Secured Offline Data Synchronization using Speech Recognition and Artificial Intelligence

Jagadish R M [1], L Swarna Jyothi [2], Aradhana D [1]

[1] Faculty of Computer Science & Engineering, BITM Bellary, Karnataka, India, rm.jagadish@gmail.com.
[2] VTU-RRC, Belagavi, Karnataka, India, swarnajyothi57@gmail.com.

***Abstract* - Offline data synchronization is a technique used to design an application that works without an internet connection. In the proposed work, offline synchronization methods for android have been enhanced along with the security and prioritization in the data file. The synchronization process has to be first validated and hence a speech recognition mechanism has also been applied in the proposed solution. Speech authentication systems along with unique feature selection and classification techniques are applied for providing the security. In addition to security, the proposed framework presents a set of cache memory which is updated when the user is online in order to optimize the synchronization process. The priority algorithm works according to user preferences. The files which are not in use for a long time are removed from the cache of offline user and the files which are getting used by the user often, get migrated to the cache memory automatically. The proposed job does not just emphasize user access, but also provides a safe way to manage the data. The proposed job also manages memory well so that the user does not find any hysteresis.**

Keywords - Relative Spectral Transform, Perceptual Linear Prediction (RASTA-PLP) filtering, Data Encryption Standard (DES) and Advance Encryption Standard (AES), Artificial Bee Colony (ABC), Artificial Neural Network (ANN).

I. INTRODUCTION

Offline data synchronization is one of the most important synchronization techniques that helps user to design an app that works without an internet connection. Synchronizing data between Android devices and Web servers can make the application more useful and attractive to the users. For example, data is transferred to the Web server for a useful backup, and the data is transferred from the server for the user to use, even if the device is offline. In some cases, users may more likely can enter and edit their data in the Web interface, so that the data can be available on the device, or users can collect the data over time and later upload it to the storage center. In mobile devices, backup is required that helps the users to access the stored data when network is not available. Thus, it becomes essential to maintain a local copy of the data model [1].

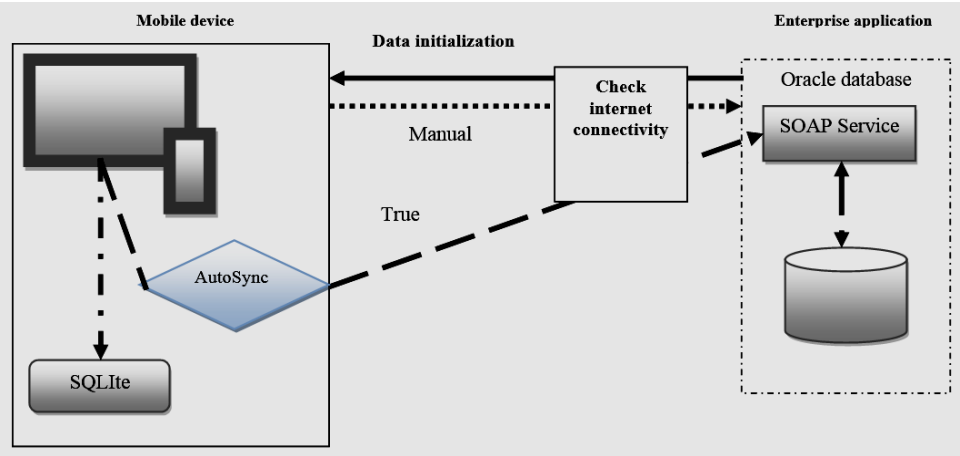

Fig. 1 Architecture of offline data Synchronization [22].

Fig.1shows the architectural details of offline data synchronization, Solid black line indicates when the data is initialized to client for the first time, dotted line indicates manual sync server database from local database, semi dotted line represents data storage into local database, semisolid line indicates auto sync mode.

Synchronization between a server and an android device helps the users to use applications more effectively when

even if the user is not connected to the internet and can save data locally and remotely [2].

There are number of benefits and drawbacks of offline data synchronization that are shown in table 1.

