International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 1, Jan-Feb 2021

Available at www.ijsred.com

REVIEW ARTICLE OPEN ACCESS

Cloud Storage Approach for Secure Authorization Using Lagrange's Based Key Management

T.Premalatha

(Computer Science and Engineering,Anna University/Dr.Sivanthi Aditanar College Of Engineering,Tiruchendur)

Abstract

Since cloud computing has been playing an increasingly important role in real life, the privacy protection in many fields has been paid more and more attention, especially, in the field of personal health record (PHR). The traditional cipher text-policy attribute-based encryption (CP-ABE) provides the fine-grained access control policy for encrypted PHR data, but the access policy is also sent along with ciphertext explicitly. However, the access policy will reveal the users' privacy, because it contains too much sensitive information of the legitimate data users. Hence, it is important to protect users' privacy by hiding access policies. In most of the previous schemes, although the access policy is hidden, they face two practical problems: 1) these schemes do not support large attribute universe, so their practicality in PHR is greatly limited and 2) the cost of decryption is especially high since the access policy is embedded in the ciphertext. To address these problems, we construct a CP-ABE scheme with efficient decryption, where both the size of public parameters and the cost of decryption are constant. Moreover, we also show that the proposed scheme achieves full security in the standard model under static assumptions by using the dual system encryption method.

Keywords: LBK management algorithm, NTRU algorithm, Privacy protection ,message locked encryption .

Introduction

:From the past few years, there has been a rapid progress in Cloud Computing. Cloud Computing delivers a wide range of resources like computational power, computational platforms, storage and applications to users via internet. The major Cloud providers in the current market segment are Amazon, Google, IBM, Microsoft, Salesforce, etc... With an increasing number of companies resorting to use resources in the Cloud, there is a necessity for protecting the data of various users. Some major challenges that are being faced by Cloud Computing are to secure, protect and process the data which is the property of the user. Below, we have described the two main states that hold your data is out in the Cloud: when the data is in motion (transit) and when the data is at rest, where the data is much expected to be more secure. The below illustrated are the two main

scenarios which we have focused to understand the security of the data in the Cloud.

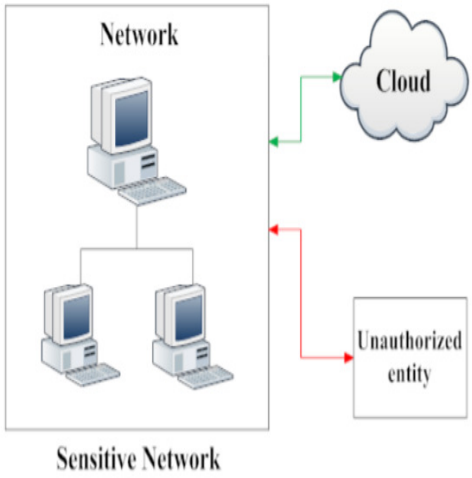

Figure 1.1 Unauthorized access of data between the network and Cloud

The above figure 1.1 describes a scenario where a local network is connected to a Cloud network, in which some part of the network data is broken out from the local network and placed in the Cloud, but the critical data resides in the local network itself. In this case, the Cloud provider does not have any privilege of accessing the data physically which is in the local network. But in some cases, the Cloud needs to access some information which is in the local network, during that access; there exists a possibility of unauthorized access of the local network resources. It describes the typical problem in network security where the information can face active attacks and passive attacks. The active attacks include masquerading, replay attack, modification of messages and denial of service. Passive attacks include traffic analysis. These attacks are likely to happen when the stream of information leaves the client network to the Cloud network.

2.LITERATURE REVIEW

2.1 A New High Capacity Separable Reversible Data Hiding in Encrypted Images Based on Block Selection and Block-Level Encryption

"A New High Capacity Separable Reversible Data Hiding in Encrypted Images Based on Block Selection and Block-Level Encryption" – Meng Chen et al 2018.

