Journal of Engineering and Applied Sciences 13 (Special Issue 1): 2382-2387, 2018
ISSN: 1816-949X

A Cloud-Based Encryption for Document Storage Using Salesforce.com

Mehdi Ebady Manaa
College of Information Technology, University of Babylon, Babil, Iraq

Abstract: Cloud computing is new trends in information technology that enables scalable and on-demand access to a shared pool of networking recourses over the internet for efficient services delivering. Cloud computing enables all the existing technologies such as dynamic provision, storages resources and networking virtualization to the user in the form of "pay as you go". One of the open challenges of the cloud computing is security. Organizations have sensitive information to access cloud computing because of multi-tenancy approach and security. The unauthorized access will lead to loss of the organization reputation and financial loss. In this study, we propose a cloud-based encryption for the documents using the platform of the salesforce.com. The salesforce cloud computing provides a free access to the cloud objects under the user account. We use the configuration of API, WSDL, SOAP, security token and attributes of account object to design and implement a secure system for uploading the organization documents. The results show that the documents can be upload and encrypted easily in a m/sec. The implemented approach shows that the access to the cloud files is denied by unauthorized users. In addition, the multi-tenancy aspect is denied to access the sensitive information due to the encrypted uploaded files using the DES algorithm in this research. Finally, the uploaded files were uploaded in the different format and size. The obtained results show the DES algorithm provide an efficiency with cloud computing due to reducing in time implementation.

Key words: Cloud computing, DES algorithm, WSDL protocol, salesforce, data encryption, implementation

INTRODUCTION

Cloud computing considers one of the hot topics in the new IT trends which offers five characteristics: on demand self-service which can be provisioned on demand without the help of the cloud provider, broad network access to provide independent platform access for the different heterogeneous client platforms, resource pooling such as computing and storage are pooled to serve multi-users using the multi-tenancy aspect which allows multi-users to be served and accessed the same hardware using the visualization, rapid elastically and measured service.

The most suitable definition for the cloud computing is described by National Institute of Standards and Technology (NIST) "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell and Grance, 2011). Cloud computing comes to play an important role in the organization. The organizations use the cloud computing for saving and analyzing the big data. The main organizations such as Oracle, Amazon, HP intell, Sun, Cisco, YouTube, Google Application Engine, Amazon EC2 and Azure VMs were adopted the cloud computing to provide access to the data stored in the main resources (Jakimoski, 2012). The cloud computing comes to play an integral role in urban applications such as cloud computing for energy, transportation and healthcare systems. It provides the application for large-scale application such as cloud computing for government, manufacturing industry and for education.

One of the open challenges for the cloud computing is to provide a dynamic provision on demand when the user needs to implement the application that needs more computation and storage without interaction with the real hardware. The other challenge for the cloud computing is to protect the essential data in the cloud because of multi-tenancy aspect. The main reason for this challenge that the essential data are hosted on many servers outside the owner to reduce tie and satisfy the scalability. The cloud computing needs robust techniques to protect essential data in the organization and to satisfy the security criteria CIA (Confidentiality, Availability and Integrity) (Manaa, 2017). The security criteria are provided in the cloud computing by protection the data from the unauthorized access using the confidentiality. Data

access through the shared storage resources in the cloud is provided by the availability. In addition, the data consistency is conducted by the integrity. Hence, losing any factor of these criteria will lead to loss of customer confidences (Aldossary and Allen, 2016). In this study, a robust method to encrypt the data in files before uploading this file to the SaaS salesforce.com cloud computing. The DES algorithm is very efficient in encryption with less time.

Literature review: The trust, security and privacy consider the most security barriers for the organization to adopt the cloud computing. To gain a trust of the organization, the cloud provider such as force.com must provide a level of security and privacy. In the computing context, the security must provide a level of security against the computer threats. Privacy concerns with the digital collection and sharing information (Anonymous, 2010).

