International Journal on Applications in Information and Communication Engineering
Volume 7 : Issue 2 : March 2021, pp 5– 9 www.aetsjournal.com ISSN (Online) : 2394 - 6237 -

A Proficient Privacy Protection Method For Cloud Computing

Ms.D.Suganya, Ms.P.Rohini, Ms.S.Saranya, Ms.K.Shanmathi, Ms.V.Thiriveni

***Abstract*—** With the rapid development of cloud computing, more cloud services are into our daily life, and thus security protection of cloud services, especially data privacy protection, becomes more important. However to perform privacy protection causes huge overhead. Thus it is a critical issue to perform the most suitable protection to decline performance consumption while provide privacy protection. The Proficient Privacy Protection Scheme (PPPS) is proposed to provide the appropriate privacy protection which is satisfying the user-demand privacy requirement and maintaining system performance simultaneously. At first, the privacy level is analyzed by users those require and quantify security degree and performance of encryption *algorithms.* Then, an appropriate security composition is derived by the results of analysis and quantified data. Finally, the simulation results show that the PPPS not only fulfills the user-demand privacy but also maintains the cloud system performance in different cloud environments.

***Keywords*—** Proficient Privacy Protection Scheme, Data Encryption Standard, Triple Data Encryption Algorithm, Advanced Encryption Standard

I. INTRODUCTION

Cloud computing is an emerging computing style which provides dynamic services, scalable and pay-per-use [6]. The different between cloud computing and other computing models are service-driven, sharing resource, and data hosting in outsourcing storage. Sharing resource makes the hardware performance be used more efficient and provides economic benefits for users to reduce the capital cost and additional expenditure [1]. The first step in the software development life cycle is the identification of the problem. As the success of the system depends largely on how accurately a problem is identified. At present, all the data is encrypted/ decrypted with same encryption method, so that all data is given same importance and so existing system is less secure. There is no application with this feature to communicate securely as well as faster. So, this project identifies that, if helps to solve the problem through the application. The software used to solve the problem and develop the application in Microsoft Visual Studio .Net 2005 and MS-SQL Server 2000. To encrypt/decrypt the data of less importance using weak encryption method so that communication is fast. To encrypt/decrypt the partial data using weak encryption method and other partial data in strong encryption method so that communication is fast and security level is raised. To encrypt/decrypt the some fields using strong encryption method and some other fields using weak encryption method so that all fields are displayed to high privilege users and some fields are displayed to low privileged users to encrypt/decrypt the watermarked contents with weak encryption method and non-watermarked contents with strong encryption method.

Ms.D.Suganya M.E., , Assistant Professor, Department of Information Technology, Velalar College of Engineering and Technology, Maruthi Nagar, Thindal, Tamil Nadu 638012. (Email: dsuganya55@gmail.com)

Ms.P.Rohini., Department of Information Technology, Velalar College of Engineering and Technology, Maruthi Nagar, Thindal, Tamil Nadu 638012. (Email: rohinipalanisamrp@gmail.com)

Ms.S.Saranya, Department of Information Technology, Velalar College of Engineering and Technology, Maruthi Nagar, Thindal, Tamil Nadu 638012. (Email: saranyaselviprt24@gmail.com)

Ms.K.Shanmathi., Department of Information Technology, Velalar College of Engineering and Technology, Maruthi Nagar, Thindal, Tamil Nadu 638012.

Ms.V.Thiriveni, Department of Information Technology, Velalar College of Engineering and Technology, Maruthi Nagar, Thindal, Tamil Nadu 638012.

II. OBJECTIVES

- To encrypt/decrypt the data of less importance using weak encryption method so that communication is fast.
- To encrypt/decrypt the partial data using weak encryption method and other partial data in strong encryption method so that communication is fast and security level is raised.
- To encrypt/decrypt the some fields using strong encryption method and some other fields using weak encryption method so that all fields are displayed to high privilege users and some fields are displayed to low privileged users.
- To encrypt/decrypt the watermarked contents with weak encryption method and non-watermarked contents with strong encryption method.