Abstract

Reversible data hiding in encrypted image (RDHEI) is a technology that can simultaneously implement privacy protection and reversible information hiding. For RDHEI, the main problem is the conflict between embedding capacity and real reversibility. In this paper, to solve such a conflict, a new block-level image encryption method is proposed to fulfill privacy protection while preserving the spatial correlation of pixels inside pixel block. On this basis, a new reversible data hiding method based on block selection is also proposed. Specifically, pixel blocks are classified into embeddable block (EB) and non-embeddable block (NEB). Then, additional data is embedded into only EBs and the position file locating EB is also embedded using a new self-embedding method. Experimental results demonstrate that the proposed method not only achieves high embedding capacity, but also guarantees lossless data extraction and perfect image recovery.

Methodology

- Reversible data hiding in encrypted image
- Privacy protection and reversible information hiding

Conclusion

A novel high capacity separable RDHEI method is proposed in this paper. After dividing the cover image into a series of pixel blocks, block-level encryption and block-level scrambling are conducted to obtain the encrypted image. Then, additional data is embedded into the EBs using the datahiding key. The receiver who has only the decryption key can get a high quality directly decrypted image. The receiver who has only the data-hiding key can losslessly extract the additional data and the receiver who has both the decryption key and the data-hiding key can losslessly extract the additional data and perfectly recover the cover image. Experimental results show that the proposed method significantly improves the embedding capacity, meanwhile, the data extraction and image recovery are free from any error. Compared with related methods, the proposed method has better potential for RDHEI applications. In the future we will study how to further improve the embedding capacity.

Disdvantages

- Loss data extraction and not perfect image recovery.

2.2 Deep Temporal Convolutional Networks for Short-term Traffic Flow Forecasting

"Deep Temporal Convolutional Networks for Short-term Traffic Flow Forecasting"-Wentian Zhao et al 2019.

Abstract

To reduce the increasingly congestion in cities, it is essential for intelligent transportation system (ITS) to accurately forecast the short-term traffic flow to identify the potential congestion sites. In recent years, the emerging deep learning method has been introduced to design traffic flow predictors, such as recurrent neural network (RNN) and long short-term memory (LSTM), which has demonstrated its promising results. In this paper, different from existing work, we study the temporal convolutional network (TCN) and propose a deep learning framework based on TCN model for short-term city-wide traffic forecast to accurately capture the temporal and spatial evolution of traffic flow. Moreover, we design the model with the Taguchi method to develop an optimized structure of the TCN model, which not only reduces the number of experiments, but also yields high accuracy of forecasting results. With the real-world traffic flow data collected from highways in Birmingham City of U.K., we compare our model with four deep learning based models including LSTM models, GRU models, SAE models, DeepTrend and CNN-LSTM models in terms of the mean absolute error (MAE) and mean relative error (MRE) regarding the actual flow data. The experimental results demonstrate that our framework achieves the state-of-art performance with superior accuracy in short-term traffic flow forecasting.

Methodology

- Recurrent neutral network
- High accuracy.

Conclusion

The short-term traffic flow forecasting is a critical problem in Intelligent Traffic System. In this paper, different from previous work, we propose a deep learning framework based on the Temporal Convolutional Network. Moreover, the Taguchi method is adopted to improve the effectiveness of the design of short-term traffic flow forecasting model. With the real data trace, we compare our model with the LSTM model, the GRU model, the SAE model, the DeepTrend model and the CNN-LSTM model to validate that our model can achieve superior forecasting results. The optimized structure of the TCN found by the Taguchi method is demonstrated to have much more improved performance over other methods. The accuracy rate can reach as high as 95%. Our work demonstrates that the TCN network can be served as a effective tool for short-term traffic prediction in cities.Our basic idea to address this issue is to build the predictor with the power of the unsupervised learning techniques. Moreover, to design a comprehensive traffic forecast, it can include travel time, traffic speed and occupancy [21]. As a future work, we will consider the further design of the TCN network to adapt the different format of traffic data, and the heavy traffic flow fluctuation influenced by the weather and holidays factors.