TABLE I. BENEFITS AND DRAWBACK OF OFFLINE DATA SYNCHRONIZATION

Sr. No	Benefits	Drawback
1	Increases application responsiveness by saving server data locally on the device	Occupy a large data space as it is mostly valuable for the user
2	Design a powerful application that can be useful when there are network problems	Occupy large bandwidth as the data sync transfers the data that may contain redundant information.
3	Even without network access, it allows end users to create and modify data	Data Synchronization requires handling multiple threads and different execution paths, which results in more development time and more potential for bugs to hide.
4	Synchronize data between multiple devices and detect conflicts when two devices change the same record	The detection operation is difficult as it does not record the changes.
5	Limit the use of high latency or network measurement over the network	The implementation of the system is complex

The proposed research work considers security as a major concern and hence before the process of synchronization, the user is validated through a speech authentication mechanism.

Speech Authentication: In the proposed work, speech authentication process is applied for the security of the system in when the setting of the current user has to be changed. Speech recognition is used for user verification. The uploaded audio file goes through different phases such as pre-processing, feature extraction and matching of the audio with the data stored in the data base [3].

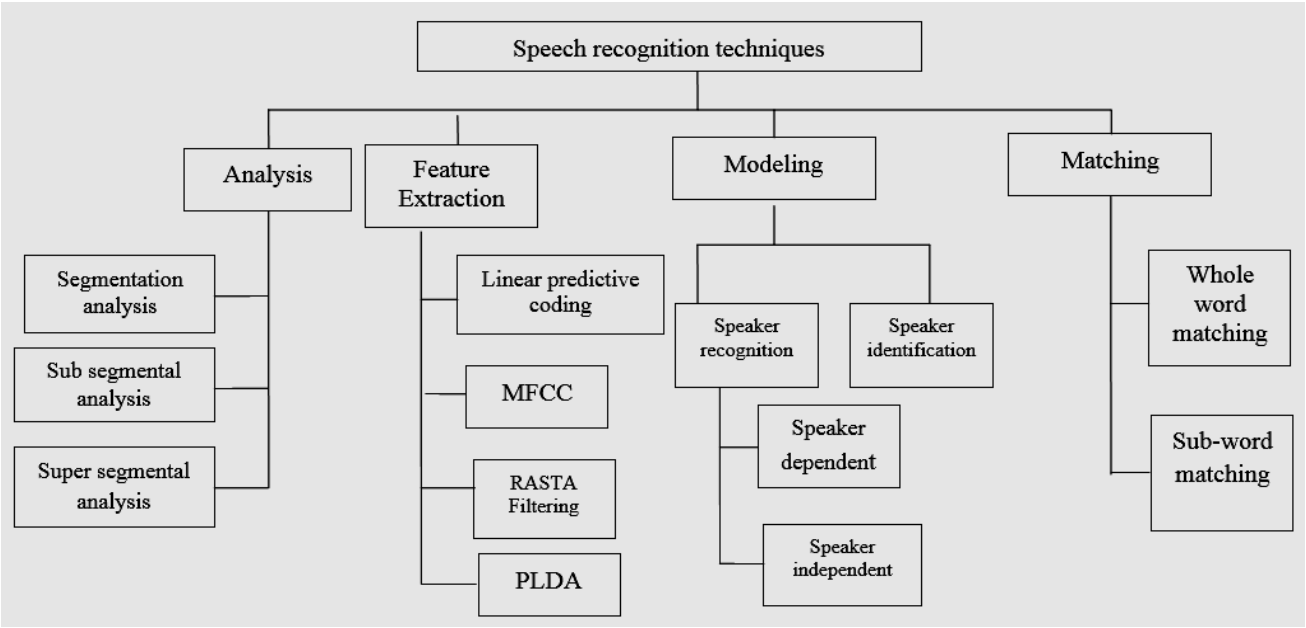

Fig.2. Speech recognition technique

The input is given to mobile device using microphone which converts the audio signal into digital signal. The audio signal is saved and preprocessed to remove the unwanted noise. RASTA-PLP feature extractor is used to extract the feature of audio in the proposed work. The performance of RASTA-PLP is not affected with the small variations in the speech signal and would result into betterment and the feature extraction part will not be affected [4].

Relative Spectral Transform - Perceptual Linear Prediction (RASTA-PLP) filtering

This method is used to increase the quality of speech when recording is done in a destructive environment. It

works similar to band pass filter [5].The flow of RASTA-PLP feature extractor is shown below.

