rating process, the votes are registered to find accurate classification results that have minimum errors. The strong classification results are obtained by finding the majority votes based on finding the local maximum of that function. This process is then called gradient ascent.

$$Y = \arg\max_{b} R\,(w_i) \tag{5}$$

Where Y represents the strong classification results, $arg\ max$ indicates an argument of the maximum function (i.e. gradient ascent) to find out the majority vote (R) of the classification result whose decision is known to the kthclassifier. In this way, accurate classification results are obtained.

Algorithm 1 describes the step-by-step process of secure data communication using the Chi-Square Detective Ensembled Cardinal Gradient Bootstrap Aggregating technique. In the registration phase, the user sends their details to the server. Accordingly, the server generates a successfully registered message for the registered user. Then the user stores the details collected from the IoT. The user wants to access the data from the server. The cloud server first verifies the authenticity of the user using the Tversky similarity coefficient. The similarity returns '+1' and then the user is said to be authorized. Otherwise, the user is said to be unauthorized. Finally, the cloud server provides the data to the authorized user. Otherwise, the cloud server denied the data to unauthorized users. In this way, secure data transmission between server and user is performed.

Algorithm 1. Chi-Square Detective Ensembled Cardinal Gradient Bootstrap Aggregating Classifier based Secured Data Communication

Input: Dataset '$\boldsymbol{DS}$', IoT device '$\boldsymbol{S = S_1, S_2, \dots, S_n}$'
Cloud user's '$\boldsymbol{CU = CU_1, CU_2, \dots, CU_n}$'
Big data '$\boldsymbol{D = D_1, D_2, \dots, D_n}$'
Cloud server '$\boldsymbol{CS}$'
Output: Secured Data Communication

Begin
For each user '$\boldsymbol{CU}$'
  Enter the details to '$\boldsymbol{CS}$'
  Enter the details to '$\boldsymbol{CS}$'
Store the details collected from IoT
End for
$\boldsymbol{CS}$ generates the successfully registered message
For each user '$\boldsymbol{CU}$'
  Collect the data from '$\boldsymbol{CS}$'
  $\boldsymbol{CS}$ validate the user detail
  Apply ensemble technique
  Construct 'k' number of weak learners
  Construct the decision tree
  Measure the similarity '$\boldsymbol{SI}$'
  $\boldsymbol{if}$ ($\boldsymbol{SI = +1}$) then
  The cloud user is said to be an authorized user
  Perform secure data communication
else
cloud user is said to be an unauthorized user
No data communication between cloud users
End if
End for
End

4. EXPERIMENTAL SETUP

Experimental evaluation of the proposed CSDECGBAC-SDC method and the existing HBRSS [1] LMAAS-IoT [2] is implemented in the Java language via CloudSim simulation. In order to experiment, secure big data communication between the cloud users was performed using the MHealth dataset collected from https://www.kaggle.com/datasets/gaurav2022/mobile-health. The dataset consists of 14 attributes and 12,15,745 instances. The main aim of the dataset is to record several physical activities for ten volunteers of diverse profiles. The ten volunteers generate many data (i.e. instances) and these data are communicated to the authorized entity.

Table 2. Attributes Description

S. No	Attrib-utes	Description
1	alx	Acceleration from left-ankle sensor (X axis)
2	aly	Acceleration from left-ankle sensor (Y axis)
3	alz	Acceleration from left-ankle sensor (Z axis)
4	glx	Gyro from the left-ankle sensor (X axis)
5	gly	Gyro from the left-ankle sensor (Y axis)
6	glz	Gyro from the left-ankle sensor (Z axis)
7	arx	Acceleration from right-ankle sensor (X axis)
8	ary	Acceleration from right-ankle sensor (Y axis)
9	arz	Acceleration from right-ankle sensor (Z axis)
10	grx	Gyro from the right-ankle sensor (X axis)
11	gry	Gyro from the right-ankle sensor (Y axis)
12	grz	Gyro from the right-ankle sensor (Z axis)
13	Activity	Corresponding activity
14	Subject	Volunteer subjects (1 – 9)

5. RESULTS AND DISCUSSIONS

In this section, the performance of the proposed

CSDECGBAC-SDC method and the existing HBRSS [1] LMAAS-IoT [2] are discussed. The performance of the proposed CSDECGBAC-SDC method is analyzed based on the following parameters as Classification Accuracy, error rate, and Classification time. The performance of these parameters is analyzed with the help of a table and graphical representation.

