Random Forest based Classification of user Data and Access Protection

M.Sumathi, S.Prabu

Abstract: Nowadays Machine learning techniques based Data Privacy is considered as an important factor in efficiency measuring of user sensitive data privacy in a public cloud. At present, data owners are willing to protect their data from unauthorized trainers and users at the time of data classification based on machine learning techniques. The current classification techniques based on privacy preserving allows single owner data sources not a multi-owner data sources. Hence, the learning process depends on single owner information. When a multi-owner data is coming for classification means the present classification system will not be classified efficiently and accurately. Hence, an alternate system is required to handle a multi-owner data classification process with a privacy preserving storage system. The proposed privacy preserving random forest scheme efficiently handles the multi-owner data sources without the involvement of the trusted curator at the time data classification. Here, the random forest classification technique is used for classification and Advanced Encryption Standard (AES)Technique is used for the purpose of maintenance of the privacy during the sending and receiving of statistical information resulted from the analysis and classification process between sender and receiver. The classification process is applied to, student grade system analysis and classification done in a different manner like horizontal and vertical data partition process. When an individual student data is required means horizontal partition is applied else if particular subject details are required means vertical partition is applied. Then, AES encryption technique is applied to protect the user information. When compared to the existing classification and privacy preserving techniques, the proposed machine learning based classification technique with AES provides better privacy to user sensitive data.

Index Terms: Privacy-Preserving, Differential Privacy, Random Forest, AES Encryption, Horizontal Partition, Vertical Partition.

I. INTRODUCTION

Now-a-days, data analysis like spam detection, economic prediction, risk assessment and many other predicting systems using machine learning based classification algorithms for their classification process. When compared to data mining techniques, machine learning based classification techniques provides better results. Hence, machine learning based classification techniques used for major prediction and classification processes. When we are going to work with two adjacent data sets is used for privacy concerns machine learning technique analysis the results of both data sets entirely and produce accurate results. When compared to the existing data mining based classification, machine learning algorithm constructed a classifier based on sample data set without any leakage of user privacy information. That is, the machine learning algorithms collect the sample dataset, train the model and produce the trusted trainer to data owners. These, kind of curators have not established in a current application processing [12]. The overcome this problem we proposed a multi-owner based data source scheme in machine learning based classification. These classification techniques avoid the trusted third party classifier. To achieve this motivation Random forest is used for the classification process because, random forest is a flexible and efficient classification technique for a multi-owner data sources. When compared to existing data mining algorithms, the machine learning algorithms are producing an improved result. Random forest algorithm is the most used algorithms because its simplicity. Now-a-days machine learning algorithm can be used for classification as well as regression tasks [13]. Machine learning techniques are majorly classified as supervised and unsupervised algorithms. In this classification, the Random Forest algorithm is a supervised learning technique. The name itself says that the Random Forest algorithm creates a forest based on given input data in a random manner and the "forest" construction is depending on an ensemble decision tree method, with bagging based training process. The bagging process increases the accuracy of classification through the combination of learning models. When compared to other classification techniques, random forest acted as a building block of machine learning technique. Random forest considers same hyper parameters like a decision tree and bagging classifiers. To improve accuracy random forest combined with decision tree. Hence, random forest technique is very easy to use than the other classification techniques. Random Forest, is also used for dealing of regression through regress process. For increasing the number of trees in a random forest, additional randomness is added to the existing model. In a random forest technique, the searching process is done through splitting and searching. When compared to complete search, splitting of trees and searching process increases the searching speed by subset searching. Hence, the searching speed is high.

Revised Manuscript Received on 30 May 2019.

***** Correspondence Author

Mrs.M.Sumathi*,, Assistant Professor, Department of Computer Science and Engineering, K.Ramakrishnan College of Engineering, Samayapuram, Trichy. Tamilnadu, India.

Mr.S.Prabu,, Assistant Professor, Department of Computer Science and Engineering, K.Ramakrishnan College of Engineering, Samayapuram, Trichy.Tamilnadu, India.