There are several advantages of RASTA-PLP:

- Enhances the quality of speech by removing the slow as well as fast environment variations in artifacts.
- Robust
- Does not require better quality microphone and is independent of the positioning of the microphone
- Captures low level frequencies
- Designed to recognize speech with more noise
- Better performance
- Works like a band pass filter

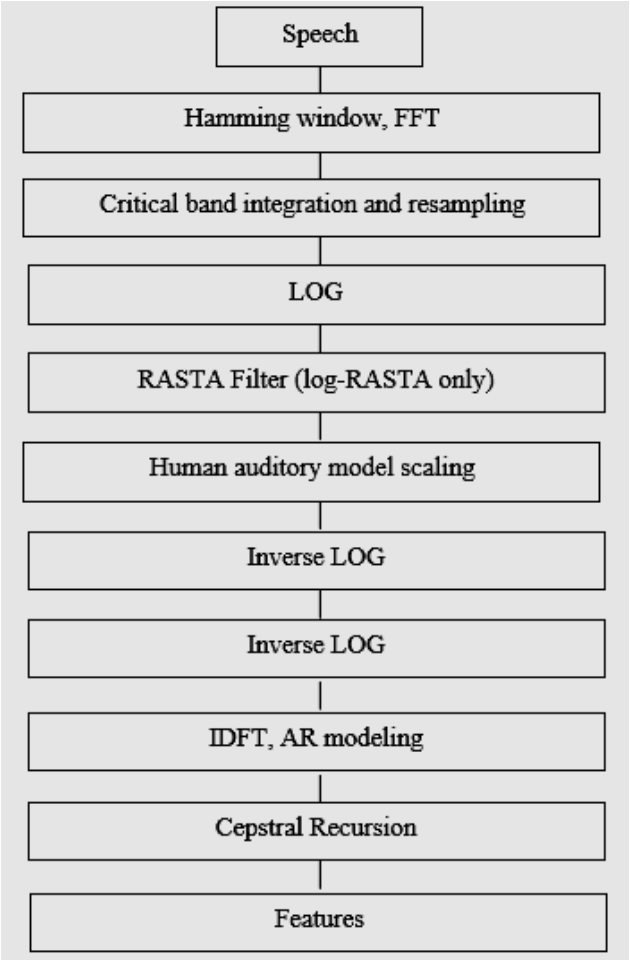

Fig.3. Flow diagram of RASTA-PLP feature extractor

Need of Encryption

The proposed research work understands the need of security at any data server. The proposed architecture considers that, no data should be kept in raw form at any server. The synchronization mechanism will receive the data in decrypted form when the user's device is considered but when it comes to keeping the data at any server, it will be kept encrypted. The proposed algorithm also considers the point that any one encryption algorithm is not suitable for any frame of data and hence the proposed algorithm uses a **complexity finder** in order to justify that which encryption is suitable for which supplied data.

Encryption Algorithms

To increase the speed of the entire process, it is necessary to use specific algorithm for encrypting the data with personal key. Data Encryption Standard (DES) and Advance Encryption Standard (AES) are the two main encryption techniques that are used in the proposed work [6, 7].

TABLE II. DES AND AES ENCRYPTION ALGORITHM

DES	AES
Developed in 1977 having key length of 56 bits	Developed in 2000 having key length of 128, 192 or 256 bits
Having smaller key size and block size of 64 bits.	Having larger key size and block size of 128 bits
Less secure	More secure
The entire data is divided into two parts	The entire data is processed as whole
It is slower	It is faster
Works on Festal Cipher principle	Works on substitution and permutation principle

Synchronization of data itself is a very tricky task whenever it comes to the user preferences. A lot of web applications like you tube, azure networks are providing the same sort of facilities. The synchronization method lags in the safety and auto detection techniques. The problem statement of this research work is based on Safety and Automatic Priority.

The aim of this research work is to design a safe and secure auto synch method to enhance the user experience. For this purpose, an authentication and a prioritization scheme is required to be present. The details are provided in the methodology section.

II. RELATED WORK

This section describes the survey on research and techniques used for online and offline data synchronization. The proposed work, methods and the outcomes are given in table III.

