Article can be accessed online at http://www.publishingindia.com

An Additional Security Layer in the Implementation of SaaS (Software as a Service) - A Survey

Laxmi Arun[*], Divyalakshmi V. L.[**], Sharmila P.[***], Rakshitha S.[****], Amith Jacob[*****]

Abstract

With the advent of web and the concerned technologies the end users can generate or share any number of documents. A service such as collaborative edition of online documents is commonly provided through Cloud Computing as Software as a Service. However, the Cloud paradigm requires the end user's to trust their service providers. Nowadays companies provide infrastructure facilities such as storage space, processing capacity, applications, etc., for user's and companies. When confidential information of user's or that of a company is stored on such remote places there are chances of security breaches. This fact discourages companies and users to adopt to cloud services. To counter this drawback, in this paper we propose a solution for this problem by providing an additional user layer for Microsoft Azure Documents. In our paper, we have used a supplement layer to the existing user layer in the browser. This layer encrypts the data before storing it on the server. Accessing the information is impossible without the right password.

Keywords: Microsoft Azure Cloud Service for documentation Virtualization Encryption

1. INTRODUCTION

In recent years, the advent and growth of Information Technologies and the decrease in cost of servers and desktop PCs has increased the demand for many companies and individuals. Among those services, Cloud Computing stands out.

Cloud Computing is a synonym for distributed computing over a network, which is the ability to run a program or application on many connected computers at the same time. The infrastructure details remains unseen for the user in cloud computing.

In Cloud Computing there are three layers, viz.

- **IaaS (Infrastructure as a Service)** is the lower level and includes infrastructure services where machines run the applications. Examples: Amazon EC2, GoGrid or RackSpace.
- **PaaS (Platform as a Service)** is the next abstraction level. In PaaS, Application designer can develop and run their software solutions without the cost and complexity of buying and managing the hardware and software layers. Examples: Cloud Foundary, ConPaas, SalesForce, Heroku

[*] Assistant Professor, Department of Computer Science, Vidya Vardhaka College of Engineering, Mysore, Karnataka, India. E-mail: laxarun10@gmail.com
[**] Student, Computer Science (8th Semester), Vidya Vardhaka College of Engineering, Mysore, Karnataka, India. E-mail: divya.vl02@gmail.com
[***] Student, Computer Science (8th Semester), Vidya Vardhaka College of Engineering, Mysore, Karnataka, India. E-mail: shari.sharmila@gmail.com
[****] Student, Computer Science (8th Semester), Vidya Vardhaka College of Engineering, Mysore, Karnataka, India. E-mail:rakshitha.gowda@hotmail.com
[*****] Student, Computer Science (8th Semester), Vidya Vardhaka College of Engineering, Mysore, Karnataka, India. E-mail:amitjacob999@gmail.com

- **SaaS (Software as a Service)** is a delivery model in which applications are hosted and managed in a service provider's data centre, paid for on a subscription basis and accessed via a browser over an internet connection. Examples: Salesforce, Zoho, Cloud9 Analytics, DataMeer

One of the main barriers to the adoption of Cloud Computing is security. The user's data are stored on provider servers and there is no guarantee that this information will not be accessible to a third party. For this reason, many users do not trust.

Cloud services. Although the privacy problem has been addressed in virtualization platforms, Cloud privacy is completely open. One of the most important problems in shared Cloud services is that there is no guarantee that the documents will be safe.

Microsoft Azure is one among the popular Cloud Computing applications in SaaS level. The users should have an account to use the services provided by the Microsoft Azure. This paper proposes an additional security layer to secure users documents with the use of an add-on for any browser.

2. SECURITY ISSUES IN MS AZURE DOCS

Here are some of the security issues in the MS Azure documents:

- Confidential information is stored on remote servers which are under the control of service providers, hence users must trust in providers but this is not feasible.
- Cloud privacy is completely open; there is no guarantee that the information stored by user will not be accessible by third party.
- Additional layer to share and edit secure documents is still missing; they need to be improvised in order to provide additional security.

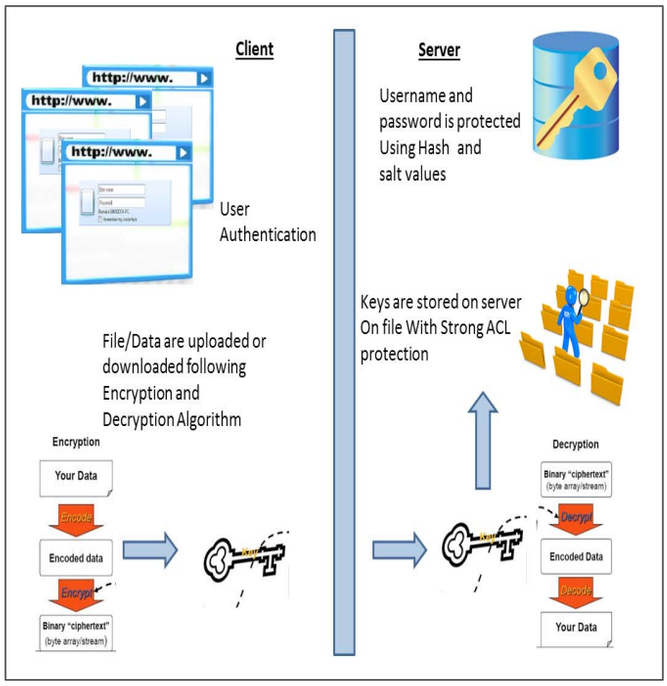
In this paper we propose a solution for the above issues. The architecture of the proposed system and the solution is explained in the following sections.