For improving accuracy of random classification and searching, random thresholds are fixed for each feature instead of searching for possible thresholds. Through this process, the huge number of random trees created it. Cloud computing provides everything as a service to organizations like Software as a Service(SaaS), Platform as a Service(PaaS) and Infrastructure as a Service(IaaS) instead of own resource maintenance. Cloud computing provides services through virtual resources instead of physical resources. Hence, storage and maintenance cost is very low and is easy to use in a large sized business organization and small scale industry and end users. The major benefits of cloud computing listed as follows:

- **Self-service provisioning:** Requester uses the resources in an on demand manner. That is based on request, the resources are allocated to requestor with nominal cost. This benefit resolved the traditional resource management process.
- **Elasticity:** When a user request increases organization can scale up their computing requirement and scale down their resources when a demands decrease. This process removes the requirement for a high cost investment in resources. Hence, the infrastructure cost is reduced as much as possible.
- **Workload Resilience:** When a user request to retain the resources for currently used in a particular process means, the cloud service providers offer the requested resources to current user for continuing their process. Hence, the requester continued their process without any delay.

The following sections are organized in a following manner, such as section 2 describes the existing works based on privacy preserving and differential privacy based machine learning with an asymmetric crypto-system is discussed. Section 3 describes the proposed random forest based classification of data over multiple resources and problem statement. Finally, section 4 and 5 describes our experimental results with the conclusions.

II. RELATED WORKS

A. Machine Learning based Privacy Preserving

The machine learning based privacy preserving algorithms are discussed by many authors with single owner data sources. The focused problem is analyzed in two different categories such as classifying a data instance into a number of parts and perform classification into the subparts. The, process is discussed as follows:

Classification: In the privacy-preserving classification, Barbital. proposed the neural networks based secure evaluation scheme in a linear branching program. This technique based on Naive Bayes classification process for protecting the confidentiality of the queried instances. Bos et al. used NB classification for the construction of a secured classification in a serial manner based on comparison and argument blocks.

Training: In general, training of classifier done in two different ways, such as collaboration and client-server manner. The proposed problem analyzed, how different data providers are trained the machine learning classifiers. Because, data classification is done in the data set without any effect the privacy of individual users. Hence, the data providers played a major role in the training process.

B. Machine Learning based Differential Privacy

Dwork et al. had analyzed the differential privacy and data protection process in the data release cases. The differential data privacy is defined an access of a data set is depended on the individual user access rights with the presence and absence of requested data. The differential privacy mechanism is implemented by a required function with a specific task and resulted from the noise of the learning process. The differential privacy is achieved through the quantifiable notion of privacy requirement. This approach adds noise directly to the raw data and performing specific randomization process in the

Recently, Abadi et al. proposed a differential privacy technique with the combination of deep learning technique. Here, the differential privacy is done in each learning results and privacy preserving Naive based classification is combined to improve the accuracy of privacy preserving techniques. The author, proposed this technique in a single user environment. Hence, it is suitable for a single data sources. They also proposed a multi-owner setting with trusted curator. The drawback of this system is the curator behaved as a malicious actor. Hence, curator is replaced in the propose system. Additionally, the existing multi-owner system works on statistical information such as the data set is placed in a public storage location, hence the trainer can easily break the privacy of individual users. In addition to that, the data to be partitioned in vertical manner. Hence, we proposed an alternate classification technique for performing the classification through the random forest classifier. Here, the data privacy is achieved through differential privacy in a multi-owner environment with a guaranteeing ownership privacy and statistic privacy.

C. Asymmetric Cryptosystem

Asymmetric crypto-system (otherwise named as private key crypto-system) uses only a single key for both encryption and decryption process of the data. The key which is used for encryption and decryption is known as secret key and only people who are authorized for the encryption/decryption would be known that key. In a symmetric crypto-system, the encrypted message is passed over secure channel. The existing model implements a Naïve Bayes algorithm for regression and classification. It comes with some disadvantages of time delay and has varied from the exact outcome.

- **Data storage:** When a data is stored in a plain text form is not secure and authentication details are stored in the cloud database as cipher-text increases data security.
- **Dynamic Data Support:** This is used for maintaining a similar level of storage the members involved in a network and assurance of the data given to authorized user in a proper manner without any change to others.

- **Demerits:** The existing security solutions are unable to simultaneously meet the following security requirements.

1. Data confidentiality and privacy of file storage
2. Lack of security in File sharing
3. Owner controllable authorization over the data owner's shared keys.
4. The time delay in pre-processing data set.
5. Different outcome measures.

III. PROBLEM STATEMENT

In a multi-owner environment, a statistic researcher would like to construct a Random Forest(RF) classifier which is used to predict the report of a student in assessments. Because, the Random Forest classifier takes analysis record as the input data and the researcher takes paradox for the consideration of analysis. If we want to train a classifier, makes the prediction is to be more accurate and it is necessary for the researcher to collect records as raw as possible from patients.