5.1 Impact of Classification Accuracy

Classification accuracy is measured as the ratio of the number of cloud users that are accurately classified as authorized or unauthorized for secure data communication. This classification accuracy is formulated as follows,

$$CA = \left[\sum_{i=1}^{n} \frac{CU_{AC}}{CU_i}\right] * 100 \qquad (6)$$

From the above equation (6), the classification accuracy 'CA' is measured based on the number of cloud users accurately classifiedCU_{AC}, CU_i denotes the number of cloud users in the simulation. It is measured in terms of percentage (%).

Table 3. Classification Accuracy

Number of Cloud Users	Classification accuracy (%)		
	CSDECGBAC-SDC	HBRSS	LMAAS-IoT
10000	99.1	98.1	97
20000	98.6	96.5	94.5
30000	97.83	94.03	91.73
40000	97.52	93.37	89.11
50000	96.96	92.84	88.30
60000	96.25	91.41	87.42
70000	95.71	90.64	86.07
80000	95.31	89.32	85.56
90000	94.68	88.05	85.38
100000	94.25	87.54	84.56

Table 3 reports the classification accuracy is measured with respect to the number of cloud users taken in the ranges from 10000 to 100000. The observed table values indicate the performance results of classification accuracy of three different methods namely the CSDECGBAC-SDC method and the existing HBRSS [1] LMAAS-IoT [2] respectively. The obtained experimental results confirm that the classification accuracy is found to be higher using the CSDECGBAC-SDC method when compared to existing methods. Let us consider the 10000 loud users for conducting the experiments in the first iteration. By applying the CSDECGBAC-SDC method, 9910 cloud users are correctly identified as authorized or unauthorized hence the classification accuracy is found to be 99.1%. The classification accuracy of HBRSS [1] LMAAS-IoT [2] is 98.1% and 97% respectively. Likewise, various experimental results are observed for each method. The obtained results of the CSDECGBAC-SDC method are compared to existing methods. The average of ten comparison results indicates that the CSDECGBAC-SDC method increases the classification accuracy by 9% and 5% when compared to [1], and [2] respectively.

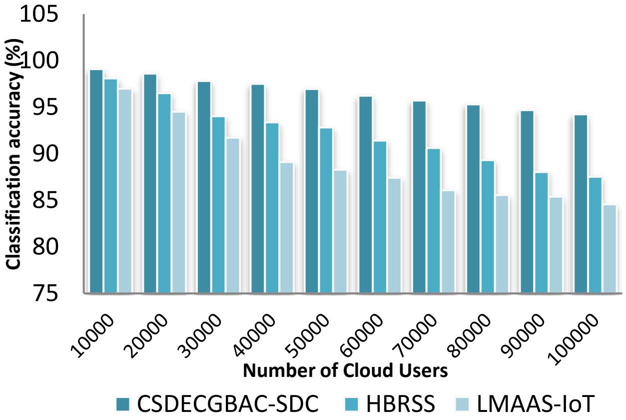

Fig.5: Performance results of classification accuracy versus the number of cloud users

Figure 5 illustrates the performance results of classification accuracy versus the number of cloud users taken in the range from 10000 to 10000. In the graphical representation, the number of cloud users is taken as input in the horizontal axis i.e. 'x' axis but the output results of classification accuracy are obtained at the vertical axis i.e. 'y' axis. The graphical plot indicates that the classification accuracy of three different methods namely the CSDECGBAC-SDC method and the existing HBRSS [1] LMAAS-IoT [2] are represented by the three various colors such as blue, red, and green respectively. The observed illustrates that the CSDECGBAC-SDC method improves the classification accuracy when compared to existing methods. This improvement of the CSDECGBAC-SDC method is achieved by applying the **Chi-**Square Interact Detective Ensembled Bootstrap Aggregating technique. The proposed ensemble technique uses the weak learner as Tversky Indexive Chi-square automatic interaction detection decision tree for verifying the user-ID with the registered ID. If these two IDs get matched, then the authorized user is identified. The ensemble bootstrap aggregating technique combines the weak classification results to make a strong output result by applying a cardinal voting scheme.