III. LITURATURE SURVEY

Data confidentiality is important for users to store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality. Because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly. Encryption is usually used to ensure the confidentiality of data [3]. It ensures that the cipher text algebraic operation results are consistent with the clear operation after encryption results; besides, the whole process

does not need to decrypt the data. The implementation of this technique could well solve the confidentiality of data and data operations in the cloud. For more flexibility and enhanced security, hybrid techniques that combine multiple encryption algorithms such as 3DES, and have been proposed while 3DES is particularly useful for encryption of block data [4]. Besides, several encryption algorithms for ensuring the security of user data in the cloud computing. A hybrid technique is proposed for data confidentiality and integrity, which uses both key sharing and authentication techniques. The connectivity between the user and the cloud service provider can be made more secure by utilizing powerful key sharing and authentication processes. A three-layered data security technique which is 3DES mechanism, the first layer is used for authenticity of the cloud user either by one factor or by two factor authentications; the second layer encrypts the user's data for ensuring protection and privacy; and the third layer does fast recovery of data through a speedy decryption process.

IV. EXISTING SYSTEM

Cloud computing is an emerging computing style which provides dynamic services, scalable and pay-per-use. The different between cloud computing and other computing models are service-driven, sharing resource, and data hosting in outsourcing storage. Sharing resource makes the hardware performance be used more efficient and provides economic benefits for users to reduce the capital cost and additional expenditure.

In the existing system, the privacy level is divided into three levels, since it is believed that users can not clearly distinguish between their privacy requirements more than three levels. In this scenario, the levels can be seen as the kinds of speed, hybrid, and security. They are explained as follows.

• Privacy Level 1 (Speed): The requirement of this level presents that no sensitive information in the data. Users want to use the weak encryption composition to obtain more performance for using cloud services.

• Privacy Level 2 (Hybrid): The requirement of this level presents that data include some sensitive information. The data requires weak encryption for partial data (such as address, mail id of corporates') and strong encryption for remaining data (such as account balances and other secure information).

• Privacy Level 3 (Security): In this privacy level, the data contains most important information. In order to protect the data security, more privileged users view most of the data and less privileged users view limited data.

A. The Drawbacks Of Existing System

The existing system has following disadvantages,

- The traditional drawback of cloud computing is that since the infrastructure of the sharing resource stored and processed users' data that do not owned by them, users' data may be revealed or breached by other malicious user in the cloud.
- Since encryption and decryption mechanism increase the processing and storage overhead, it reduces the overall efficiency.
- Since all the data is handled with same protection mechanism, unwanted over-security is applied.
- If same privilege is given to all kind of users, tight security can not be maintained.

V. PROPOSED SYSTEM

In the proposed system, the existing privacy levels which were divided into three levels seen as the kinds of speed, hybrid, and security are implemented. In addition content type wise security is provided. In this aspect, some of the document types such as already watermarked images and audio content are given less security and accessed by all kind of users whereas normal content are given more security i.e., strong cryptography is applied. This reduces the processing and communication overhead since the secure breach is not a major concern in terms of watermarked content.

A. Benefits Of Proposed System

The proposed system has following advantages,

- Since different levels of encryption and decryption mechanism are applied, the processing and storage overhead is different and reduced in most of the situation.
- Since the different data is handled with same protection mechanism, communication overhead is also reduced.
- Different privilege is given to different kind of users, so tight security need not be maintained.
- Different content types can be accessed with different security level and so speed is increased.

VI. MODULES

The following modules are present in the project.

a) Message Selection
b) Encryption
c) Speed
d) Hybrid
e) Security
f) Content Type Wise
g) Decryption
h) Speed
i) Hybrid
j) Security
k) Content Type Wise

A. Message Selection

In this module, the message content is keyed in text box control or selected from file. The message is saved into the 'RawMessages' table.

B. Encryption

In this module, four types of encryption word are carried out.

C. Speed

The requirement of this level presents that no sensitive information in the data. Users want to use the weak encryption composition to obtain more performance for using cloud services.

D. Hybrid:

The requirement of this level presents that data include some sensitive information. The data requires weak encryption for partial data (such as address, mail id of corporates') and strong encryption for remaining data (such as account balances and other secure information).

E. Security

In this privacy level, the data contains most important information. In order to protect the data security, more privileged users view most of the data and less privileged users view limited data.

F. Content Type wise

In this privacy level, some of the document types such as already watermarked images and audio content are given less security and accessed by all kind of users whereas normal content are given more security i.e., strong cryptography is applied.