The researcher has the duty to keep the privacy of each. Such as, the attractive security system should be designed to facilitate the researcher to execute training over the record sets without instructive too much information about any single individual in them. In this application, health records are training samples, each patient can be seen as a data provider, and the researcher can be seen as a data receiver. To make the trained classifier differential private via a confidential machine, the noises that are added to the statistics (e.g., counts) should be related to the whole dataset aggregated from the provided dataset. However, for a provider, other providers are the contents of his/her own dataset must not by others. Thus, a untrusted to undertake the aggregation task. Consequently, the view of a provider, his/her privacy should be protected against the receiver, the collector, and other providers via some techniques.

IV. PRELIMINARY

A. Random Forest Classifier

A Random forest technique is used to build ‘n’ number of decision trees and combine these trees together for getting an accurate and stable prediction result”. In general, Random Forest creates a forest and makes it somehow random values. The "forest" it constructs, through an ensemble of Decision Trees and the majority of the occasion trained with the "bagging" method. The universal idea of the bagging method is, that a grouping of learning models are boost the overall result. The advantage of random forest is, that it can be used for both classification and regression problems, which form the majority of current machine learning systems.

B. Decision Tree Learning

Decision trees are an admired technique for a variety of machine learning errands. Tree learning "come adjoining to gathering the requirements for serving as an off-the-shelf procedure for data mining", say Hastie et al., "because it is invariant to the below scaling and a variety of other alteration of feature values, is vigorous to the enclosure of immaterial features and produces examine able models. However, they are rarely precise ". In particular, trees that are developed very deep tend to learn highly irregular patterns: they over-fit their training sets, i.e. have the low bias, but very high discrepancy. Random forests are a way of averaging numerous deep decision trees, trained on dissimilar parts of the similar training set, with the objective is reducing the discrepancy. This comes at an expenditure of a tiny boost in the bias and a few losses of an interpretability, but usually very much boosts the performance in the final model.

C. Asymmetric Crytosystems

In an asymmetric cryptosystem, two different keys are used for an encryption and decryption of user private data. The key used for encryption is reserved public is known to all and the decryption key is reserved top secret is known by an exacting user only. The keys are generated in such a way that it is impracticable to obtain the private key from the public key. The sender and the receiver both have two keys in an asymmetric system.

D. Base64 Algorithm

Base64 is an algorithm that uses the concept of modern encryption algorithms. It is a block cipher algorithm that operates on a bit, but the Base64 mode is easier in its implementation than other encryption technique. Base64 is a general term for a similar encoding scheme that encodes binary data and translates it into a representation of the base 64. The term comes from the Base64 MIME encoding process. The base64 encoding scheme is typically used when there is a need to encode binary data that needs to be stored and transferred through media designed to deal with textual data. This is to ensure that the data remains intact without modification during shipping. Base64 is used commonly in multiple applications including email through MIME and storage of complex data in XML. Base64 needs to be learned because the transformation base64 widely used on the Internet as a medium to transmit data. Due to the result of the transformation base64 be plain text, then this value will be much more easily shipped, compared to the form of binary data format.

E. Key Manager

Data storage and memory management are effectively applied in the system model for encrypted data stored in the cloud system using advanced file manager and Meta Data Manager. Two types of keys used for file authorization and a verification process, such as Public Key and private key.

- **Public Key -** The key which is used for data encryption in a data storage system, file ownership in a digital signature system and file management.
- **Private Key -** The key which is used for file sharing, data decryption and access of another user’s file with authorization and OTA support.

V. METHODOLOGY

To build reliable models, Knowledge Discovery and Data Mining process were considered. The process consists of a number of steps, which can be followed in a knowledge discovery project in order to identify patterns in data. The process of knowledge discovery included the following steps: data collection, preprocessing, data mining, and interpretation of the results.

This study aims to reveal student academic performance in distributed examination courses, based on models developed using five classification algorithms implemented in Scikit-learning (Decision Tree CART, Extra Trees Classifier, Random Forest Classifier, Logistic Regression, and C-Support Vector Classification). Each model was evaluated using two cross-validation methods (stratified tenfold cross validation and leave-one label-out cross-validation). Students were classified as either 1 (passed) or 0 (failed), in accordance with their performance indicators. The latest version of Scikit-learn (machine learning), version 0.19, was used to design the experiments for the proposed model.

A. Data Collection

The data used in this work were obtained from the K.Ramakrishnan College of Engineering. The data set includes course records of students from different department is gathered over a period, for a distributed examination course, Object Oriented Programming. Therefore, the data has not been gathered expressly for educational data mining purposes. In accordance with the course, the examination can be achieved through the final exam and distributed examination. For courses with final examination could be established optional midterm examination during the study period, while the final exam is scheduled at the end of the semester (final examination period), after completion of the study period.