5.2 Impact of Error Rate

The error rate is measured as the ratio of cloud users wrongly classified to the total number of cloud users. This formula for calculating the error rate is expressed as follows,

$$ER = \left[\sum_{i=1}^{n} \frac{CU_{wc}}{CU_i}\right] * 100 \qquad (7)$$

From the above equation (7), 'ER' denotes an error rate, CU_{wC} denotes a cloud user wrongly classified, CU_i number of cloud users It is measured in terms of percentage (%).

Table 4. Error Rate

Number of Cloud Users	Error rate (%)		
	CSDECGBAC-SDC	HBRSS	LMAAS-IoT
10000	0.9	1.9	3
20000	1.4	3.5	5.5
30000	2.16	5.96	8.26
40000	2.47	6.62	10.88
50000	3.04	7.16	11.69
60000	3.75	8.58	12.58

70000	4.28	9.35	13.92
80000	4.68	10.68	14.43
90000	5.31	11.95	14.61
100000	5.74	12.45	15.43

Table 4 given above illustrates the performance results of the error rate using three different methods namely the CSDECGBAC-SDC method and the existing HBRSS [1] LMAAS-IoT [2] with respect to the number of cloud users considered from 10000 to 100000. The above-observed results indicate that the performance of error rate using the CSDECGBAC-SDC model is significantly minimized than the two existing HBRSS [1] LMAAS-IoT [2]. By considering '10000'cloud users for experimentation and the overall error rate was observed to be '0.9%', '1.9 %', and '3%' using CSDECGBAC-SDC, HBRSS [1] LMAAS-IoT [2]. Similarly, other performance results are observed with respect to various numbers of cloud users. The observed results indicate that the error rate is considerably reduced by 57% using the CSDECGBAC-SDC method when compared to [1] and 70% compared to [2] respectively.

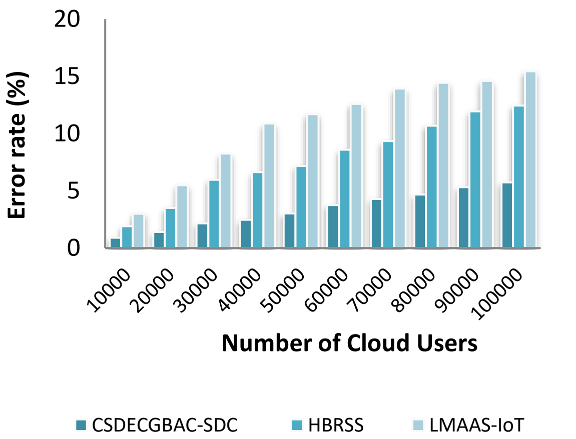

Fig. 6: Performance results of error rate versus the number of cloud users

Figure 6 given above exhibits the graphical illustration of the error rate using three different methods and a different number of cloud users. The above graphical representation illustrates that the error rate using the CSDECGBAC-SDC method is found to be relatively lesser when compared to conventional methods. The reason behind this significant improvement was the application of cardinal voting and gradient ascent function. By applying cardinal voting, the weak learner results are ordered based on the training error. The weak learner with a higher error rate is removed. Finally, the gradient ascent function is applied to find the majority votes of the samples. Therefore, the obtained ensemble results improve the accuracy and minimize the error rate.

5.3 Impact of Classification Time

The classification time is defined as the amount of time consumed by the algorithm for classifying the authorized and unauthorized users. The formula for classification time is measured as given below,

$$CT = \sum_{i=1}^{n} CU_i * Time\ [classification] \quad (8)$$

Where CT denotes a classification time 'CU_i denotes the number of cloud users and the time consumed in classification '$Time\ [classification]$'. It is measured in terms of milliseconds (ms).

Table 5. Classification Time

Cloud Users	Classification Time (ms)		
	CSDECGBAC-SDC	HBRSS	LMAAS-IoT
10000	4600	6100	7500
20000	4800	6800	8000
30000	5100	6900	7500
40000	6400	8000	9200
50000	7100	9500	10000
60000	9120	10800	11400
70000	9800	12600	14000
80000	10400	13600	15200
90000	11250	14400	17100
100000	13200	15000	18000