TABLE III. COMPARATIVE ANALYSIS OF EXISTING TECHNIQUE

Reference	Proposed work	Propose method	Outcomes
[8]	A platform used for executing web based applications on mobile phone.	Rich Internet Application (RIA)	Provide online synchronization facility The system is used only for i Google Gadget
[9]	Synchronize offline data with online data	Database sync, offloading	The system maintains the transaction history System is secure by using login id and password
[10]	The proposed system comprises of data server, data historian, a web Server and a cluster for analyzing data. A data analytical method has been used for processing large, high speed data.	Frequency monitoring network (FNET/GridEye), wide area measurement system (WAMS)	The computation power has been increased by using paralleling algorithms and distributing loads among nodes.
[11]	A numerous synch protocols used for synchronizing. Personal digital assistant (PDA) with wireless devices such as mobile.	Palm's HotSync, Pumatech's Intellisync, and the industry-wide SyncML	CPIs is most stable among other synch techniques
[12]	A system that is used for providing notification whenever metadata changes over numerous sources.	PARSING method used to find data from script directive PUSH or PULL method used for aggregation	Reduce human effort by maintaining data regularly
[13]	Presented a system used for synchronizing data from user to the server. Synchronization has been done by transmitting data related to the starting time of the last synch process and the starting time of the current synch process.	MAPITEM synch message record has been used	The proposed method overcomes the forgoing and another problem with the defined method.
[14]	A system that accesses data online as well as offline by using an app. An app collected data from different remote data sources through internet.	Gathering information from different remote data sources. Management of information access, application synchronization and caching by client.	A user may access the information either online or offline without programming the application capabilities.
[15]	Proposed a context dependent scheme for recognizing speech	Artificial neural network	Accuracy up to 70.7% has been attained.
[16]	Speech has been recognized by training the data using TIMIT.	Recurrent Neural network (RNN)	By using RNN system error up to 17.7 % has been obtained
[17]	Proposed a system to recognize the speech of male and female using Gaussian mixture model.	RASTA-PLP feature extractor	The proposed system is completely noise free and robust having accuracy more than 98 %.

III. PROPOSED ALGORITHMS

The algorithms used for the execution of the proposed work such as complexity finder algorithm, ABC algorithm, ANN algorithms are explained below:

A. Complexity Finder

Complexity finder evaluates the complexity of the data. It is required because each kind of data length of different length. Different encryption algorithms have different advantages and different disadvantages. Any algorithm cannot be termed as bad or good. Hence the complexity finder algorithm decides that which encryption algorithm would be efficient for which data.

It defines the complexity of the speech. The complexity is measured on the basis of size of the data and the total amount of data stored into the database.

Function Complexity_finder (Trained_data, Test_data)
LC= Length of Test_data
PC= Length of Trained_data
$cm = \frac{LC}{PC}$, Where cm is complexity
If $\theta < cm < k_p$
DES encryption algorithm is selected
Else if $cm < \lambda$
AES encryption algorithm is selected
End if

The selection of the encryption algorithm depends upon the complexity. To identify the complexity of the data

document some rules have been set. The rules that are used in the research work are shown above

B. ABC (Artificial Bee Colony) Algorithm

The proposed research work considers that output is the encrypted bits and not 100 % pure data when the encryption is performed. The unrelated data wastes the server memory and hence Artificial Bee Colony Optimization is applied to reduce the unwanted bits in the encrypted data. The architecture of ABC is given as follows.

It is a swarm inspired technique used to optimize the data. The word swarm refers to the group of interacting agents and individuals. ABC mainly consists of three components namely, Employed bee, Scout bee, an onlooker bee.

Employed Bee: The employed bee here in this case would be the encrypted elements, which need to be optimized [18].

Onlooker Bee: The onlooker bee would be the threshold of selection and the criteria is defined in the algorithm "Artificial Bee Colony";

Scout Bee: There would be no scout bee in the proposed architecture as each bee would be either selected or rejected. [19].

C. Artificial Neural Network (ANN)

ANN is based on the computation model that works similar to the biological neurons. ANN mainly comprises of three layers named as input layer, hidden layer, and output layer [20].