For distributed examination courses, a number of mandatory examinations are provided during the study period. Grade point average (GPA), Cumulative Grade Point Average (CGPA), Semester (S1), Semester (S2), Semester (S3), Semester (S4), Semester (S5), data pre-processing step, feature selection based on statistical tests were performed. We computed the chi-squared statistical test to select the best features from our data sets. During this iterative process, those predictor attributes that have the strongest relationship with the output class were selected student membership to the advanced study group, the number of Credits earned in the previous year, average activity mark, A number of attendances in practical activity meetings, average examination mark, and the number of examinations. The selected predictor attributes and the output class for sample data representation were given in table 1. Figure 1 shows the system architecture of the proposed system.

- **Multi-Owner Management**

Every user must register himself. All the details regarding user such as his personal data, company name, present working areas will be stored into the database. If any data owner needs a cloud space they can send a space request to cloud manager. That Cloud space request is sent to cloud manager. The security will send a secret key to the user for the metadata file.

Table 1. Attributes used in classification Models

Name	Year	S1	S2	S3	S4	S5	S6	GPA	CGPA
Anisha	4	90	90	82	85	89	87	8.3	8.3
Aarthi	4	80	54	54	65	87	85	8.5	8.5
Raj	4	60	78	89	74	56	96	7.6	7.6
Ram	4	89	58	96	82	54	57	6.5	6.5
Ravi	4	87	85	92	50	41	74	5.7	5.7

- **Encrypted File Upload**

After getting the secret key for metadata, the user have to upload an original file with metadata and then file will be encrypted using AES Algorithm. Now user gets an encrypted file and user can store the file into the cloud using a secret key. The user can view the encrypted file (a stored file) from cloud stored space.

- **Upload Data Set**

This module implemented to upload dataset for data mining techniques. The data set called student_marks.csv is used for this proposed model. More than 200 students marks are entered and have been calculated the total and average. The individual results, classifications are to be done by a random forest algorithm.

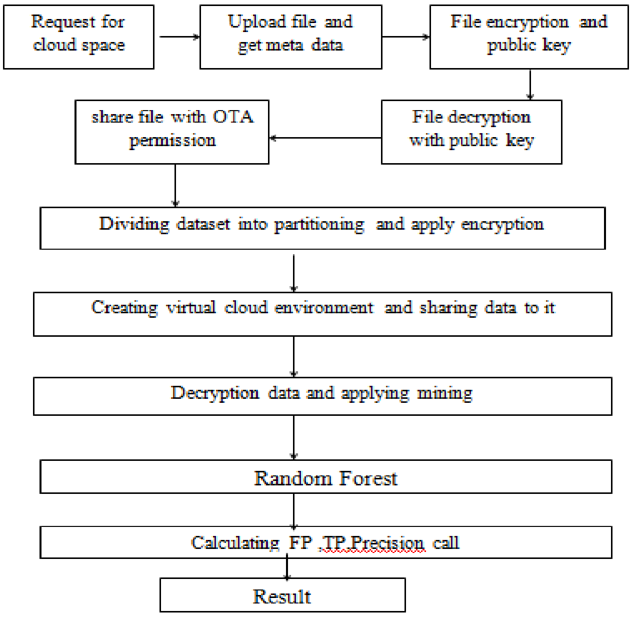

Request for cloud space
Upload file and get meta data
File encryption and public key
File decryption with public key
share file with OTA permission
Dividing dataset into partitioning and apply encryption
Creating virtual cloud environment and sharing data to it
Decryption data and applying mining
Random Forest
Calculating FP ,TP,Precision, call
Result

Figure 1. System Architecture

Algorithm 1: Random Forest Based Classification and Privacy

Input : Student Grade, Threshold Value

Output: Data Partition (Horizontal and Vertical), Encryption

Method:

1. Do pre-processing before the classification
2. Prepare the training data set
3. Get user request
4. If the user request match to any attribute
5. Partition the attribute from remaining attribute list
6. Test the attribute with a training set.
7. Perform AES encryption to that partition
8. Else if check other attributes.
9. Else the user request match to any record
10. Repeat step 6 and 7
11. Return the encrypted attribute or record

- **Pre-processing and Classification**

The data set is to be classified into different aspects such as Department, year, class.

The data set model will be trained for preprocessing and testing. We use 75% of the data for training data and 25% for testing data.