G. Decryption

In this module, four types (speed, hybrid, security and content type wise) of decryption work is carried out.

Fig 1: Screen Shot 1

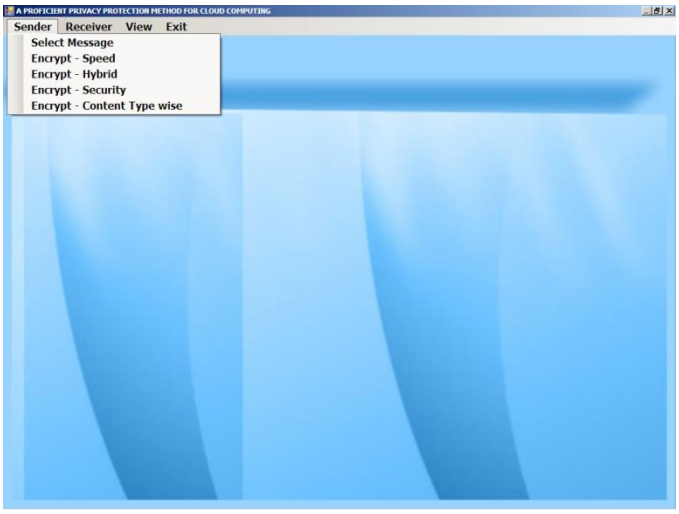

Fig 2: Screen Shot 2

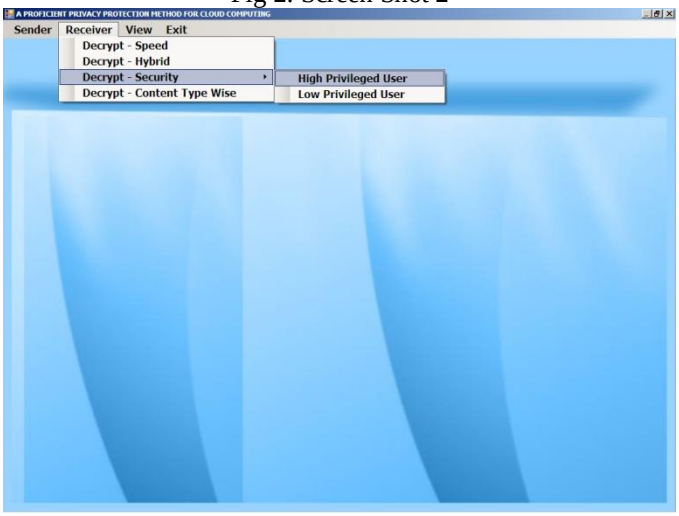

Fig 3: Screen Shot 3

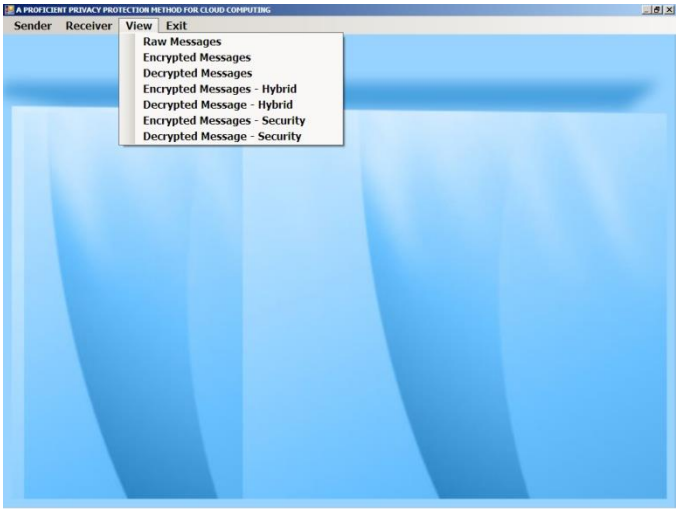

Fig 4: Screen Shot 4

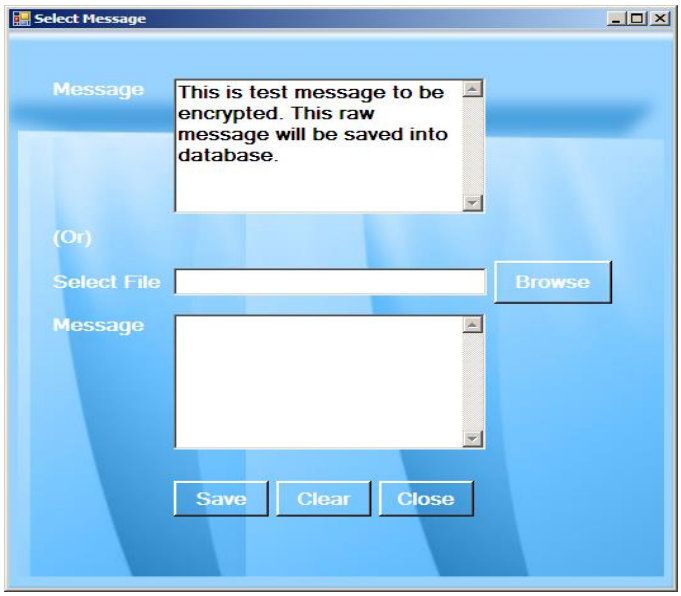

Fig 5: Screen Shot 5

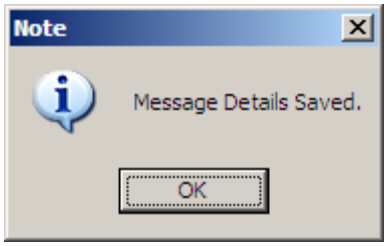

Fig 6: Screen Shot 6

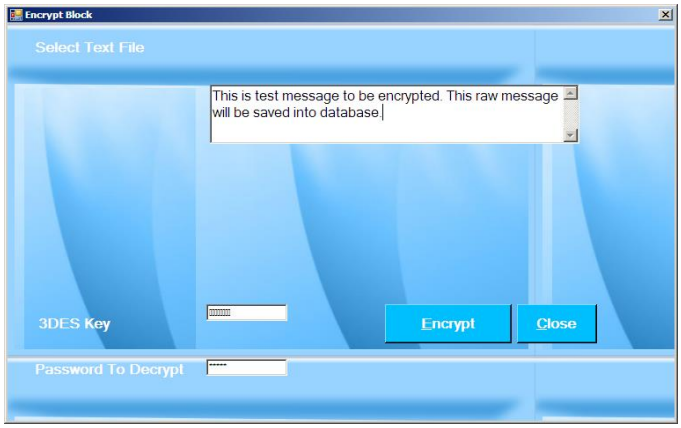

Fig 7: Screen Shot 7

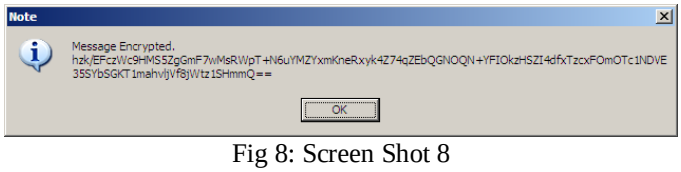

Fig 8: Screen Shot 8

Fig 9: Screen Shot 9

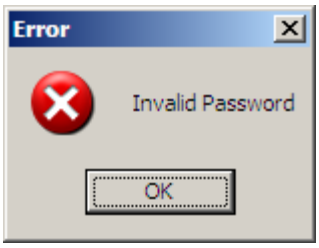

Fig 10: Screen Shot 10

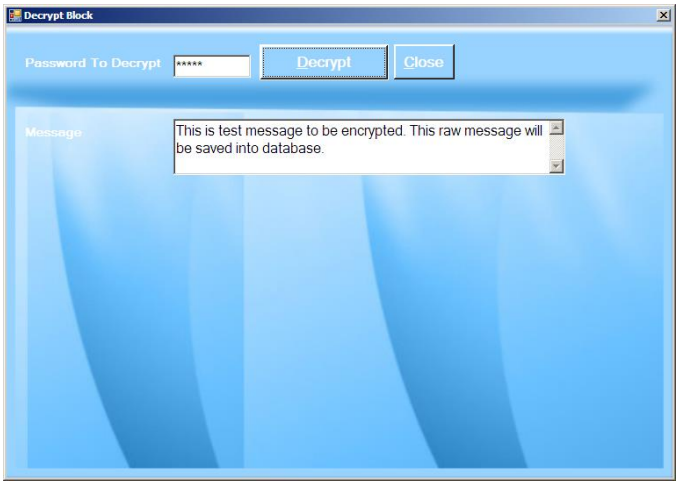

Fig 11: Screen Shot 11

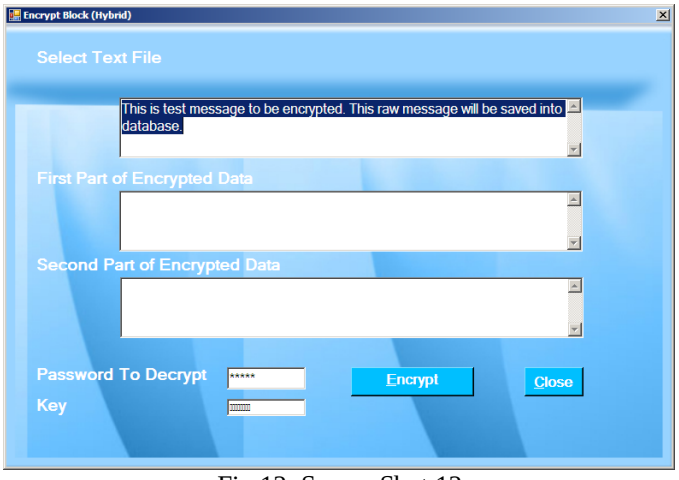

Fig 12: Screen Shot 12

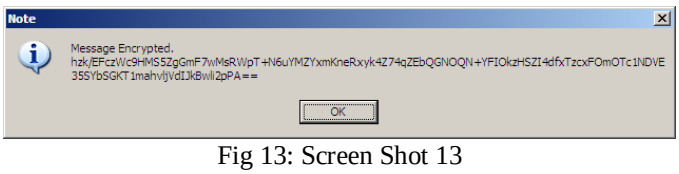

Fig 13: Screen Shot 13

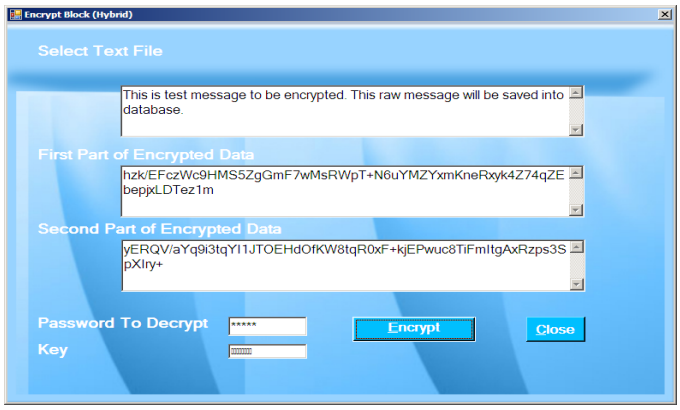