Chaudhari and Mandre (2016) present a scheme to encrypt the data using rijndael encryption algorithm on cloudSim. The sensitive data is encrypted in less time and upload to the cloud. The results illustrate the time required for encryption and decryption process. In addition, the time required to generate the encryption key versus the number of the attributes is presented. The main configuration for the cloud is not showing up and the length of the key is not presented in the encryption algorithm (Chaudhari and Mandre, 2016).

Sarker and Kumer (2016) present a security model from three entities. The first entity Cloud Service Provider-1 (CSP1) performs the computation for the user to interact with the other CSP-2 and CSP-3 to share the key and encryption algorithms. The CSP-2 deals with encryption-decryption and key generations. The data storage and temporary files ate stored in the CSP-3. The results are not evaluated in terms of encryption and decryption time (Sarkar and Kumer, 2016).

Rewagad and Pawar (2013) have proposed a hybrid encryption scheme using digital signature and Diffie-Hellman key with the encryption algorithm (AES) advanced encryption algorithm to protect the confidentially of the data in the cloud. The scheme shows the robust in the user private key because the facility of the Diffie-Hellman key becomes useless in the hacking process by the unauthorized user. The results are not described the time of the key generating and encryption/ decryption algorithms (Rewagad and Pawar, 2013). Bansal and Singh (2015) proposed an efficient approach to encrypting the data using blowfish and RSA algorithm.

The system was implemented using the FPGA device Virtex-4 320 I/O with the total pins 64 which are used for input and output. The 64 bits key size is used in this research (Bansal and Singh, 2015).

The security of the cloud layers (SaaS, IaaS and PaaS) are examined by Yesilyurt and Yalman (2016) by presenting a study that the vulnerabilities in IaaS layer are less common compared to other layers. Trojan and malware are most common threats in the PaaS virtual layer. The cloud layer needs examination at regular intervals from the harmful software.

MATERIALS AND METHODS

The proposed system

Cloud models: The NIST defines three models for the cloud computing: Software as Service (SaaS), Platforms as Service (PaaS) and Infrastructure as Service (IaaS). The brief description for each model is described as: (Mell and Grance, 2011; Saxena and Chourey, 2014; Bendovschi and Ionescu, 2015).

Software as a Service (SaaS): The complete software and application are provided to the users in this layer. It is the first layer of cloud computing which focuses on the end-user requirements and sometimes referred as "on demand software". The web browser is used to access all the software and applications in the cloud platform. The security is the main challenge is this model for user's data because of the threats. Examples of SaaS model are Salesforce.com, Facebook, Google Apps, Zoho, Dropbox, Taleo, Microsoft office 365, LinkedIn, Slideshare and Youtube.

Platform as a Service (PaaS): This layer enables the users to deploy the applications and programs using Application Programming Interface (API) and software libraries because the users are responsible for developing configuration and managing the cloud infrastructure. The essential data is unsecured because the underlying infrastructure (servers, network, storage and operation system) are managed by the cloud provider. Example of PaaS model is Google App Engine force.com, Windows Azure, Heroku, Gigaspace, AppScale, Loglump.

Infrastructure as a Service (IaaS): This layer provides the user with the capability to provision computing and storage resources in term of the virtual machine instance and virtual storage. The users install and manage their OS and application. Cloud provider is manged the underlying

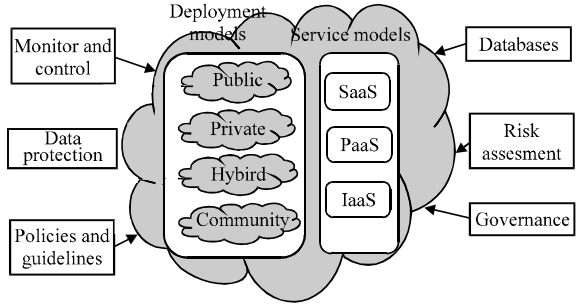

Fig. 1: Cloud services with deployment models

Table 1: Cloud deployment models for organization

Cloud models	Available to	Provided by
Public cloud	General public and for large industrial group	External service provider
Private cloud	Single organization	Internal/external service provider
Hybrid cloud	Individual users	Public cloud: internal/external
	Small and medium enterprise	service provider
	Large organization	Private cloud: internal/external
	Governments	service provider
Community cloud	Several organizations supporting specific community	internal/external service provider