Disadvantages

- Less forecasting accuracy

2.3 Short-term traffic flow forecasting by selecting appropriate predictions based on pattern matching

"Short-term traffic flow forecasting by selecting appropriate predictions based on pattern matching"- Dongfang Ma et al 2018

Abstract

Forecasting short-term traffic flow is one critical component in traffic management to improve operational efficiency. Data driven method, which trains the predictor with historical data across a given past period, have been proved to perform well. However, days which experience significantly different traffic flow patterns, negatively influence forecasting results. This paper proposes an advanced method, making use of appropriate prediction based on pattern matching. First, historical data is divided into several groups, according to their patterns, by clustering algorithms. Then the predictor is trained for each group based on a Convolutional Neural Networks and Long-ShortTerm-Memory (CNNs-LSTM) model. For each time point, the degree of similarity between the target day and each group is measured, and the predictor trained by the group possessing the highest degree of similarity is selected to be appropriate. Based on a case study from Seattle, we show that selecting an appropriate predictor can significantly improve the accuracy of predictions. In addition, we demonstrate that the new method can, in general, outperform alternative methods in terms of prediction accuracy and stability.

Methodology

- Temporal convolutional networks**.**
- High quality services**.**

Conclusion

we have proposed a new method for shortterm traffic prediction which is based on end to end deep neural network modeling of periodic traffic data. This new method is able to remove the negative influence of historical data that possesses different traffic flow patterns when compared to the target day, which is able to improve forecasting performances in terms of accuracy and robustness. A Seattle based case study has been conducted with one years' data obtained from eight loop detectors, located on a freeway. Historical days are split into four groups and we have applied the CNNs-LSTM model for each group, and the appropriate predictor was selected for each time period for the target day using a matching algorithm. The results show that the average error across the ten target days is approximately 7.66%, which is lower than the average error values for common parametric methods and other deep learning methods. The findings of this paper can be used for traffic signal control, as well as traffic route guidance. In the future, we will further optimize the network structure and increase the richness of input data to obtain better results for traffic prediction problems. Moreover, it would be interesting to investigate other deep learning algorithms for traffic flow prediction and to apply these algorithms on different public open traffic data sets to examine their effectiveness, for example, public bus ID

Disadvantages

- Longer processing time so little delay produced.

2.4 BL-MLE: Block-Level Message-Locked Encryption for Secure Large File Deduplication

BL-MLE: Block-Level Message-Locked Encryption for Secure Large File Deduplication" -Dongfang Ma et al 2018**.**

Abstract

According to the analysis of the International Data Corporation (IDC), the volume of data in the world will reach 40 trillion gigabytes in 2020 [?]. In order to reduce the burden of maintaining big data, more and more enterprises and organizations have chosen to outsource data storage to cloud storage providers. This makes data management a critical challenge for the cloud storage providers. To achieve optimal usage of storage resources, many cloud storage providers perform deduplication, which exploits data redundancy and avoids storing duplicated data from multiple users.

Methodology

- Message locked encryption
- More efficient duplication for encrypted large files.

Conclusion

In this paper, we formalized a new primitive called BlockLevel Message-Locked Encryption for DLSB-

deduplication of large files to achieve space-efficient storage in cloud. We put forward the following directions for further research. First, we ask whether a fully randomized BL-MLE can be constructed for lock-dependent messages [?] to obtain stronger privacy. Secondly, the proposed scheme is proven

.Disadvantages

- Cloud storage not secured data mining

2.5 DW-AES: A Domain-wall Nanowire Based AES for High Throughput and Energy-efficient Data Encryption in Non-volatile Memory

"DW-AES: A Domain-wall Nanowire Based AES for High Throughput and Energy-efficient Data Encryption in Non-volatile Memory"-Wei Wei Jiang et al 2019.

