International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 4, August 2016, pp. 1792~1799
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i4.9916

A Novel Loom for Alacrity of Protected Lawsuit Dealings Using Cloud Computing Environment

B.V. Subba Rao, J. Rajendra Prasad, D. Kavitha, J. Sirisha, K. Swaroopa Rani
Dept of IT, PVP Siddhartha Institute of Technology, Vijayawada, A.P, India

Article Info

Article history:

Received Jan 13, 2016
Revised Apr 11, 2016
Accepted Apr 25, 2016

Keyword:

Advanced encryption standard
Big data
Cloud environment
Litigation

ABSTRACT

This paper suggest a well-organized information system for facilitate the litigation procedures Information System courts. The purpose is to decrease the duration of processing cases in courts. The aspiration is to save the time and effort of judges and lawyer. In addition, we make use of the advantages of electronic systems and reducing traffic especially in developed countries. Advanced Encryption Standard is used to encrypt all the manipulated data for each case. All read document are encrypted to attain secure information system Litigation process. This is because the big data for all cases will be stored on cloud environment.

Corresponding Author:

B.V. Subba Rao,
Department of Information Technology,
PVP Siddhartha Institute of Technology,
Kanuru, Vijayawada-7, AP, India.
Email: bvsrau@gmail.com

1. INTRODUCTION

Currant century has witnessed many developments in the field of security and safety of big data in the cloud. Because of the significant progress that the whole world has witnessed and appeared as revolution of information and communication, it has reflected on all aspects of life, and crystallized in the emergence of e-commerce, e-government and other areas. Therefore, ordinary litigation with its traditional concept and paper procedures has become unable to meet the challenges of the era that calling an urgent need for the existence of an electronic system to facilitate the litigation procedures [1] .The idea of electronic litigation means movement from the traditional method of paper to electronic form, and the restructuring of the way of dealing with lawsuits in the judiciary annex. It is an effective and excellent mean in achieving positive results in terms of costing and secure the existence of the court at any time and everywhere [2]. Moreover, adoption of electronic litigation saves time and efforts and reduce costs, in addition of offering many other advantages [3] .The proposed approach (design a system to facilitate the litigation) is a technical informational system allows the litigation parties to submit their lawsuits to competent court in electronic manner, deposit their evidences and documents electronically in preparation to get to the sentencing and then implement it.

This system also facilitates judges work and reduces their efforts by enabling them to directly litigation by this system.Also, it cannot be overlooked the great importance of this program in storing the court data and protect them from loss, manipulation or damage, through encrypted, through converting written words or documents to numbers or symbols that cannot be decoded - accessing to data or information to foreign parties – unless they have the suitable password [4].

Perhaps the numerous progressions in the field of information technology in recent industry, which can be exactly identified in the sixties of the last century, is the emergence of cloud computing. This

technology leads to simplifying of the flow of cloud operations, which will enable the user to eliminate tedious administrative tasks that might hinder him during the achievement of more important goals.

1.1. Litigation Process

When a person starts a civil lawsuit, the person evolves into a process called litigation. Under the different rules of Civil Procedure that govern actions in state and federal courts, litigation includes a series of steps that may lead to a court trial and ultimately a resolution of the matter [5].

The integration of justice, Information and Communications Technology is now a new way to be not only in terms of functionality and cost management, but also to adjust the quality standards; it is shown the procedure of civil telematics in its architecture, in its draft implementation and advantages arising from its actual use [6].

The operation of a legal system may affect many branches of development: equity, the optimal Allocation of resources, and the increase in total factor productivity. Moreover, the role of the judicial system in measuring its dysfunctions can affect economic growth.

For example, when the investigation of money laundering cases, it is known that banking and financial institutions activities are carried out through computers devices where all daily transactions are saved, when public prosecutions ordered unloading the contents of these data. Thus, we can imagine the vast amount of documents, evidence and data papers, which will connect with case binders in accordance with the traditional system. However, employing of our proposal system will permit downloading and saving in an electronic system through which all big data in binders of lawsuit will be analyzed and classified easily. This will help judges in dealing with the huge information attached in the cases easily. In addition, it will help other parties in the lawsuit to access and view these large data, thus the proposal system will save time, efforts and costs. In addition to the era crimes, especially terrorist crimes that contain huge and numerous evidences to the extent make their inventorying may be difficult to link them on paper, because of the geographical area to commit the crime on the one hand, and the multiplicity of the perpetrators and the diversity of its means on the other hand, which makes dealing with the large number of evidence and information Crime According to the paper-based system, is very difficult. Not to mention the IT crimes which has spread dramatically in the present day as a result of technological development, which calls for considering the large of the data, which is important evidence of the lawsuit, whether it was civil or criminal. We cannot forget that international crimes as a crime of genocide that are too big data.