- **Random Forest Algorithm**

  Based on the reports the results will be calculated by random forest technique and it will be shown in the admin panel.

- **Data Manager and Decrypt Data**

  When a user needs a file, then the user has to send a file request to file manager for download a file. Then file manager sends the file to the user after receiving the file, user decrypts the file and then the only user can read the file.

- **OTA File sharing using a Private Key**

  File sharing with other users in the cloud system is built with OTA (One Time Access) Control which allows the users to download the file only once. After that User cannot access the file again, if the user wants to access, then user has to get the approval from data owner.

VI. EXPERIMENTAL RESULTS

This section discussed about the experimental results of the proposed system. Windows 7 is used for the development of this work with PHP, Apache is used as a front end and MYSQL as a backend. Pentium IV 2.4 GHz with 160 GB is used in the implementation process. The experimental dataset contains 1000 student records with multiple attributes like name, marks, GPA, CGPA and results. The classification is done for both record level and attribute level. Figure 2 shows the initial dataset taken for our work and figure 3 shows the classification of data based on years. Figure 4 shows the classification of data in department wise.

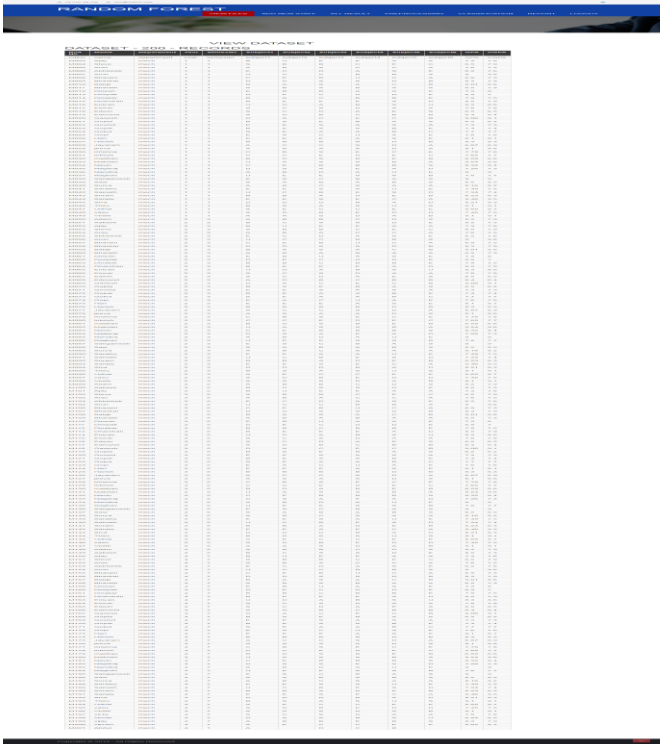
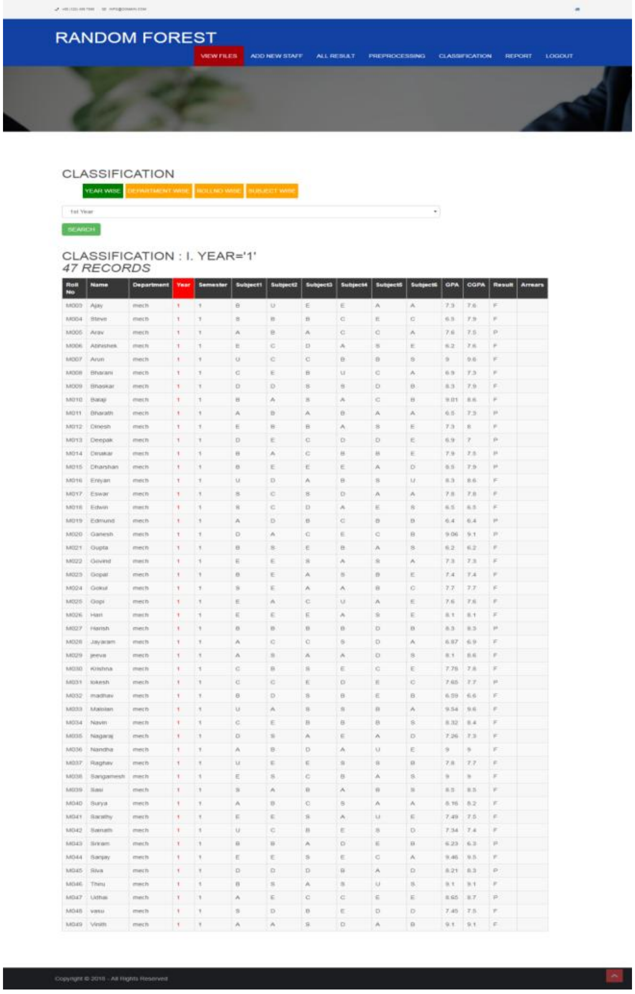