Abstract

Big-data storage poses significant challenges to anonymization of sensitive information against data sniffing. Not only will the encryption bandwidth be limited by the I/O traffic, the transfer of data between processor and memory will also expose the input-output mapping of intermediate computations on I/O channels that are susceptible to semi-invasive and noninvasive attacks. Limited by the simplistic cell-level logic, existing logic-in-memory computing architectures are incapable of performing the complete encryption process within the memory at reasonable throughput and energy efficiency. In this paper, a block-level in-memory architecture for Advanced Encryption Standard (AES) is proposed. The proposed technique, called DW-AES, maps all AES operations directly to the domainwall nanowires. The entire encryption process can be completed within a homogeneous, high-density and standby-power-free non-volatile spintronic based memory array without exposing the intermediate results to external I/O interface. Domain-wall nanowires based pipelining and multi-issue pipelining methods are also proposed to increase the throughput of the baseline DWAES with insignificant area overhead and negligible difference on leakage power and energy consumption. The experimental results show that DW-AES can reduce the leakage power and area by orders of magnitude compared to existing CMOS ASIC accelerators. It has an energy efficiency of 22 pJ/bit, which is 5× and 3× better than the CMOS ASIC and memristive CMOL based implementations, respectively. Under the same area budget, the proposed DW-AES achieves 4.6× higher throughput than the latest CMOS ASIC AES with similar power consumption. The throughput improvement increases to 11× for pipelined DW-AES at the expense of doubling the power consumption.

Methodology

- Advanced encryption standard
- Increase the throughput of the baseline

Conclusion

A block level in-memory architecture for AES encryption has been proposed. All the logic operations required for the computation of AES cipher are realized within the memory array using the DW nanowires that feature ultra-low leakage power dissipation. The predominant XOR gates in

CMOSbased AES are replaced by DW-XOR gates, the ShiftRows transformation by DW shifter and the S-box function by DW-LUT. The spintronic devices used are similar to the devices used for the non-volatile storage elements, which make the integration of the complete in-memory AES computing architecture highly uniform and compact. The throughput of the proposed DW-AES can be boosted by pipelined and multi-issue techniques with the insertion of SW-FIFO and additional DW nanowires computing units for stage balancing. Our experiment results show that the proposed pipelined DWAES exhibits the best energy efficiency of 22 pJ/bit among its rivals, with 5.2× and 3× improvements over CMOS ASIC and memristive CMOL based AES implementations, respectively

Disadvantages

- High leackage power and area by orders of magnitude.

3.EXISTING SYSTEM

With cloud storage services, users can remotely store their data to the cloud and realize the data sharing with others. Remote data integrity auditing is proposed to guarantee the integrity of the data stored in the cloud. In some common cloud storage systems such as the electronic health records system, the cloud file might contain some sensitive information. The sensitive information should not be exposed to others when the cloud file is shared. Encrypting the whole shared file can realize the sensitive information hiding, but will make this shared file unable to be used by others. How to realize data sharing with sensitive information hiding in remote data integrity auditing still has not been explored up to now. In order to address this problem, we propose a remote data integrity auditing scheme that realizes data sharing with sensitive information hiding in this paper. In this scheme, a sanitizer is used to sanitize the data blocks corresponding to the sensitive information of the file and transforms these data blocks' signatures into valid ones for the sanitized file. These signatures are used to verify the integrity of the sanitized file in the phase of integrity auditing. As a result, our scheme makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is hidden, while the remote data integrity auditing is still able to be efficiently executed. Meanwhile, the proposed scheme is based on identity-based cryptography, which simplifies the complicated certificate management. The security analysis and the performance evaluation show that the proposed scheme is secure and efficient.