It can be concluded the ability of our proposed system in achieving the highest level of justice for litigants. Since, it facilitate the judges to adopting and consider all the evidences in the lawsuits which help to achieving justice, unlike the traditional system, which relies large paper data that cannot be examined by the judge and thus justice will not be achieved.

1.2. Cloud Computing Environment

The concept of "cloud computing", or computer services within internet network, means a set of tasks related to a set of communications and software that employing the software and hardware devices connected to network servers which are loaded with their data in a virtual cloud ,aiming to guaranteeing continuous contact without interruption. This technological boom has caused a big shift in ideas and applications related to information technology services, especially with regard to the infrastructure solutions on which the companies and institutions depend in their completion and facilitating of activities .We can say that the adoption of cloud computing technologies is no longer an option for organizations that seek for safety but it can be considered an obligatory issue in its strategically fate. National Institute of Standards and Technology has confronted to determine the meaning of cloud computing, this concept has some significance in light of the prevailing belief is standard and relying upon by them when dealing with cloud computing, that perception to this concept has evolved along passage of time.

The definition of the Institute as cloud computing is a model for enabling a timely and permanent access to the network at any time, for the participation of a wide range of computing services, which can be published and made available with minimal effort or interaction with the service provider. By the definition of the National Institute several characteristics of cloud computing can be extracted, that are represented by the following

- self-service without support
- Easy access to the network
- reducing of costs and flexibility through the pooling of resources
- Ability to use a quantitative measure

Although, all of computing services such as software and service platforms and service infrastructure, there is a list of security-related challenges and security and safety of the data in the cloud, we will review briefly in turn.

1.3. The big data in court:

Big data subject has occupied a great space of attention because of its importance effect on society and cyberspace. There are numerous concepts and definitions to what is called "*big data*", but till now there is no adoption of a specific definition or concept of the meaning of big data, for example, Wikipedia web site defines it, as a broad term for data sets with huge size that the traditional data processing applications cannot process it. In approximate statistics about big data, it is found that daily output of them reached 1.7 million billion bytes per minute, in various websites, particularly the e-mail and social networking sites. Through this figure we can imagine the vast amount of data which calls for addressing the processing and handling them. we can seek the importance of big data from the announce released by Conference of communication and information technology held in 2013, that considered big data a high-energy to drive economic development through the creation of real-time and quick information and with very little cost compared with other sources. In spite of the difficulty of establishing a uniform definition for big data, but there are certain characteristics that can diagnose which of these data.

- The amount of data: numerous or huge amount of this data is the most prominent feature for their description. For example, analysis of questionnaire data that performed on the general population gives a more acceptable results than the analysis of a questionnaire with limited number as 100 persons.
- Flexibility: big data give the institutions and industrial enterprises greater flexibility in dealing with the economic reality and needs of the market. This data will help them in decision-makers on the speed in making appropriate decisions.
- Diversity: The diversity stems from being dispersed data and cannot be counted in a given aspect, since it includes texts, photographs, videos, maps etc...

We can grope the importance of this system when dealing with big data of the courts . We can find that many cases, particularly the criminal ones, have evidences hidden inside electronic devices.

1.4. The Principles of Data Encryption Algorithm

Because of the defects and disadvantages that accompanied the application of the algorithm 3DES, as it became difficult to use it the future. In the National Institute of Standards and Technology received (NIST) received ideas and proposals for the development of encryption standard. In 2001, Institute was able of the adoption of Advanced Encryption Standard (AES) in an official capacity (FIPS 197). The number of advanced algorithms in the institute was 15 algorithms. Only five algorithms have been selected for competition and voting on them. The five algorithms are (TWOFISH), (MARS), (SERPENT), (RC6) and (Rijndael). By the end of the vote, the AES algorithm (Rijndael) won and has been approved and issued officially. Algorithm (AES) also known as "Rijndael", is superior on Comparing to its predecessor 3DES in terms of its higher security, and better in performance and efficiency. In addition, it excels in terms of memory requirements, flexible software and hardware. Experts have concluded that the symmetric key encryption algorithms such as AES are very resistant to time violation.It is worth mentioning that the National Institute on adopting of this algorithm has identified its mass symmetric average with block length equal to 128-bit, and it is able to support key length (128), (192) and (256) bits.(AES) was able to impose itself as a standard for encryption around the world because of its good specifications, especially its length of the encryption standard, that making it used in a wide range of areas, particularly in the banking institutions and companies, as well as it is involved into the military uses. This was notable especially after we can DES encryption volition in 2008 after , that make many persons believe that it is not safe, and paving the way to spreading of the algorithm (AES), because of the specifications mentioned above, especially with regard strongly safety.