Fig 13: Screen Shot 13

VII. CONCLUSION

Through this project, the problem of secure communication is eliminated. In addition, the application required less working experience in systems to run the software. The application is tested well so that the end users use this software for their whole operations.

It is believed that almost all the system objectives that have been planned at the commencement of the software development have been net with and the implementation process of the project is completed. A trial run of the system has been made and is giving good results the procedures for processing is simple and regular order. The process of preparing plans been missed out which might be considered for further modification of the application. The project effectively stores and retrieves the records from the cloud space database server. The records are encrypted and decrypted whenever necessary so that they are secure.

VIII.FUTURE SCOPE

- The application if developed as web services, then many applications can make use of the records.
- The data integrity in cloud environment is not considered. The error situation can be recovered if there is any mismatch.
- The web site and database can be hosted in real cloud place during the implementation

REFERENCES

[1] Alistair Mc Monnies, “Object-oriented programming in VisualC#. NET”, Pearson Education, and ISBN: 81-297-0649-0, First Indian Reprint 2004.
[2] Robert D.Schneider, Jetty R.Garbus, “Optimizing SQL Server”, Second Edition, Pearson Education Asia, ISBN: 981-4035-20-3
[3] Jittery R.Shapiro, “The Complete Reference Visual C# .NET” Edition 2002, Tata McGraw-Hill, Publishing Company Limited, New Delhi
[4] http://msdn.microsoft.com
[5] http://www.c-sharpcorner.com
[6] http://www.codeproject.com
[7] http://www.programmersheaven.com