infrastructure for the cloud. In this case, the user essential data is unsecured because the data is saved in remote servers. The services provided to the user in the term of "pay-per-use paradigm". RackSpace, Joynet, Terremarkm opSource, Savvis and Enamoly are examples of IaaS cloud computing. The cloud deployment models are classified into public, private, hybrid and community. Figure 1 illustrates the cloud deployment models regarding the IaaS, PaaS and Saas. Cloud deployment models are categorized into public, private, hybrid and community depending on company policies in term of cost and sharing. Table 1 shows cloud deployment models with available and provided owner for the organization and users.

Security in the cloud computing: There are many types of attacks that jeopardized the cloud computing in different models. In cloud computing, the unauthorized user tries to access the essential information in the cloud due to multi-tenancy aspect and send many bogus packets. One of the dangerous attacks is the DDoS attack which affects on the security criteria (Availability integrity and confidentially) (Manaa, 2017). Virus, Trojan, web browser attacks, Brute force attack, SQL injection, cross-site scripting attack, a man in middle attack and data loss are cloud computing attacks (Chou, 2013; Khalil *et al*., 2014; Kumar and Iyakutti, 2014).

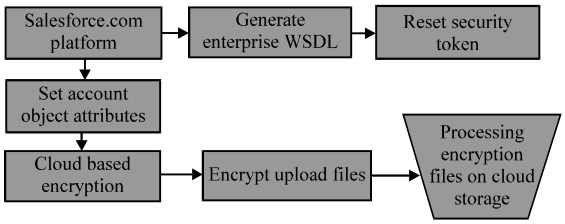

Fig. 2: The proposed system of a cloud-based encryption for document storage

Data encryption is one of the promising solving approach using in the cloud computing. The uploaded file needs to be encrypted before upload to the cloud using many of the encryption methods. In this study, we encrypt the data for different file such as PDF, PNG, Word, Excel file, …, etc. to be encrypted during the upload to the cloud. Salesforce.com is used as the cloud platform. The deployment design for A cloud-based encryption for document storage using salesforce.com for this study is described in Fig. 2.

Salesforce.com: Force.com is PaaS cloud platform that allows developers to provide multitenant adds on applications on Salesforce.com platform. Saleforce.com is SaaS cloud computing that provides built-in Customer Relationship Management (CRM) applications that helps the client to analyze, sell, market and connect with the customers. Salesforce helps the client to provide built in Application Programming Interface (API) to interact with the cloud platform. It provides sources for saving the information in cloud data storage resources.

Salesforce provides different services such as self-service management, channel services, partner marketing. In addition, it provides search, tagging and subscription. It provides integrated service with Google Apps and Google Adwords.

WSDL and SOAP protocols: Web service is a computer software that makes uses to access these services over the internet and to take advantages of its functions. It uses the standardize XML schema and provide access to the application using types of services:

- REST service
- WSDL and SOAP

Web Services Description Language (WSDL) is utilized to provide web service by Simple Object Access