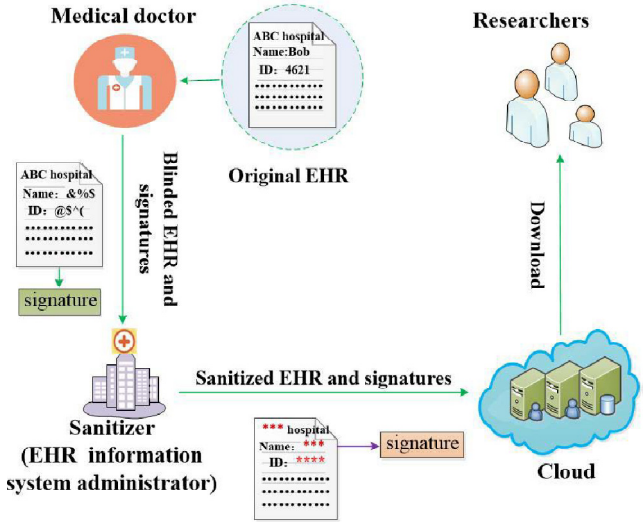

Fig 3.1 Existing system block diagram

Here, we give an illustrative example for EHRs in Fig. 3.3. In this example, the sensitive information of EHRs contains two parts. One is the personal sensitive information (patient's sensitive information), such as patient's name and patient's ID number. The other is the organization's sensitive information (hospital's sensitive information), such as the hospital's name._ Generally speaking, the above sensitive information should be replaced with wildcards when the EHRs are uploaded to cloud for research purpose. The sanitizer can be viewed as the administrator of the EHR information system in a hospital. The personal sensitive information should not be exposed to the sanitizer. And all of the sensitive information should not be exposed to the cloud and the shared users. A medical doctor needs to generate and send the EHRs of patients to the sanitizer for storing them in the HER information system. However, these EHRs usually contain the sensitive information of patient and hospital, such as patient's name, patient's ID number and hospital's name. To preserve the privacy of patient from the sanitizer, the medical doctor will blind the patient's sensitive information of each HER before sending this EHR to the sanitizer. The medical doctor then generates signatures for this blinded EHR and sends them to the sanitizer. The sanitizer stores these messages into HER information system. When the medical doctor needs the EHR, he sends a request to the sanitizer. And then the sanitizer downloads the blinded EHR from the EHR information system and sends it to the medical doctor. Finally, the medical doctor recovers the original EHR from this blinded EHR. When this EHR needs to be uploaded and shared in the cloud for research purpose, in order to unify the format, the sanitizer needs to sanitize the data blocks corresponding to the patient's sensitive information of the EHR. In addition, to protect the privacy of hospital, the sanitizer needs to sanitize the data blocks corresponding to the hospital's sensitive information.

3.1.1 DRAWBACKS

- According to this concept out sourcing patient record does not have any prior permission from patients .
- There is no option to outsource only permitted patient records.

3.2 PROPOSED SYSTEM

Distributed database plays a vital role in day to day life because in the present era, business environment is increasing at very fast rate so our basic desire is to get reliable information from any source. Since our database is distributed, means data is located at different geographical locations and finally helps to easily access our valuable & precious data. We propose an architecture that integrates cloud database services with data integrity and the possibility of executing concurrent operations on encrypted data. It is the solution supporting geographically distributed clients to connect directly to an encrypted cloud database, and to execute the concurrent and the independent operations including those modifying the database structure. Distributed database is the emerging technique which focuses on concurrency control and security issues under this distributed database. In this research work, data

security is enhanced by using NTRU (N-th degree Truncated polynomial Ring Unit or Number Theory Research Unit) asymmetric key algorithm in which the different keys are used for encryption of plaintext and decryption of ciphertext. These keys are named as public and private keys. NTRU being fast and secure hashing algorithm which will provide more security to the system, in terms of throughput and their processing speed. Its main characteristics are the low memory and computational requirements as providing a highsecuritylevel.Itisaverywell-organized public-key cryptosystem.

3.2.1 METHODOLOGYUSED

There search is focused on the implementation of an algorithm that provides a better security by usingcombinationofNTRUalgorithmandMD5 hash function. So the distributed databases are more protected from adversaries. The main design for such approach is as following:

1. The methodology of the work will requiretheimplementationofMD5hash functionwhichisusedforauthentication purpose and NTRU algorithm which is used to provide security for uploading, downloading document and then this algorithm will perform their encryption and decryption of textdocument.
2. Use java platform to implement algorithm.
3. Calculated and analyzed these parameters which are described as: Encryption time, Decryption time and Authenticationtime.

The implementation of the proposed research work goes through various steps which are described as following and shown in Figure5.1.

Step1: Activation of Wamp Server and NetBeansIDE the very first step of the proposed work is to run the Wamp server which is used as backend to store the data base and NetbeansIDE as a frontend where algorithms are implemented in java language.

Step 2: Initiate the Servers In this phase, we have to initiate all the servers that are used to process the user requests.

Step 3: User Registration and User Login In this ,if the user is registered then he/she can login in order to see user's request and user can login for sending the request otherwise he has to do registration first.