Figure 2. Initial Dataset

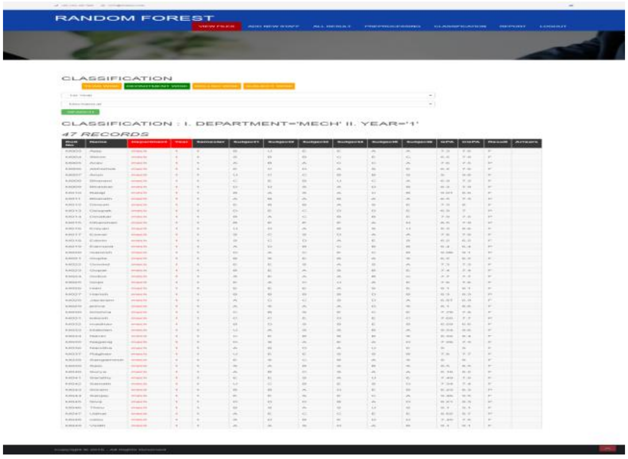


CLASSIFICATION

CLASSIFICATION : I. YEAR='1'
47 RECORDS

Roll No	Name	Department	Year	Semester	Subject1	Subject2	Subject3	Subject4	Subject5	Subject6	GPA	CGPA	Result	Arrears
M003	Ajay	mech	1	1	B	U	E	E	A	A	7.3	7.6	F	
M004	Steve	mech	1	1	S	B	B	C	E	C	6.5	7.9	F	
M005	Arav	mech	1	1	A	B	A	C	C	A	7.6	7.5	P	
M006	Abhishek	mech	1	1	E	C	D	A	S	E	6.2	7.6	F	
M007	Arun	mech	1	1	U	C	C	B	B	S	9	9.6	F	
M008	Bharani	mech	1	1	C	E	B	U	C	A	6.9	7.3	F	
M009	Bhaskar	mech	1	1	D	D	S	S	D	B	8.3	7.9	F	
M010	Balaji	mech	1	1	B	A	S	A	C	B	9.01	8.6	F	
M011	Bharath	mech	1	1	A	B	A	B	A	A	6.5	7.3	P	
M012	Dinesh	mech	1	1	E	B	B	A	S	E	7.3	8	F	
M013	Deepak	mech	1	1	D	E	C	D	D	E	6.9	7	P	
M014	Dinakar	mech	1	1	B	A	C	B	B	E	7.9	7.5	P	
M015	Dharshan	mech	1	1	B	E	E	E	A	D	8.5	7.9	P	
M016	Eniyan	mech	1	1	U	D	A	B	S	U	8.3	8.6	F	
M017	Eswar	mech	1	1	S	C	S	D	A	A	7.8	7.8	F	
M018	Edwin	mech	1	1	S	C	D	A	E	S	6.5	6.5	F	
M019	Edmund	mech	1	1	A	D	B	C	B	B	6.4	6.4	P	
M020	Ganesh	mech	1	1	D	A	C	E	C	B	9.06	9.1	P	
M021	Gupta	mech	1	1	B	S	E	B	A	S	6.2	6.2	F	
M022	Govind	mech	1	1	E	E	S	A	S	A	7.3	7.3	F	
M023	Gopal	mech	1	1	B	E	A	S	B	E	7.4	7.4	F	
M024	Gokul	mech	1	1	S	E	A	A	B	C	7.7	7.7	F	
M025	Gopi	mech	1	1	E	A	C	U	A	E	7.6	7.6	F	
M026	Hari	mech	1	1	E	E	E	A	S	E	8.1	8.1	F	
M027	Harish	mech	1	1	B	B	B	B	D	B	8.3	8.3	P	
M028	Jayaram	mech	1	1	A	C	C	S	D	A	6.87	6.9	F	
M029	jeeva	mech	1	1	A	S	A	A	D	S	8.1	8.6	F	
M030	Krishna	mech	1	1	C	B	S	E	C	E	7.78	7.8	F	
M031	lokesh	mech	1	1	C	C	E	D	E	C	7.65	7.7	P	
M032	madhav	mech	1	1	B	D	S	B	E	B	6.59	6.6	F	
M033	Malolan	mech	1	1	U	A	S	S	B	A	9.54	9.6	F	
M034	Navin	mech	1	1	C	E	B	B	B	S	8.32	8.4	F	
M035	Nagaraj	mech	1	1	D	S	A	E	A	D	7.26	7.3	F	
M036	Nandha	mech	1	1	A	B	D	A	U	E	9	9	F	
M037	Raghav	mech	1	1	U	E	E	S	S	B	7.8	7.7	F	
M038	Sangamesh	mech	1	1	E	S	C	B	A	S	9	9	F	
M039	Sasi	mech	1	1	S	A	B	A	B	S	8.5	8.5	F	
M040	Surya	mech	1	1	A	B	C	S	A	A	8.16	8.2	F	
M041	Sarathy	mech	1	1	E	E	S	A	U	E	7.49	7.5	F	
M042	Sainath	mech	1	1	U	C	B	E	S	D	7.34	7.4	F	
M043	Sriram	mech	1	1	B	B	A	D	E	B	6.23	6.3	P	
M044	Sanjay	mech	1	1	E	E	S	E	C	A	9.46	9.5	F	
M045	Siva	mech	1	1	D	D	D	B	A	D	8.21	8.3	P	
M046	Thiru	mech	1	1	B	S	A	S	U	S	9.1	9.1	F	
M047	Udhai	mech	1	1	A	E	C	C	E	E	8.65	8.7	P	
M048	vasu	mech	1	1	S	D	B	E	D	D	7.45	7.5	F	
M049	Vinith	mech	1	1	A	A	S	D	A	B	9.1	9.1	F	