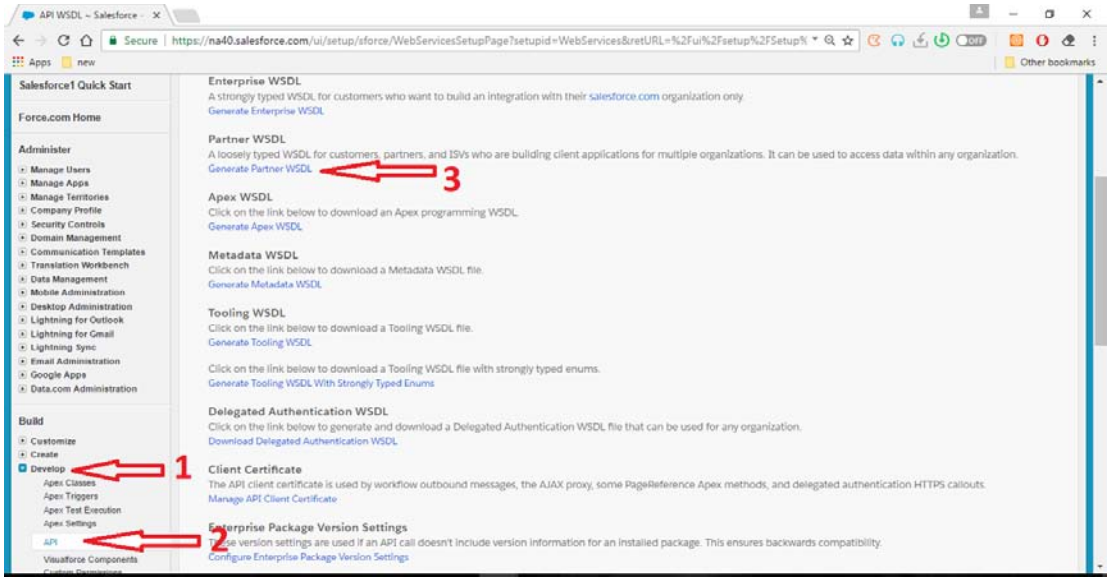

Fig. 3: Enterprise WSDL in Salesforce.com

Protocol (SOAP) and by using XML schema. SOAP protocol is used for exchanging structured information in the implementation of the web services. Salesforce.com makes interaction with the client by using the partner WSDL. It allows the client to download it and import it in the application programming language as references. The WSDL file structure is XML-based schema to embed the definition of the objects. When the client uses the Salesforce cloud. Figure 3 shows the genrating of enterprise WSDL from Salesforce.com.

The SOAP considers as Remote Procedure Call (RPC) for calling the function in WSDL. The XML format is used via. SOAP to define the extensible messaging framework which makes human understand messages in an easy way. The SOAP API provides many types of functions such as creating, redesigning, updating and deleting records. Salesforce provides an account object with many attributes to enable client saving the information in the cloud and retrieval it on demand. The SOAP API is also used in any programming language that permits the users to build application in Salesforce.com.

Data encryption approach: DES (Data Encryption Standard) algorithm is a symmetric-key algorithm that is used by NIST (National Institute of Standards and Technology) in 1977. It is used 64 bit for Plaintext block and 56 bit for the key (64 bits but 8 are parity) to generate ciphertext based 64 bit. In brief, it consists of three phases in the first one, the plain text with 64 bit is passed to the permutation process to produce the right input for the next phase via. reordering of bits. The second phase has permutated the text with 16 times to produce left and right text. The ciphertext in the last phase is produced using the inverse of the initial permutation. The general description of this algorithm is illustrated by Stallings and Tahiliani (2014). The decryption process is applied the same encryption algorithm except for the application of the subkeys is reversed. In this study, the DES algorithm was used to encrypt the data attachment on the Salesforce (cloud server). The integration program uses the C# program as the client that upload the encrypted file in the cloud Salesforce.com platform. The connection is provided the secure connection using the Transport Layer Security TLS 1.1 and/or TLS 1.2TL. The scripts shows the TLS 1.1/ TLS 1.2 secure connection:

```
ServicePointManager.SecurityProtocol =
SecurityProtocolType.TLS12| SecurityProtocolType.
TLS11| SecurityProtocolType.TLS
```

Algorithm 1 describes the main steps of the configuration with Salesforce.com cloud using the C# application program.