Step 4: MAC address comparison for the authentication of the valid user during login process the MAC address of the system is compared which is stored as encrypted way in the database. If it is matched then further operations are performed otherwise not.It shows the MAC address blocked message or invalid username-password message.

Step 5: Perform Different operation during this phase different operations are performed as view logon user, all user profile, intruder log and upload a file. The intruder log keep there cord of intruder party details as record of MAC Address, User name, Password, IP Address, Date and Time.

Step 6: Upload File this phase includes the uploading of file by the user, which is to be encrypted and stored in the database server. Server receives the file and generates a unique key.

Step 7: Encryption of File this phase includes the encryption of the file uploaded by the user with help of encryption/decryption algorithm i.e. NTRU algorithm.

Step8:DecryptionofFile this phase include the decryption of the file using NTRU that is stored in the database and should be downloaded bythe user.

Step 9: Detailed report generated this phase generates the report of the whole work .It represents the authentication time taken and the time taken for the encryption and decryption of file while sharing on distributed database system. Final results are validated. The given results are analyzed and provide the conclusion on the basis of results obtained.

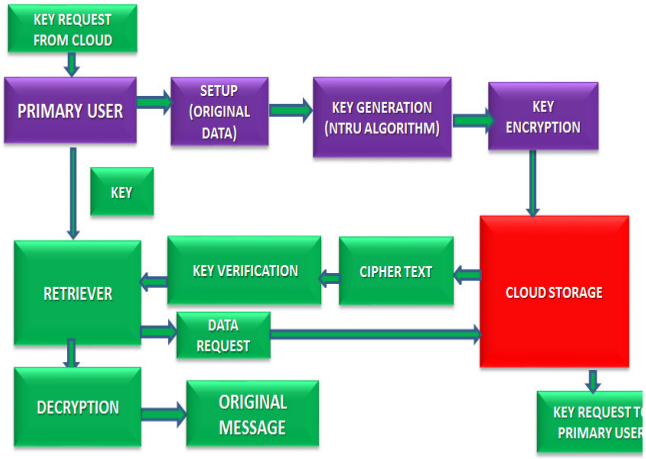

Fig 3.2 Proposed system block diagram

4. IMPLEMENTATIONS

Oracle Corporation is the current owner of the official implementation of the Java SE platform, following their acquisition of Sun Microsystems on January 27, 2010. This implementation is based on the original implementation of Java by Sun. The Oracle implementation is available for Mac OS X, Windows and Solaris. Because Java lacks any formal standardization recognized by Ecma International, ISO/IEC, ANSI, or other third-party standards organization, the Oracle implementation is the de facto standard.

The Oracle implementation is packaged into two different distributions: The Java Runtime Environment (JRE) which contains the parts of the Java SE platform required to run Java programs and is intended for end-users, and the Java Development Kit (JDK), which is intended for software developers and includes development tools such as the Java compiler, Javadoc, Jar, and a debugger.

OpenJDK is another notable Java SE implementation that is licensed under the GPL. The implementation started when Sun began releasing the Java source code under the GPL. As of Java SE 7, OpenJDK is the official Java reference implementation.

The goal of Java is to make all implementations of Java compatible. Historically, Sun's trademark license for usage of the Java brand insists that all implementations be "compatible". This resulted in a legal dispute with Microsoft after Sun claimed that the Microsoft implementation did not

support RMI or JNI and had added platform-specific features of their own. Sun sued in 1997, and in 2001 won a settlement of US$20 million, as well as a court order enforcing the terms of the license from Sun.As a result, Microsoft no longer ships Windows with Java.

4.1 WINDOWS (OPERATING SYSTEM)

Windows OS**,** (OS) developed by Microsoft to run (PCs). Featuring the first (GUI) for -compatible PCs, the Windows OS soon dominated the PC market. Approximately 90 percent of PCs run some version of Windows. The first version of Windows, released in 1985, was simply a GUI offered as an extension of Microsoft's existing disk operating system, or MS-DOS. Based in part on licensed concepts that Apple Inc. had used for its Macintosh System Software, Windows for the first time allowed DOS users to visually navigate a virtual desktop, opening graphical "windows" displaying the contents of electronic folders and files with the click of a mouse button, rather than typing commands and directory paths at a text prompt.