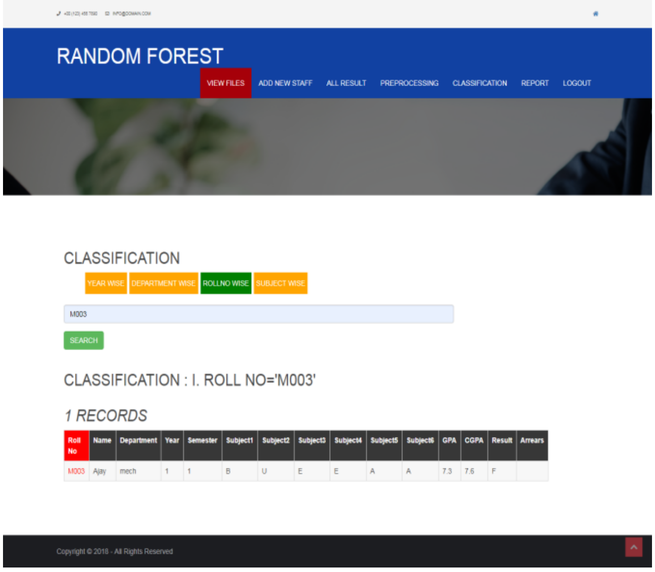
Figure 3. Classification based on Years



CLASSIFICATION

CLASSIFICATION : I. DEPARTMENT='MECH' II. YEAR='1'
47 RECORDS

Figure 4. Classification based on a Department



CLASSIFICATION

M003

CLASSIFICATION : I. ROLL NO='M003'

1 RECORDS

Roll No	Name	Department	Year	Semester	Subject1	Subject2	Subject3	Subject4	Subject5	Subject6	GPA	CGPA	Result	Arrears
M003	Ajay	mech	1	1	B	U	E	E	A	A	7.3	7.6	F	