The three layers shown in the figure are interconnected with each other. The input is given to the first layer that is being passed to the hidden layer where weights are added and then passed to the output layer. The output obtained at each node is known as activation value. The weights of the neurons are adjusted according to some learning rules [21].

Algorithm: Artificial Bee Colony

```
Function ApplyABC (Encrypted_Data )
Population_Size= Encrypted_Data
Reduced_Bit=[ ]; // Initializing the reduction of bits
Bitcount=0 ;// initializing the reduced bit count
Foreach ele in Population_Size
Employed_Bee=Population_Size(ele); // employed bee is the bit
value of each encrypted section value
Onlooker_Bee= Mean( Encrpted_Bit_Value);
Network.Variation= Random; // random variation of the network
Bit_Opt_Value =
Fitness_Bee(Employed_Bee,Onlooker_Bee,Network_Variation);//
passing the data into the fitness function of ABC
If Bit_Opt_Value==1  // If fitness function returns 1 then it means
that the encrypted bit sequence is good else we have to drop the
bit value
Reduced_Bit[bitcount]= EmployedBee;
Bitcount=Bitcount+1;
End if
End For
End Function
Function Bee_Fitness (Emp, Onlooker , Networkv)
R=0;
If Emp*Networkv < Onlooker*NetworkV
R=1;
End
Return R
```

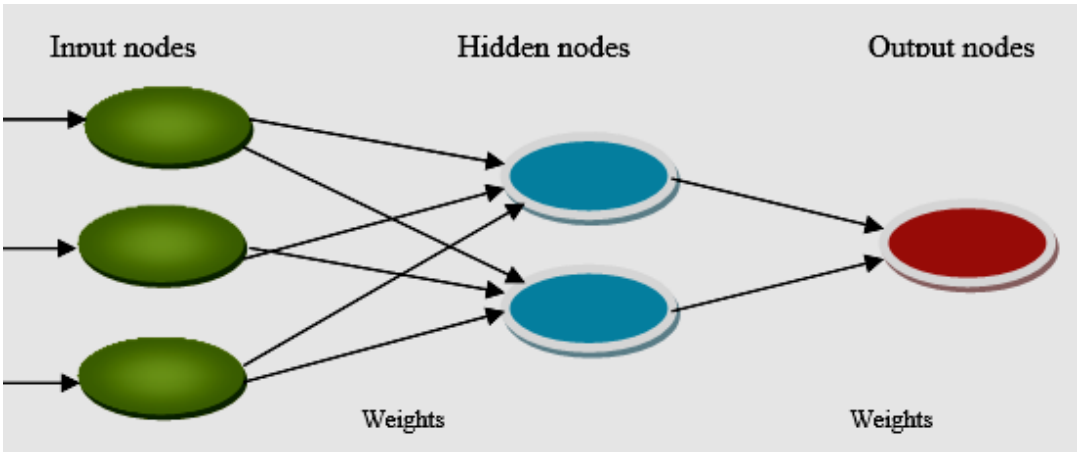

Fig.4: Artificial Neural Network

.

The proposed research work utilizes Artificial Neural Network in order to perform the synchronization mechanism when the user goes online.

Neural Network takes the uploaded files of server as the input. The aim of neural network is to justify the files which have to be transferred to the cache memory of the user based on the utility of the kept file. The Neural Network takes the total number of hits of each file as the training feature. The neural network processes the hit count at its intermediate layer. The input layer considers each file as

one group and hence the input layer is also supplied with the file group values. The architecture is illustrated with the following example set.

Data file	Hit Count
Raw.txt	12
Eef.txt	5
Aeri.txt	18

The training feature set would be [12 5 10] and the group set will be [1 2 3] where 1, 2, 3 represents different text files. This hit count will be converted into weight Matrix at the intermediate layer of Neural Network and the output layer of Neural Network will return the Group element value. The file related to the returned group value will be migrated. The general architecture of Neural Network is described below.