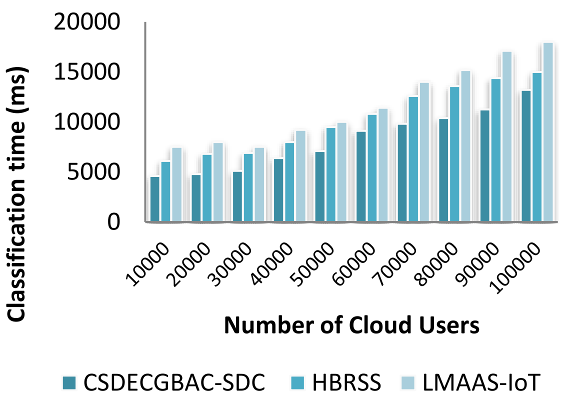

Fig. 7: Performance results of classification time versus the number of cloud users

Table 5 and figure 7 represent the classification time of three different methods namely the CSDECGBAC-SDC method and the existing HBRSS [1] LMAAS-IoT [2]. The observed results indicate that the classification time of the CSDECGBAC-SDC model is comparatively lesser than the other two existing methods. The above table reveals that the classification time is considerably reduced for all the ten different runs. For each run, the input counts of samples get increased as a result the classification time of three different methods also gets increased. By considering the '10000' samples in the first iteration, the classification time of the CSDECGBAC-SDC model was found to be '$4600ms$', '$6100ms$' using [1], and '$7500ms$' using [2] respectively. Similarly, the various runs were carried out with different counts of input data. The overall results indicate that the classification time of the CSDECGBAC-SDC model is considerably reduced by 22% and 31% when compared to HBRSS [1] and LMAAS-IoT [2] respectively. This is because of performing the user registration, before the data collection and secure data communication. Initially, the users' details are registered and then the server collects the data from the registered user. Then the classification is performed using the ensemble technique with the help of the Tversky similarity index. The similarity function matches the ID of the user to find the authorized or unauthorized.

6. CONCLUSION

The technology of big data is integrated into the cloud to facilitate the real-time applications for data security. This paper presents a CSDECGBAC-SDC model using the IoT for a cloud environment, which aims to increase the security of big data communication. The proposed CSDECGBAC-SDC model reduces the possibility of unauthorized data access, enhances accuracy, and provides more protection. The CSDECGBAC-SDC model first performs the registration process that includes user information. Then the registered user allows storing their data collected from the IoT device to server. Then any user who wants to access the data, first they verify the authenticity using Chi-Square Detective Ensembled Cardinal Gradient Bootstrap Aggregating technique. The ensemble technique accurately finds the authorized user or unauthorized user based on the cardinal voting and gradient ascent function. This process enhances the classification accuracy and minimizes the error rate. The performance of the CSDECGBAC-SDC model is analyzed with different metrics such as classification accuracy, error rate, and classification time. Therefore, the quantitative results and discussion conclude that the presented CSDECGBAC-SDC model is highly promising to provide higher classification accuracy with a lesser time as well as error rate than the conventional methods.

7. CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

8. REFERENCES

[1] S L, Swapna., V Saravanan. Survival Analysis on Secured Data Communication in Cloud. International Journal of Computer Applications. 2022. https://doi.org/10.5120/ijca2022921864

[2] Hui, Xie., Zhengyuan., Zhang., Qi, Zhang., Shengjun, Wei., Changzhen, Hu.: HBRSS: Providing high-secure data communication and manipulation in insecure cloud environments. Computer Communications (2021). https://doi.org/10.1016/j.comcom.2021.03.018

[3] Ahmed Yaser, Fahad, Alsahlani., Alexandru, Popa.: LMAAS-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment. Journal of Network and Computer Applications (2021). https://doi.org/10.1016/j.jnca.2021.103177

[4] Mohamed Ahzam, Amanullah., Riyaz Ahamed, Ariyaluran, Habeeb., Fariza, Hanum, Nasaruddin., Abdullah, Gani., Ejaz, Ahmed., Abdul, Salam, Mohamed, Nainar., Nazi,hah, Md, Akim., Muhammad, Imran.: Deep learning and big data technologies for IoT security. Computer Communications (2020). https://doi.org/10.1016/j.comcom.2020.01.016

[5] David, G. Rosado., Julio., Moreno., Luis, E. S´anchez., Antonio, Santos-Olmo., Manuel, A. Serrano., Eduardo, Fern´andez-Medina.: MARISMA-BiDa Pattern: Integrated Risk Analysis for Big Data. Computers & Security (2021). https://doi.org/10.1016/j.cose.2020.102155