Copyright © 2018 - All Rights Reserved

Figure 5 Classification of Data - Record Level

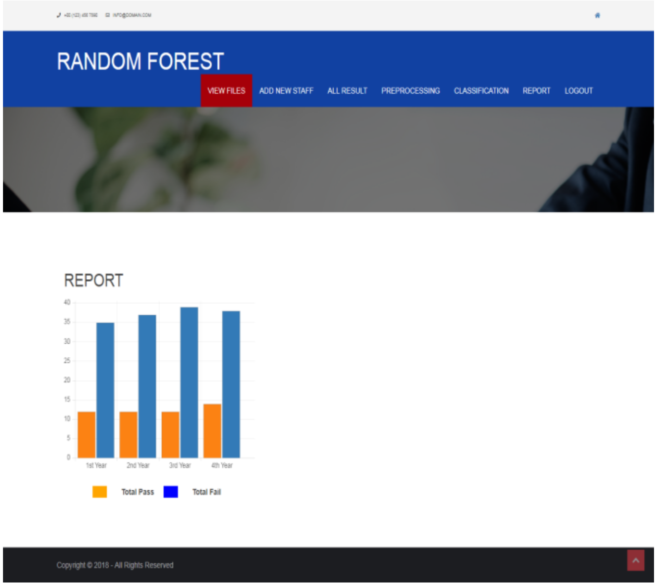


Figure 6. Comparison of pass and fail range

VII. CONCLUSION AND FUTURE ENHANCEMENT

The proposed system, used a random forest classifier for classifying the student databases based on a requirement of a requestor. When a requestor want to a specific department or specific student record, the data can be portioned into the required format by using random classification technique. After partitioning process, the partitioned data is to be encrypted by AES algorithm and sent to the requested user through a secure channel. Here, the data collected from multi-owner data sources and performing classification without the involvement of curator. Hence, the proposed system provides more security and privacy for a user private data in a public cloud storage system. Through random forest machine learning algorithm, the propose system provides better classification results. Hence, the overall system efficiency is improved. In future, the same work is going to be implemented in real cloud with a asymmetric key environment.

REFERENCES

1. M.Sumathi, Dr.S.Sangeetha, “Scale based sensitive data protection on cloud based banking system”, International Journal of Electronic Business, Inderscience, 2018.
2. B. Li, y. Huang, z. Liu, j. Li, z. Tian, s.-m. Yiu, hybridoram: practical oblivious cloud storage with constant bandwidth, inf. Sci. (2018), doi:10.1016/j.ins.2018.02.019..
3. J. Li,Y.K. Li,X. Chen,P.P. Lee,W. Lou, A hybrid cloud approach for secure authorized duplication, IEEE Trans. Parallel Distributing. Syst. 26 (5) (2015)1206–1216..
4. J. Li,Z. Liu,X. Chen,F. Xhafa,X. Tan,D.S. Wong, L-Encdb: a lightweight framework for privacy-preserving data queries in cloud computing, Knowledge Based System. 79 (2015) 18–26.
5. R. Bost,R.A. Popa,S. Tu,S. Goldwasser, Machine learning classification over encrypted data., IACR Cryptol. ePrint Arch. 2014 (2014) 331.
6. Z. Brakerski,V. Vaikuntanathan, Efficient fully homomorphic encryption from (standard) LWE, SIAM J. Comput. 43 (2) (2014) 831–871.
7. X. Chen,J. Li,J. Ma,Q. Tang,W. Lou, New algorithms for secure outsourcing of modular exponentiations, IEEE Trans. Parallel Distributing System. 25 (9) (2014) 2386–2396.
8. J. Li,J. Li,X. Chen,C. Jia,W. Lou, Identity-based encryption with outsourced revocation in cloud computing, IEEE Trans. Compute. 64 (2) (2015) 425–437.
9. P. Li,J. Li,Z. Huang,T. Li,C.-Z. Gao,S.-M. Yiu,K. Chen, Multi-key privacy-preserving deep learning in cloud computing, Future Generation. Computing Syst. 74(2017) 76–85.
10. T. Li,Z. Liu,J. Li,C. Jia,K.-C. Li, CDPS: a cryptographic data publishing system, J. Compute. Syst. Sci. 89 (2016) 80–91.
11. O. Ohrimenko,F. Schuster,C. Fournet,A. Mehta,S. Nowozin,K. Vaswani,M. Costa, Oblivious multi-party machine learning on trusted processors, in: Proceedings of the USENIX Security, 16, 2016, pp. 619636.
12. M.Sumathi, U.Rahamathunnisa, A.Anitha, Druheen Das, Nallakaruppan.M.K, “Comparison of Particle Swarm Optimization and Simulated Annealing applied to Travelling Salesman Problem”, International Journal of Innovative Technology and Exploring Engineering, Volume-8, Issue-6, April 2019, PP 1578-1583.
13. M.Sumathi and S.Sangeetha, “Survey on Sensitive Data Handling-Challenges and Solutions in Cloud Storage System”, Proceeding Advances in Big Data and Cloud Computing, Springer Nature Singapure, Vol.750, PP 598-609, 2018.

AUTHORS PROFILE

Mrs.M.Sumathi, B.E, M.Tech working as a Assistant Professor in Department of Computer Science and Engineering at K.Ramakrishnan College of Engineering, Trichy from 2015. She has 13 years of teaching experience and her area of interest is cloud data security and data mining.

Mr.S.Prabu, B.E, M.E working as a Assistant Professor in Department of Computer Science and Engineering at K.Ramakrishnan College of Engineering, Trichy from 2017. He has 6 years of teaching experience and her area of interest is cloud data security and data mining.