Algorithm : Artificial Neural Network
Initialize the ANN
Net= newff (Training_data, Ggroup, Neurons)
Where, Training_data=All data
Ggroup= No. of categories
Neurons=50
Initialize the training parameters
Epoch=1000

Algorithm: Levenberg marquardt
Performance= MSE, gradient, mutation, & validation checks
Net= Train (Net, Training_data, Group)
Return Net as output of ANN

IV. SIMULATION MODEL

In the proposed research work, a secure system is developed by using DES and AES encryption techniques. Speech recognition has been used in which the features are extracted by using RASTA-PLP algorithm. The flow of the work involves 7 steps:

Step 1: Develop a GUI for the Speech Recognition according to the requirement, after that upload audio files for the training purpose.
Step 2: Develop code for RASTA-PLP for the feature extraction of uploaded audio signal.
Step 3: Initialize a loop for uploading audio files from the dataset of audio signal for the training purpose.
Step 4: Extract the features for all loaded audio signals and save them in a Matlab database.
Step 5: Upload a test audio and apply feature extraction algorithm RASTA-PLP on loaded audio signal.
Step 6: Develop a code for the sum rule which helps to match the technique. test audio from database are recognized using sum rule, .
Step 7: The recognition parameters like Accuracy, True positive and False positive are calculated.

A. Speech Recognition Algorithm using RASTA-PLP

A speech recognition algorithm using Relative Spectral Transform - Perceptual Linear Prediction (RASTA-PLP) technique is presented in the research.

Algorithm: RASTA-PLP feature extractor
Load speech signal
Sampling frequency=
Sampling rate=
Dorasta=1
Modeloader=8
Where Dorasta=1, if all features are calculated
=0, if only PLP feature is calculated
For i=1 to all signals
[feature (i), frame(i)]= Rasta [speech_signal, f_s, s_r , Dorasta, Modeloader]
End (for)
Return, Rasta feature= feature (i)

There are various phases of the proposed algorithm:

Training Phases

Phase 1: Load audio signals X for training from different types of databases.
Phase 2: Extract feature of X using RASTA-PLP.
Phase 3: Store all extracted features in the database.
Phase 4: Generate categories for different types of audio signals.

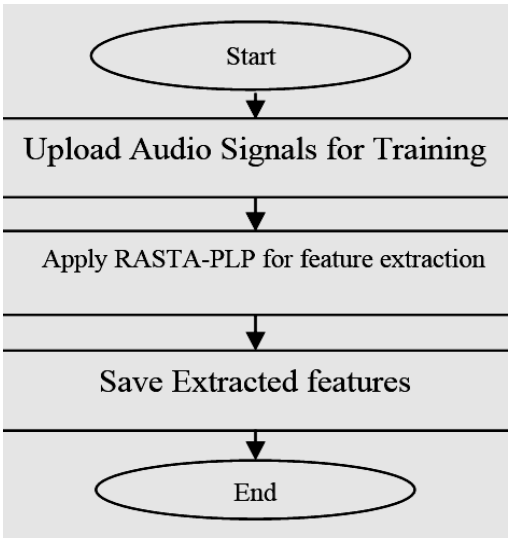

Fig.5: Flowchart of training phase.

Testing Phases

Phase 1: Load test audio signals Xt for testing from any type of database.
Phase 2: Extract feature of Xt using RASTA-PLP.
Phase 3: Store extracted T features in the database.

Phase 4: Load all trained features and apply sum rule on T features with all features.
Phase 5: If feature of test audio signal is preset in the trained feature then the speech is "Recognized" otherwise "Not-Recognized".
Phase 6: Calculate the accuracy of recognition and also calculate True positive and False positive rate.

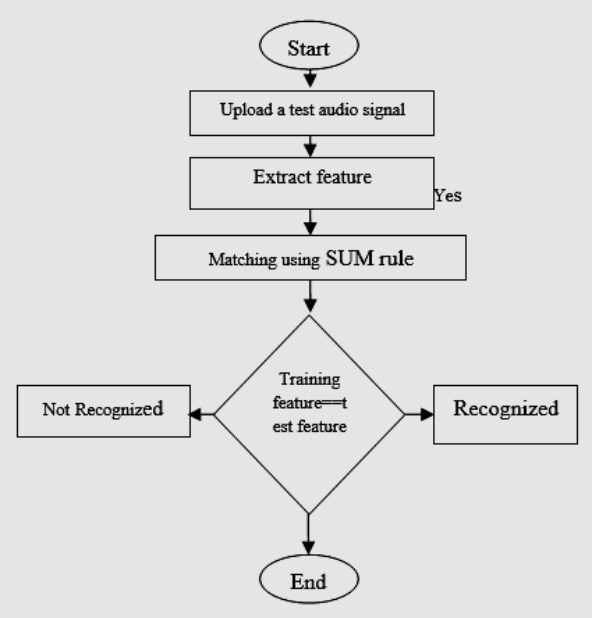

Fig.6: Flowchart of the training phase

V. EXPERIMENT AND RESULT.

The entire code was simulated in MATLAB.