Algorithm 1; The configuration parameters with Salesforc.com cloud platform:

Input: Email User (EU); Password (PW); Security Token (ST), Enterprise WSD

Output: Open connection with cloud using SOAP protocol

Begin

IF (userName and password is corrected) {
IF (Verification EU by send code == true) {
Start connection
Rest security token from Salesfocrc.com

Get organization ID from Salesforce.com
Integrate API
Generate enterprise WSDL
Use SOAP to interact with cloud
} }
Else
{
System.out.println ("Unauthorized userName or Password")
}
End algorithm

The programming language is used to interact with the cloud using the SOAP protocol. The upload file is encrypted using the DES algorithm. The main steps of encrypting the uploaded files in the cloud are illustrated in Algorithm 2.

Algorithm 2; The encryption of the uploaded file in the Salesforce.com:

Input: Encryption Key (K), Upload File (F)
Output: Encrypted file in the Salesforce.com
Begin
Generate K for encryption
Get the file bytes in array of bytes
Applying DES one each byte
Set Account Object body in the Salesforc.com to encrypted file
Uploaded the encryption file to the Salesforce.com
End algorithm

The main steps of the decryption algorithm is described in Algorithm 3.

Algorithm 3; Decryption of the file from salesforce.com cloud:

Input: Key (K), Encrypted File (EF)
Output: Original file
Begin
Key generation
Get Encrypted File from Salesforce.com Server
Apply decryption using DES algorithm for each file
Optionally, compare the original file with the decrypted file
End algorithm

RESULTS AND DISCUSSION

The main goal of this study is using the cloud to reduce time in encryption time when the file is uploaded to the Salesforc.com. The cloud server provides a powerful capability that helps to increase the encryption process and prevent the multitenant from accessing these files in the public cloud. The obtained results are showed that the proposed method includes two stages in term of integration programming with the cloud. The first stage creates library jar file which includes integration of WDSL and Force.com Web Services Connector (WSC) in the jar file to open the secure connection with Salesforce. The second stage includes implements DES data encryption upload the encrypted file to the cloud. Table 2 the data type, size and time of encryption in local and cloud in second.

Table 2: Time of DES encryption in local computer and salesforce.com

Type of uploaded file	Data size (bytes)	Time of encryption in local (sec)	Time of encryption in cloud (sec)
PDF	11,168,583	0.968	2.125
PDF	7,385,288	0.797	1.515
PDF	1,894,678	0.250	0.422
PPT	3,567,616	0.440	1.972
PDF	29,131,385	2.844	5.609
PDF	36,525,454	3.125	6.547
DOC	26,517	0.033	0.065
PDF	2,939,00	0.328	0.672
PDF	16,851,679	1.761	3.080
PDF	12,704,841	1.375	2.547
PNG	131,832	0.047	0.110
Mp4	145,914,602	12.258	25.699
DOC	1,041,785	0.192	0.407
TXT	3,149	0.019	0.043
GIF	49,270	0.035	0.060

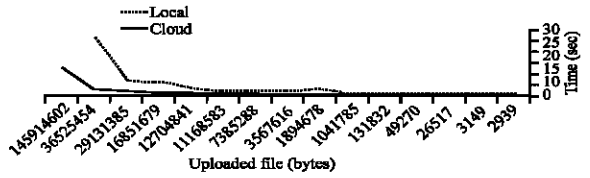

Fig. 4: Time of uploaded file encryption using Salesfocre.com

Figure 4 shows the chart for Table 2. It is clearly noticed that the cloud Salesforce.com platform has less time than the local time to encrypt the file uploaded.