Although, it is common in the application that the algorithm is a one-way standard, but there is no conclusive evidence that it was one-way encryption function. As for the possibility of decoding algorithm and impenetrable it is believed they are not to do so. The structure of AES algorithm is described in Figure 1.

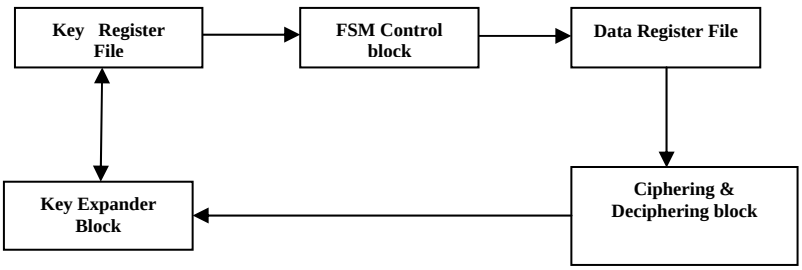


Figure 1. Data Encryption/Decryption

2. EXPERIMENT- PROPOSED SYSTEM

The application of this system which is designed to facilitate the litigation procedures through the use of modern scientific data to improve the performance of the courts, and the application of electronic litigation, will facilitate litigation procedures, and achieve the following features:

- Speed and accuracy for litigants and lawyers. Where shorten the lawyer a lot of unnecessary administrative reviews of the courts and which could be in his office access to the case file, and view it , study and follow-up , leading to the upgrading of its work and improve its performance .
- Prevent prolong the litigation. This prevents the court hearing delayed or deferred, and facilitate querying judicial transactions, and relieve congestion in the courts, also reduces the bickering between adversaries, especially in family cases.
- It requires the use of this system to prevent distortion of data, speech, or increase in, or the shortage of it.
- Reduce costs: This system contributes to reduce expenses and costs, and makes justice accessible to everyone.
- The application of this system leads to the reduction of time and effort for judges, lawyers, litigants and public prosecution.
- This system also contributes to dispense justice huge archive, and compensates for the large stores that occupy large places, and this limits the use of the suits have files, or damage to, or save them in the wrong location.

2.1. The Structure of the projected System for data manipulation in courts

The proposed system consists of the main interface that contains two parts department Admin and department user Admin the only one that encrypts the data using the encryption key which is the only one who gives authorization for the user to access the data and decryption using the same key to the encryption in it where the Admin upload Data for the job and then encrypted using the encryption key and then gives authorization for the user authorized to access the data using the same key for decryption. Thus, we have provided protection and complementary data not rigged them from unauthorized persons as Figure 2.

Is evident from the chart above that Admin is controlled information system to the case pending before the court , which alone gives validity and determines the type of this authority to each of the (judge) and (plaintiff's counsel) and (the defendant 's lawyer) and (DPP) and (plaintiff) and (the defendant), and each one of them and the validity of the user interface through which access to information concerning him .The court clerk role in the alternative would test the validity of input before storing them in the database and is shown in Figure 3.