Environment

The performance parameters that were evaluated are shown below.

TABLE IV. CONTENT COMPLEXITY WITH AND WITHOUT OPTIMIZATION

No. of Iteration	Complexity without Optimization	Complexity with Optimization
1	36.74	10.74
2	35.46	11.98
3	35.79	11.47
4	35.98	12.36
5	34.12	12.67
6	34.67	11.76
7	36.65	11.56
8	37.54	12.45
9	39.84	12.93

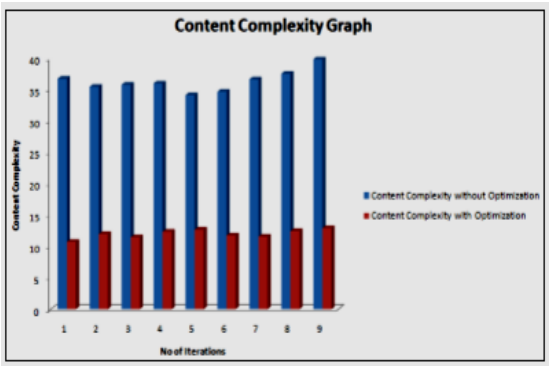

Fig.7: Content Complexity

The values obtained for Content Complexity of the proposed work is written in table IV and its graphical representation has been shown in figure 7.From the above figure, it has been observed that the content complexity with optimization is less compared to that using optimization techniques. The average value of complexity for optimized data is 11.99.

Encryption Time

The total time required to encrypt the data is known as Encryption time. The proposed algorithm encrypts text file format. The encryption time observed for the file is written in table below.

TABLE V. ENCRYPTION TIME W.R.T ALGORITHMS USED

Algorithm	Encryption Time(sec)
DES	.65
AES	.76

From the table V, it is concluded that DES algorithm requires less time as compared to AES encryption algorithm.

Retrieval time

The rate at which data is retrieved is known as retrieval rate. Highest rate determines the fast retrieval. So, the Retrieval time would be high so that all the jobs are retrieved on time. Table VI contains the simulation results obtained for the retrieval time in seconds.

TABLE VI. RETRIEVAL TIME RATE W.R.T ALGORITHMS USED

Algorithm	Retrieval time rate (sec)
DES	1
AES	1.5

VI. CONCLUSION

This research work proposed an architecture for Android phone to make use of applications developed for offline mode and secured data handling. A Speech authentication system was introduced based on the RASTA-PLP feature extractor that makes the system more secure and safe. An ANN was implemented to verify the user's identity. The most frequently used applications are stored in the cache memory and the applications that are not in use for a long time will be deleted automatically. Encryption algorithms such as DES and AES were used for the security of the server data and to speed up the processing. All the encrypted bits are analyzed using ABC algorithm. The unnecessary bits are dropped using ABC. The selection of appropriate encryption algorithm was done using the complexity finder algorithm whose details were described in the earlier sections. A personal key is generated when the process of encryption takes place. It is concluded that the AES encryption algorithm performs well compared to DES algorithm. The Neural Network is solely responsible for the decision of a file to be transferred to the local or global server. A total improvement of about 25% was noticed with each evaluated parameter.

REFERENCES

[1] Chase Jr, Charlie David. "Automatic data synchronization between a handheld and a host computer using pseudo cache including tags and logical data elements." U.S. Patent No. 5,974,238. 26 Oct. 1999.

[2] Sethuraman, Raj, Roger A. Kerin, and William L. Cron. "A field study comparing online and offline data collection methods for identifying product attribute preferences using conjoint analysis." *Journal of Business Research* 58.5 (2005): 602-610.