3. ARCHITECTURE OF PROPOSED SYSTEM

Data security has always been an important aspect of quality of service. Data storage is a process where the users' (or company's) confidential information is stored in servers possibly located in different geographical area, so its security and privacy can be compromised. Organizations that plan to use cloud computing to run their application require a complex procedure to deploy. These procedures needs to be upgraded frequently, should also be made available for the users and programming standards and security capabilities need to be adapted. This is a hectic task for the organizations. With SaaS, customers pay to use software via the web as a service on demand, by paying a subscription fee rather than outright purchase.

We are developing a web application where a user trusts on the service provider. A web-based application is an application that uses a web browser as a client. A web application relies on web browser in order to make the application work. Browser applications typically require little or no disk space on the client. Users do not have to worry about hardware/software compatibility and support to run an application. Since we are taking cloud services from Microsoft Azure, web application is the best way to provide additional security to the user's documents.

Figure 1. Overview of implementation of an additional security to SaaS



4. SOLUTION

We propose an additional layer to add privacy to Microsoft Azure documents, the procedure is as follows:

1. The procedure employs encryption/decryption of files during storage of files on remote servers using symmetric key encryption. In order to encrypt/decrypt the content of the document, information such as password is used to cipher each document.
2. AES encryption algorithm is used for symmetric key encryption. It generates keys, which may be identical or there may be a simple transformation to go between the keys of the end users. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.
3. Add-ons can be implemented to provide security. Once the add-ons are authorized (enabled), a new popup window pops-up, asking the user for password to compute the information, so that the variations made in the document can be saved. In contrast, the information will be in crypted form if at all the user tries to read or write the encoded (ciphered) document when all the add-on are not enabled (disabled).
4. We propose to implement exchange of symmetric/secret key through public key algorithm like Diffie-Hellman-Merkle Key exchange with the use of digital certificate and X.5O9 certificate. The Diffie–Hellman-Merkle key exchange method allows setting up a shared secret key collaboratively by two unknown parties over an unprotected communication channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
5. The files are stored in DB in an encrypted format using AES encryption from the user side. Symmetric/Secret key used for encryption is stored on client side. Secret key is unique to each user. Secret key is stored in password protected file with ACL (access control list - restricted permissions depending on the type of user accessing it) applied.

For example: Joe and Martha use a common communication channel to exchange information. Joe assigns a flag to all the files set for sharing, and also assigns the user ID to whom the file needs to be shared. Joe generates and shares a secret (cryptographic) key using Diffie-Hellman-Merkle key exchange algorithm.The keys can also be used as digital signature schemes. The exchange of digital signature usually happens through a secure communication channel such as e-mail. Martha can use the secret shared key to decrypt the file shared by Joe.

5. RESULTS

Our implementation of an add-on layer encrypts the information before storing it on servers. Accessing the information is impossible without the right password. This in turn will make the cloud more secure and more adoptable by many companies and individuals who have not been inclined towards the cloud services, due to lack of security and privacy.

6. CONCLUSION

In this paper, a new security mechanism for SaaS Application has been introduced. This mechanism provides an additional security layer which ensures more privacy to the end user by protecting their documents with a very simple user interface. The information or the data stored in the cloud are encoded using security mechanism that we have proposed. This data cannot be retrieved until and unless a matching password is provided by the user. The data is unreadable if the user forgets the password or any intruder tries to access the data without password.

REFERENCES

1. Leon-Garcia, A. & Widjaja, I. (2009). *Communication Networks- Fundamental Concepts and Key Architectures* (2nd ed.). Tata McGraw-Hill.
2. Forouzan, B. A. (2006). *Data Communications and Networking* (4th ed.). Tata McGraw-Hill
3. Adkinson-Orellana, L., Rodríguez-Silva, D. A., Gil-Castiñeira, F. & Burguillo-Rial, J. C. (2010). *Privacy for Google Docs: Implementing a Transparent Encryption Layer*. 2nd Cloud Computing International Conference - Cloud Views 2010. Portugal.
4. Adkinson-Orellana, L., Rodríguez-Silva, D. A. & González-Castaño, F. J. (2011). *Sharing Secure Documents in the Cloud, A Secure Layer for Google Docs*. Proceedings of 1st International Conference on Cloud Computing and Services Science.
5. Mir, N. F. (2007). *Computer and Communication Networks*. Pearson Education.
6. Sebesta, R. W. (2009). *Programming the World Wide Web* (4thed). Pearson Education.
7. http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
8. Assorted images from www.google.com