4.2 FEATURES

1) Windows Easy Transfer : One of the first things you might want to do is to transfer your files and settings from your old computer to the brand new computer. You can do this using an Easy Transfer Cable, CDs or DVDs, a USB flash drive, a network folder, or an external hard disk.

2) Windows Anytime Upgrade : This feature of Windows Operating System allows you to upgrade to any higher windows version available for your system, so you can take full advantage of enhanced digital entertainment and other features.

3) Windows Basics : If you are new to Windows or want to refresh your knowledge about areas such as security or working with digital pictures, this features will help you to get started.

4) Searching and Organizing : Most folders in Windows have a search box in the upper- right corner. To find a file in a folder, type a part of the file name in the search box.

5) Parental Controls : Parental Controls give you the means to decide when your children use the computer, which website they visit, and which games they are allowed to play. You can also get reports of your children's computer activity as well.

6) Ease of Access Center : Ease of Access Center is the place to find and change settings that can enhance how you hear, see and use your computer. You can adjust text size and the speed of your mouse. This is also where you can go to set up your screen reader and find other helpful tools.

7) Default Programs : This is a features of your Windows Operating System where you can adjust and set your default programs, associate a file type or a protocol with a program, change and set auto play settings, set program access and computer defaults.

5. RESULT VIEW

User Login

Fig 5.1 User Login page

Admin login

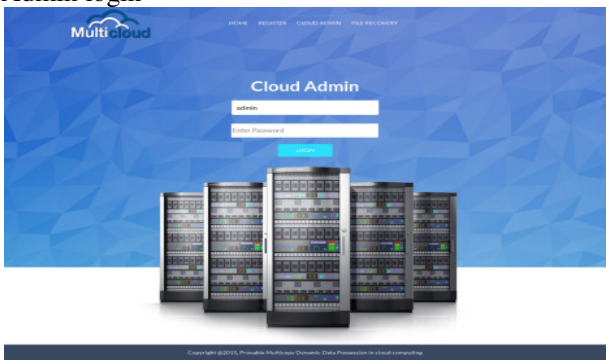

Fig 5.2 Admin login page

Retriever view file :

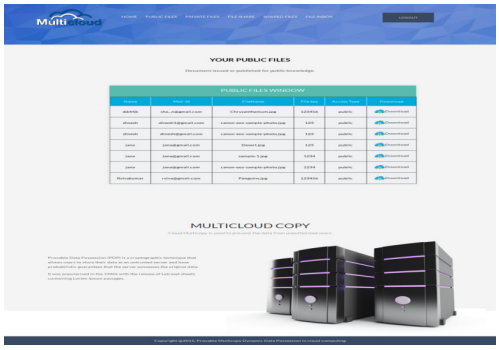

Fig 5.3 Key decryption

6.CONCLUSION

Now-a-days security has become one of the most important aspects in every field. Each information should be secured as any changes in information leads to very serious problem. Data should be secured from malicious attacks and unauthorized access. In this research we mainly deal with the distributed database communication, and solved the concurrency control and security related problems. Security plays important role in this work as to protect our sensitive information from the unauthorized user. This dissertation has implemented the NTRU algorithm in netbeans. In this research we have studied the existing Ramp Secret Sharing Scheme used for encryption and decryption of data and to improve the reliability of distributed de-duplication system. But there are some limitations of existing RSSS technique to overcome the limitations of existing technique NTRU algorithm is used.

6.1 FUTURE ENHANCEMENT

The proposed technique requires less time for encryption and decryption of data while sharing the files in distributed database system and also takes less time for authentication purpose.

In the area of security, research area of distributed database security is very wide. Security is required in military, banking and radio or satellite communication. The future scope of our work

1) Implementationforaudio,videoand.exe (executable)files.
2) Usage for window smartphone.