[3] Nefian, A. V., Liang, L., Pi, X., Xiaoxiang, L., Mao, C., & Murphy, K. "A coupled HMM for audio-visual speech recognition." *Acoustics, Speech, and Signal Processing (ICASSP), 2002 IEEE International Conference on*. Vol. 2. IEEE, 2002.

[4] Kim, Chanwoo, and Richard M. Stern. "Power-normalized cepstral coefficients (PNCC) for robust speech recognition." *Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on*. IEEE, 2012.

[5] Dupont, Stéphane, and Juergen Luettin. "Audio-visual speech modeling for continuous speech recognition." *IEEE transactions on multimedia* 2.3 (2000): 141-151.

[6] Nie, Tingyuan, and Teng Zhang. "A study of DES and Blowfish encryption algorithm." *Tencon 2009-2009 IEEE Region 10 Conference*. IEEE, 2009.

[7] Thakur, Jawahar, and Nagesh Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis." *International journal of emerging technology and advanced engineering* 1.2 (2011): 6-12.

[8] Kao, Y. W., Lin, C., Yang, K. A., & Yuan, S. M. "A Web-based, Offline-able, and Personalized Runtime Environment for executing applications on mobile devices." *Computer Standards & Interfaces* 34.1 (2012): 212-224.

[9] Anil Jaiswal , Rahul Sonawane , Mrs. Sangeeta Oswal , Mrs. Geocy Shejy . "Offline and Online Bank Data Synchronization System," International Journal of Computational Engineering Research (IJCER), 5 (2015): 13-16.

[10] Zhou, D., Guo, J., Zhang, Y., Chai, J., Liu, H., Liu, Y., ... & Liu, Y. "Distributed data analytics platform for wide-area synchrophasor measurement systems." *IEEE Transactions on Smart Grid* 7.5 (2016): 2397-2405.

[11] Agarwal, Sachin, David Starobinski, and Ari Trachtenberg. "On the scalability of data synchronization protocols for PDAs and mobile devices." *IEEE network* 16.4 (2002): 22-28.

[12] Rajan, Steeranga P., and Jonathan Wu. "Method and apparatus for enabling real time monitoring and notification of data updates for WEB-based data synchronization services." U.S. Patent No. 6,633,910. 14 Oct. 2003.

[13] Novak, Lars, and Jörgen Birkler. "Method for optimization of synchronization between a client's database and a server database." U.S. Patent No. 6,643,669. 4 Nov. 2003.

[14] Bloch, E. D., Carlson, M. D., Kang, P., Kimm, C., Steele, O. W., & Temkin, D. T. "Enabling online and offline operation." U.S. Patent No. 7,275,105. 25 Sep. 2007.

[15] Bloch, E. D., Carlson, M. D., Kang, P., Kimm, C., Steele, O. W., & Temkin, D. T. "Context-dependent pre-trained deep neural networks for large-vocabulary speech recognition." *IEEE Transactions on audio, speech, and language processing* 20.1 (2012): 30-42.

[16] Graves, Alex, Abdel-rahman Mohamed, and Geoffrey Hinton. "Speech recognition with deep recurrent neural networks." *Acoustics, speech and signal processing (icassp), 2013 ieee international conference on*. IEEE, 2013.

[17] Zeng, Y. M., Wu, Z. Y., Falk, T., & Chan, W. Y. . "Robust GMM based gender classification using pitch and RASTA-PLP parameters of speech." *Machine Learning and Cybernetics, 2006 International Conference on*. IEEE, 2006.

[18] Karaboga, Dervis, and Bahriye Basturk. "A powerful and efficient algorithm for numerical function optimization: artificial bee colony (ABC) algorithm." *Journal of global optimization* 39.3 (2007): 459-471.

[19] Karaboga, Dervis, and Bahriye Basturk. "On the performance of artificial bee colony (ABC) algorithm." *Applied soft computing* 8.1 (2008): 687-697.

[20] Wang, Sun-Chong. "Artificial neural network." *Interdisciplinary computing in java programming*. Springer US, 2003. 81-100.

[21] Gupta, Neha. "Artificial neural network." *Network and Complex Systems* 3.1 (2013): 24-2.