CONCLUSION

Salesforce.com is SaaS platform that provides access, analyze and update data in the cloud using the WSDL-based XML and SOAP protocol. The objects attribute such as account object in the Salesforce cloud help to employ the user local application with the cloud. The account object provides many attributes to encrypt the data from local to the cloud. It is clearly noticed in the results that the cloud help in reducing the time for the uploaded file using the efficient encryption DES algorithm. The key for the encryption/ decryption is used for the same file before upload it and after download it from the cloud. The integration API services that are provided by the cloud salesfroce.com provider can be used with the local programming language on the client computer. Hence, the results provide a less time in the encryption process using the cloud, it is beneficial to apply this technique on large files for the organization that have essential information and protect these files from unauthenticated access.

RECOMMENDATIONS

The future research will be applied in more than one encryption algorithms for the efficient encryption process. We need to employ other platforms such as Heroku platform because some of the cloud platforms have limited free access to integrate with its service.

REFERENCES

Aldossary, S. and W. Allen, 2016. Data security, privacy, availability and integrity in cloud computing: Issues and current solutions. Intl. J. Adv. Comput. Sci. Appl., 7: 485-498.

Anonymous, 2010. Secure, private and trustworthy: Enterprise cloud computing with Force.com. FinancialForce.com, San Francisco, California, USA.

Bansal, V.P. and S. Singh, 2015. A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs. Proceedings of the 2015 2nd International Conference on Recent Advances in Engineering and Computational Sciences (RAECS), December 21-22, 2015, IEEE, Chandigarh, India, ISBN: 978-1-4673-8253-3, pp: 1-5.

Bendovschi, A.C. and B.S. Ionescu, 2015. The gap between cloud computing technology and the audit and information security. Audit Financiar, 13: 115-121.

Chaudhari, S.H. and B.R. Mandre, 2016. Secure data retrieval based on attribute-based encryption in cloud. Intl. J. Comput. Appl., 134: 31-35.

Chou, T.S., 2013. Security threats on cloud computing vulnerabilities. Int. J. Comput. Sci. Inf. Technol., 5: 79-88.

Jakimoski, K., 2012. Security techniques for protecting in cloud computing. Intl. J. Grid Distrib. Comput., 9: 49-56.

Khalil, I.M., A. Khreishah and M. Azeem, 2014. Cloud computing security: A survey. Comput., 3: 1-35.

Kumar, B.S. and K. Iyakutti, 2014. A novel technique: Data leakage hindering in cloud computing using swarm intelligence. Intl. J. Comput. Technol. Appl., 5: 1886-1891.

Manaa, M.E., 2017. Data encryption scheme for large data scale in cloud computing. J. Telecommun. Electron. Comput. Eng., 9: 1-5.

Mell, P. and T. Grance, 2011. The NIST definition of cloud computing recommendations of the national institute of standards and technology. Nist Spec. Publ., 145: 1-7.

Rewagad, P. and Y. Pawar, 2013. Use of digital signature with Diffie Hellman key exchange and AES encryption algorithm to enhance data security in cloud computing. Proceedings of the 2013 International Conference on Communication Systems and Network Technologies (CSNT), April 6-8, 2013, IEEE, Gwalior, India, ISBN: 978-1-4673-5603-9, pp: 437-439.

Sarkar, M.K. and S. Kumar, 2016. Ensuring data storage security in cloud computing based on hybrid encryption schemes. Proceedings of the 2016 4th International Conference on Parallel, Distributed and Grid Computing (PDGC), December 22-24, 2016, IEEE, Waknaghat, India, ISBN:978-1-5090-3669-1, pp: 320-325.

Saxena, T. and V. Chourey, 2014. A survey paper on cloud security issues and challenges. Proceedings of the 2014 International Conference on IT in Business, Industry and Government (CSIBIG), March 8-9, 2014, IEEE, Indore, India, ISBN:978-1-4799-3063-0, pp: 1-5.

Stallings, W. and M.P. Tahiliani, 2014. Cryptography and Network Security: Principles and Practice. Pearson, London, UK.,.

Yesilyurt, M. and Y. Yalman, 2016. New approach for ensuring cloud computing security: Using data hiding methods. Sadhana, 41: 1289-1298.