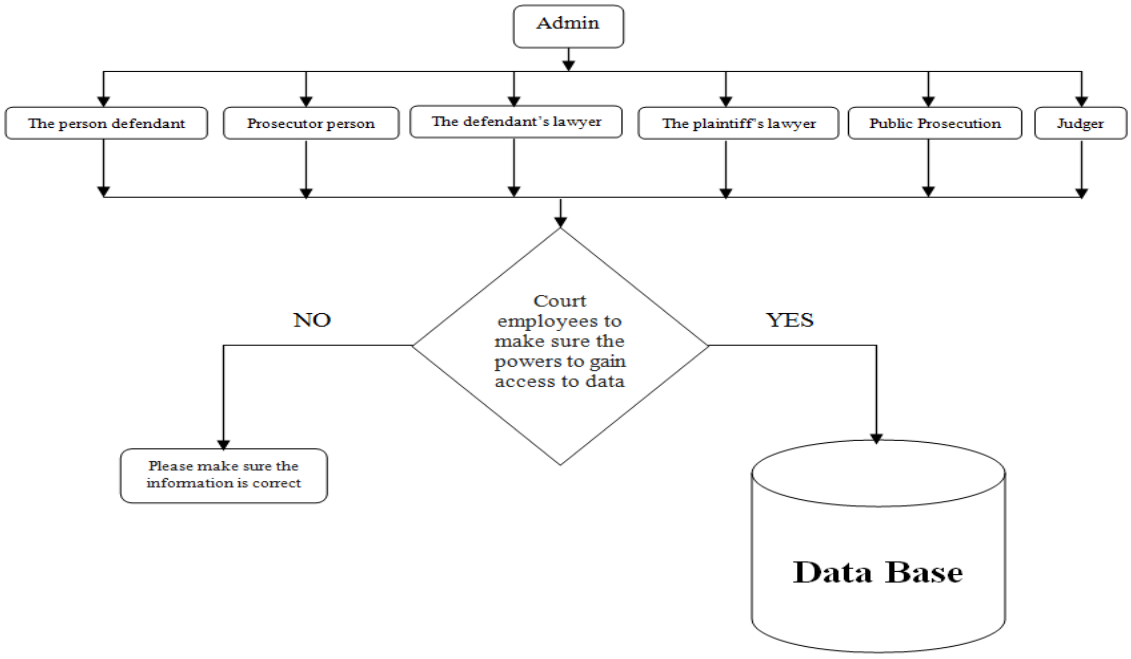


Figure 2. The proposed information system for courts

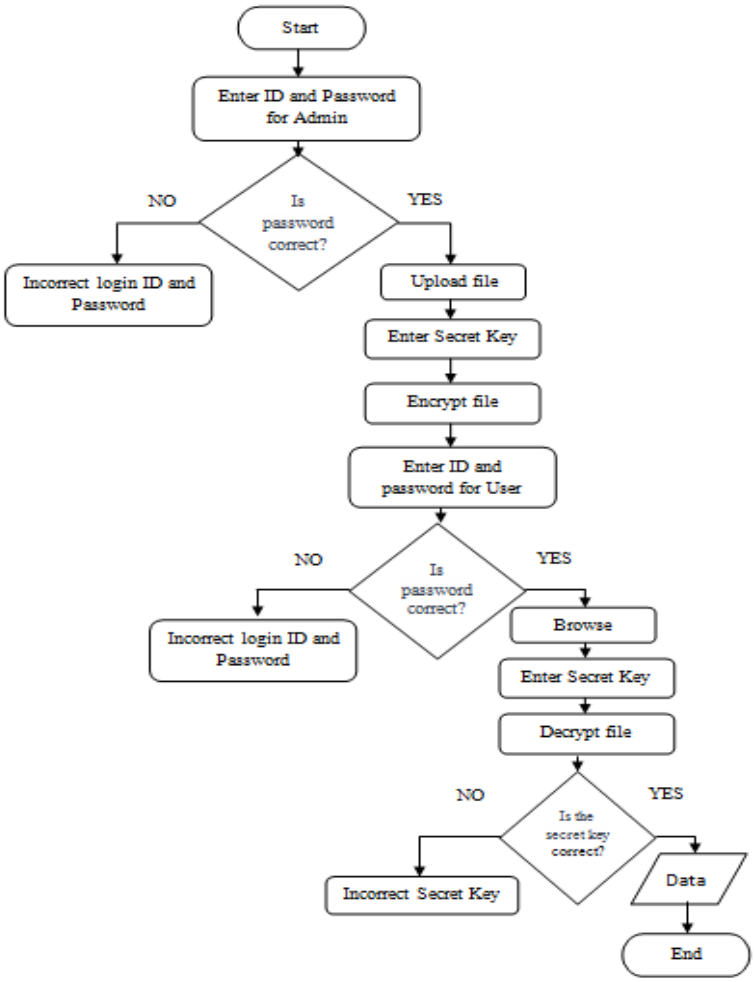


Figure 3. Litigation procedures

Containing binders lawsuit on many of the data , and this data by nature is not at the same level of importance and gravity , and can summarize data that must be the focus of protection process , both in terms of its importance , or in terms of confidentiality, as follows:

A) Big important evidence: and it is gaining importance as the basis for the suit, without losing their legal proceedings and corroboration. These are the data:
   - Loan bonds, check
   - Formal and customary editors
   - Contracts of all kinds as a contract of sale or purchase or management contracts representations before the courts
   - Medical examination results

B) Confidential data: gaining importance either because of prejudice to the reputation of the family, or individuals, or prejudice to that State. These are the data:
   - Minutes of private meetings, as in paternity cases, rape and sodomy
   - Juvenile cases with respect to the mystery of the profession as Doctors and lawyers, for example
   - Confidential expert reports (presidents and senior officials' trial of compromising the security of the state).