7.REFERENCE

[1] DiaaSalamaAbdElminaam,"Improving the Security of Cloud Computing by Building New Hybrid Cryptography Algorithms"., I.J. of Electronics and Information Engineering, Vol.8, No.1, PP.40-48, Mar. 2018 (DOI: 10.6636/IJEIE.201803.8(1).05)

[2] Acqueela G Palathingal, Anmy George , Blessy Ann Thomas and Ann Rija Paul," Enhanced Cloud Data Security using Combined Encryption and Steganography", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072.

[3] Mohammad UbaidullahBokhari, QahtanMakkiShallal and YahyaKordTamandani, "Reducing the Required Time and Power for Data Encryption and Decryption Using K-NN Machine Learning" IETE JOURNAL OF RESEARCH, 2018.

[4] DhuratëHyseni, BesnikSelimi, ArtanLuma and BetimCico, "The Proposed Model to Increase Security of Sensitive Data in Cloud Computing", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol.9, No. 2, 2018.

[5] Hitesh Marwaha and Rajeshwar Singh, "The Secure Migration of Data to Cloud using Data Sanitization and MAC address based AES". International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7, Issue-6, March 2019.

[6] X. Chen, J. Andersen, Z.M. Mao, M. Bailey, and J. Nazario, "Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware," IEEE Intl. Conf. on Dependable Systems and Networks With FTCS and DCC (DSN), 2008, pp. 177–186.

[7] S. Vijayakumar, Q. Zhu, and G. Agrawal, "Dynamic Resource Provisioning for Data StreamingApplications in a Cloud Environment," IEEE Second Intl. Conf. on Cloud Computing Technology and Science, 2010, pp. 441–448.

[8] F. Rocha, S. Abreu, and M. Correia, "The Final Frontier: Confidentiality and Privacy in the Cloud,"IEEE Computer, vol. 44 (9), Sept. 2011, pp. 44–50.

[9] S. Pearson, "Taking account of privacy when designing cloud computing services," ICSE W. on Software Engineering Challenges of Cloud Computing, 2009, pp. 44–52.

[10] "The CIA Principle." [Online]. Available: http://www.doc.ic.ac.uk/~ajs300/security/CIA.htm.

[Accessed: 15 Mar. 2017].

S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, andsolutions," J. Netw. Comput. Appl., vol. 75, Nov. 2016, pp. 200–222.

[12] N. Gruschka and M. Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services,"

IEEE 3rd Intl. Conf. on Cloud Computing, 2010, pp. 276–279.

[13] O. Dieste, N. Juristo, and M. D. Martin, "Software industry experiments: A systematic literature review," 1st Intl. W on Conducting Empirical Studies in Industry (CESI), 2013, pp. 2–8.

[14] J. Ramey and P.G. Rao, "The systematic literature review as a research genre," IEEE Intl. Professional Comm. Conf., 2011, pp. 1–7.

[15] M. Pautasso, "Ten Simple Rules for Writing a Literature Review," July 2013. Availableon: http://journals.plos.org/ploscompbiol/article/file?id=10.1371/journal.pcbi.1003149&type=printabl e

[16] K. Padron, "LibGuides: Guide to Science Information Resources: Backward and Forward ReferenceSearching, " Sept. 2016. Available on: http://libguides.fau.edu/c.php?g=325509&p=2182112

[17] S. Zhang, X. Chen, S. Zhang, and X. Huo, "The comparison between cloud computing and grid computing," Intl. Conf. on Computer Application and System Modeling (ICCASM), vol 11, 2010, pp. 72-75.

[18] F. Berman, G. Fox, and A.J.G. Hey, Grid Computing: making the global infrastructure a reality. Wiley, 2003.

[19] J. Tian, ''Reversible data embedding using a difference expansion,'' IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[20] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication," in EUROCRYPT, 2013, pp. 296–312.

[21] Y. Tian and L. Pan, "Predicting short-term traffic flow by long short-term memory recurrent neural network," in Smart City/SocialCom/SustainCom (SmartCity), 2015 IEEE International Conference on. IEEE, 2015, pp. 153–158.

[22] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Trans. Parall. and Distrib. Syst., vol. 22, no. 5, pp. 847–859, 2011.