[6] Wuchao, Liang., Wenning, Li., Lili, Feng.: Information Security Monitoring and Management Method Based on Big Data in the Internet of Things Environment. IEEE Access (2021). https://doi.org/10.1109/ACCESS.2021.3064350

[7] Imane, El Alaoui., Youssef, Gahi.: Network Security Strategies in Big Data Context. Procedia Computer Science (2020). https://doi.org/10.1016/j.procs.2020.07.108

[8] Uma, Narayanan., Varghese. Paul., Shelbi, Joseph.: A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment. Journal of King Saud University - Computer and Information Sciences (2020). https://doi.org/10.1016/j.jksuci.2020.05.005

[9] Abdul, Razaque., Nazerke, Shaldanbayeva., Bandar, Alotaibi, Munif, Alotaibi., Akhmetov. Murat., Aziz, Alotaibi.: Big Data Handling Approach for Unauthorized Cloud Computing Access. Electronics (2022). https://doi.org/10.3390/electronics11010137

[10] Rohit, Sharma., Rajeev, Arya.: Secure transmission technique for data in IoT edge computing infrastructure. Complex & Intelligent Systems (2021). https://doi.org/10.1007/s40747-021-00576-7

[11] Dongfeng, Fang., Yi, Qian., Ro, Qingyang, Hu.: A Flexible and Efficient Authentication and Secure Data Transmission Scheme for IoT Applications. IEEE Internet of Things Journal (2020). https://doi.org/10.1109/JIOT.2020.2970974

[12] Deebak, B.D., Fadi, Al-Turjman.: Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing. Future Generation Computer Systems (2021). https://doi.org/10.1016/j.future.2020.11.010

[13] Qingyang, Zhang., Hong, Zhong., Weisong, Shi., Lu, Liu.: A trusted and collaborative framework for deep learning in IoT. Computer Networks (2021). https://doi.org/10.1016/j.comnet.2021.108055

[14] Mohammad, Wazid., Ashok Kumar, Das., Vivekananda, Bhat, K., Athanasios, V. Vasila.: LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. Journal of Network and Computer Applications (2020). https://doi.org/10.1016/j.jnca.2019.102496

[15] Seunghwan, Son., Yohan, Park., Youngho Park.: A Secure, Lightweight, and Anonymous User Authentication Protocol for IoT Environments. Sustainability (2021). https://doi.org/10.3390/su13169241

[16] Manasha, Saqib., Bhat, Jasra., Ayaz Hassan, Moon.: A Lightweight Three Factor Authentication Framework for IoT Based Critical Applications. Journal of King Saud University - Computer and Information Sciences (2021). https://doi.org/10.1016/j.jksuci.2021.07.023

[17] Hesham, A. El Zouka., Mustafa, M. Hosni.: Secure IoT Communications for Smart Healthcare Monitoring System. Internet of Things (2021). https://doi.org/10.1016/j.iot.2019.01.003

[18] Ashish, Singh., Kakali, Chatterjee.: Securing smart healthcare system with edge computing. Computers & Security (2021). https://doi.org/10.1016/j.cose.2021.102353

[19] Mustafa, A. Al Sibahee., Songfeng, Lu., Zaid Ameen, Abduljabbar., Xin, Liu., Hemn Barzan, Abdalla., Mohammed Abdulridha, Hussain., Zaid Alaa, Hussien., Mudhafar, Jalil Jassim Ghrabat.: Lightweight Secure Message Delivery for E2E S2S Communication in the

IoT-Cloud System. IEEE Access (2020). https://doi.org/10.1109/ACCESS.2020.3041809

[20] Sheeba Rani, S., Jafar, A. Alzubi., Lakshmanaprabu, S. K., Deepak, Gupta., Ramachandran, Manikandan.: Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers. Multimedia Tools and Applications (2020). https://doi.org/10.1007/s11042-019-07760-5

[21] Pampapathi, B. M., Nageswara, Guptha, M., Hema, M. S.: Data distribution and secure data transmission using IANFIS and MECC in IoT. Journal of Ambient Intelligence and Humanized Computing (2022). https://doi.org/10.1007/s12652-020-02792-4

[22] R John, Martin. IoMT Supported COVID Care – Technologies and Challenges. International Journal of Engineering and Management Research, (2022). DOI: 10.31033/ijemr.12.1.16