3. EXPERIMENTAL RESULTS

3.1. Data Measurements

The proposed system has been tested on large number of data. The device specification (CPU Core I5 2.30 GHz, 4096RAM, Windows 10 Operating System and Mat lab R2013a) that has been used to create the program is shown in Figure 4.

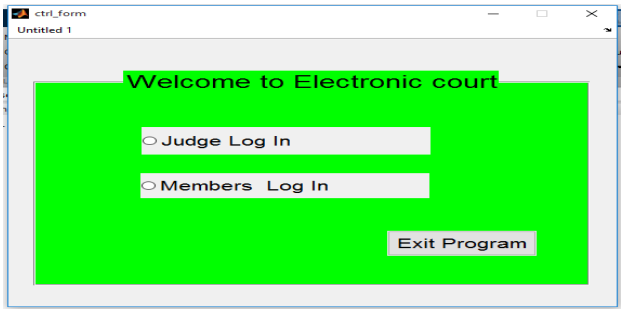


Figure 4. Main Program Form that control the entrance to the program as: 1- Judge 2-Member

The case-study scenario consists of two forms; judge Form to encrypt data and member Form to decrypt data As shown in Figure 5(a, b). Performance of the method depends on the devices specifications. During Experiments Judge encrypt various numbers of files system respond with (Size of file and Encryption Time). Members can decrypt the Files again the system responds with (Replacements, Size of file and Decryption Time).

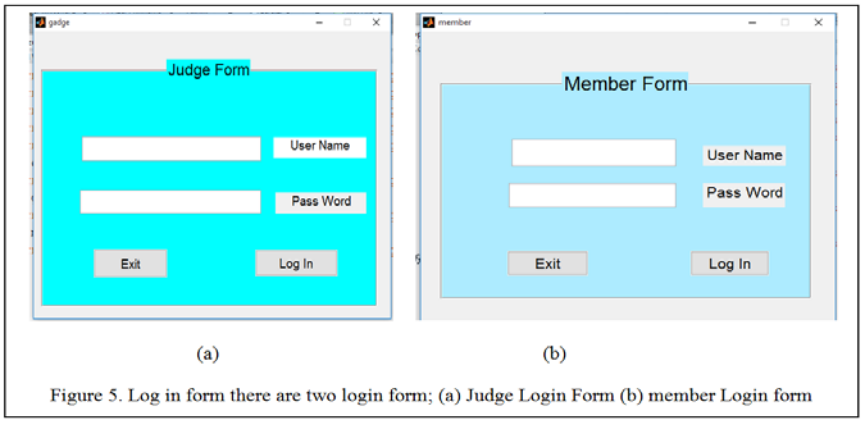
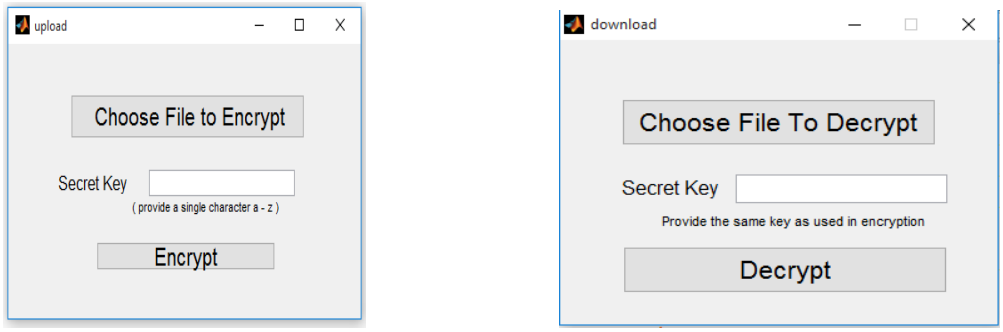


Figure 5. Log in form there are two login form; (a) Judge Login Form (b) member Login form

3.2. Data Presentation

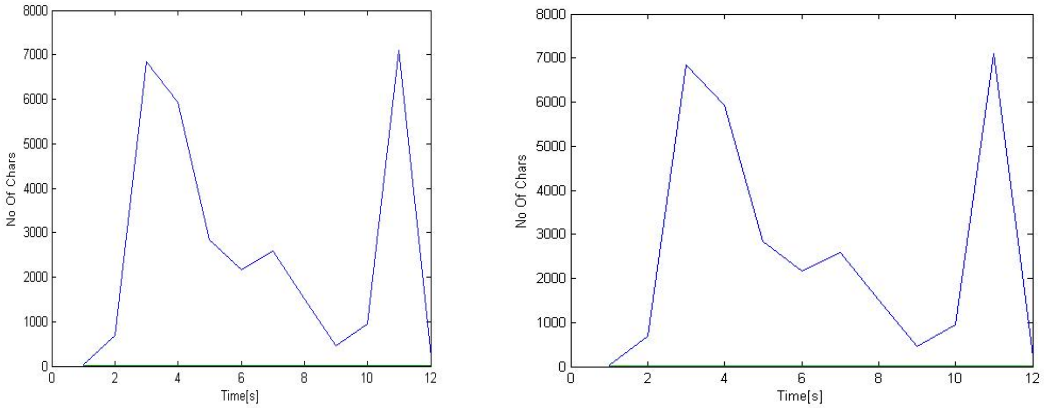
At the beginning of the experiments the system check the type of entered person depends on (type and Account information the system open the desired form). There exit two operational forms; Upload form that can be accessed via Judge to encrypt data and Download form that can be accessed via members to decrypt data Figure 6 (a,b).



(a) (b)

Figure 6. Two operational Forms; (a) Upload Form for judge to Encrypt data with private key (b) Download Form for Members to Decrypt data with the same private key

As a test of Encryption of any file system print states as follow:
Elapsed time is 0.027583 seconds. No_of_Char = 6837
As Test example of decryption of any file system print states as follow:
Character = m is decrypted to =b
…….. // to the end of file
Elapsed time is 0.003224 seconds. No_of_Char =31
Result of the application can be seen Figure 7.



(a) (b)

Figure7. Number of Characters respect to time ;(a) No of Encrypted Char respect to time ,(b) No of Decrypted Char respect to time

4. RESULTS AND DISCUSSIONS

Our system is carefully tested on large number of data sets. We used Core i5 processor with 2.30GHz and with 4GB RAM and used Matrix Laboratory with Windows 19 OS. We have created two forms like Judge Form and Member form for encryption and decryption.

For 6837 characters we got an elapsed time as 0.027583 seconds and for 31 characters we got we got an elapsed time as 0.003224 seconds. Those results showed our systems efficiency and performance with other similar systems like Sony's BMG system and NextGen case management systems. We found that our systems performance metrics are better than BMG and NextGen systems. The results and encrypted and decrypted operational form and graphs generated using our system is shown at section 3.2.

5. CONCLUSION

An efficient information system for facilitating the litigation procedures has been presented. Such information system will be applied on different types of courts. The period of processing cases in courts has been reduced. In addition, the time and effort of judges and lawyer has been saved. All the manipulated documents are encrypted to achieve secure information system. It is recommended to use such efficient system in courts to solve the main problems in developed countries.

REFERENCES

[1] C. Wang, *et al.*, "Privacy Preserving Public Auditing for Secure Cloud Storage," *IEEE Trans. Computers*, vol/issue: 62(2), pp. 362–375, 2013.
[2] B. Wang, *et al.*, "Storing Shared Data on the Cloud via Security-Mediator," in *International Conference on Distributed Computing Systems – ICDCS*, 2013.
[3] C. K. Chu and W. G. Tzeng, "Identity-Based Proxy Re-encryption without Random Oracles," in *Information Security Conference (ISC'07), ser. LNCS*, vol. 4779, pp. 189–202, 2007.
[4] C. K. Chu, *et al.*, "Conditional Proxy Broadcast Re-Encryption," in *Australasian Conference on Information Security and Privacy (ACISP '09), ser.LNCS*, vol. 5594, pp. 327–342, 2009.
[5] S. S. M. Chow, *et al.*, "Efficient Unidirectional Proxy Re-Encryption," in *Progress in Cryptology -AFRICACRYPT 2010, ser. LNCS*, vol. 6055, pp. 316–332, 2010.
[6] G. Ateniese, *et al.*, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," *ACM Transactions on Information and System Security (TISSEC)*, vol/issue: 9(1), pp. 1–30, 2006.