DEVELOPING SECURED INTEROPERABLE CLOUD COMPUTING SERVICES

Al-Khanjari, Z.
Alani, A.
Department of Computer Science, College of Science,
Sultan Qaboos University, Muscat, Oman

Abstract

Developers of cloud computing systems are responsible for identifying the requirements of Quality Attributes and developing security of cloud computing systems. Developing a quality cloud computing systems needs to satisfy interoperability, security, safety, dependability, performance, and other. Security of cloud computing services represents another incentive that will promote the use of cloud services by related stakeholders. Also, security is considered as an important issue when dealing with cloud services' interoperability. Using good protected access control technique can prevent many security problems. This paper proposes steganography scheme as a new architecture to secure the data in cloud computing by exploiting text properties. Also, it describes the implementation of the data steganography technique, which could provide more security to the cloud computing environment to achieve the trusted computing technology.

Keywords: Cloud computing, Data Steganography, Steganalysis, Interoperability, Protected Access Control

1. Introduction

Cloud computing is available over the internet to share data, applications and hardware. Cloud computing provides unlimited infrastructure to store data and execute the applications. The customers do not need to own the infrastructure. One of the main problems with cloud based computing services, is that the uncertainty about the level of information security offered by these services. Infrastructure-as-a-service (IaaS) of cloud computing system is seen as providing all access control security. In the clouds, data are sent to and processed in the environment that is not under the user or data owner control. Therefore, it could potentially be compromised either by clouds insiders or by other users sharing the same resource. Data must be secured during all processing stages including:

uploading, processing, storing, streaming and/or visualizing. Policies and security requirements must be bound to the data. To enforce these policies, the corresponding security mechanisms should be in place.

Demchenko and colleagues [1] presented and developed the Intercloud Architecture that addresses problems with multi-domain heterogeneous cloud based applications, integration, inter-provider and inter-platform interoperability. They analyzed the security issues in provisioning complex heterogeneous multi-provider intercloud infrastructures. Their analysis provided a good basis for further intercloud security infrastructure definition and development. Sharon and colleagues [2] explored the vulnerabilities and threats of cloud storage. Cloud storage represents one of the domains of cloud computing that affects the different cloud service models. Mayank [3] described an online compiler, which helps in reducing the problems of portability and storage space by using the concept of cloud computing. Aniruddha and Chaudhari [4] discussed in detail the types of infrastructures that can be made available as services with all issues regarding designing and implementing IaaS. Also, they described the IaaS model of the cloud computing and discussed all the up to date information on the IaaS. Ateniese and colleagues [5] proposed a secured distributed storage scheme based on proxy re-encryption. Specifically, they described how to use the symmetric content keys to encrypt blocks of data content. The content keys are then encrypted with a master public key, which can only be decrypted by the master private key kept by the data owner. The data owners use their master private key together with user’s public key to generate proxy re-encryption keys. In this way, the semi-trusted server can then convert the cipher text into that for a specific granted user and fulfill the task of access control enforcement. Ravij and colleagues [6] discussed the issue of how to prevent data from such attacks. They proposed a technique, which is actually a combination of Identity Based Encryption (IBE) and Mediated RSA (mRSA) techniques for Cloud environment. They used to reduce difficulties and overhead of certificate management during communication between users. This could be done by using Hash functions. Also, Mediated RSA technique could be used to provide easy key generation and key management during communication. Ankur and colleagues [7] summarized the area of cloud security by focusing on virtualization security. Yuri and colleagues [8] developed and presented the architectural framework for cloud based infrastructure services provisioning. They proposed architecture, which intended to provide a basis for building multilayer cloud services integration framework and to allow optimized provisioning of computing, storage and networking resources. Also, they proposed Inter-Cloud architecture, which would facilitate cloud services’ interoperability and integration. Selvn and colleagues [9] discussed the issue of how to secure the data while storing it in the cloud server. They suggested following few steps, including the implementation of: 1. new data displacement strategies, 2. service level agreement between the user and the cloud service provider and 3. quality of service verification. Steve [10] defined the cloud computing as a technology that uses the internet and central remote servers to maintain data and applications. They discussed the ability of cloud computing to allow consumers and businesses to use applications without installation and to access their personal files at any computer with internet access. They claimed that this technology would offer much more efficient computing facilities by centralizing storage, memory, and processing bandwidth.

The rest of the paper is organized as follows: Section 2 discusses the cloud computing and its related issues. It also describes the service and deployment models. Section 3 provides information about steganography, and the barriers and challenges of Steganalysis. Section 4 describes the purpose of the development of the Steganography Scheme Architectural Model in cloud computing. It also describes the steganography scheme used to hide the data when requested, process data and display it with all text properties. Finally, Section 5 provides concluding remarks of the work and future prospects.

2. Cloud Computing

Everyone is talking about cloud computing today, but not everyone means the same thing when they do. While there is this general idea behind the cloud – that applications or other business functions exist somewhere away from the business itself – there are many iterations that companies are looking for in order to actually use the technology. Cloud computing offers a variety of ways for businesses to increase their IT capacity or functionality without having to add infrastructure, personnel, and software in their business. Also, cloud computing is available 24/7, which allows people to work when they want to, not restricting them to office hours only [11].

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 [9]. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models [8].

2. Service Models

Cloud computing provides three types of services listed as follows:

- **Cloud Software-as-a-Service (SaaS):** This provides the use of applications running on the cloud provider’s infrastructure. These services can be accessible from any heterogeneous system or any interface. These services may be defined with exception of limited user specific usage.

- **Product-as-a-Service (PaaS):** This provides development platform for the user to develop applications using the tools provided by the PaaS provider.
- **Cloud Infrastructure-as-a-Service (IaaS):** This provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources. This way enables the consumer to deploy and run arbitrary software, which can include operating systems and applications [6, 12].

2.2 Deployment Models

Each company chooses a deployment model for a cloud computing solution based on their specific business, operational, and technical requirements. There are four primary cloud deployment models listed as follows:

- **Public Cloud:** This is the deployment model that is most commonly described as cloud computing. In this model, all of the physical resources are owned and operated by a third party cloud computing provider.
- **Private Cloud:** This model describes computer services that are delivered to a single organization.
- **Community Cloud:** This model contains features of both the public and the private cloud models.
- **Hybrid Cloud:** This model employs aspects of all other cloud models and is the most commonly found cloud deployment model used within large organizations [13].

2.3 Characteristics

Cloud computing exhibits the following key characteristics [10]:

- Improves with users' ability to re-provision technological infrastructure resources.
- Offers Application Programming Interface (API) accessibility to software that enables machines to interact with cloud software in the same way as the user interface facilitates interaction between humans and computers.
- Claims the reduction of the computing cost, since in a public cloud delivery model capital expenditure is converted to operational expenditure.

- Provides device and location independence. This enables users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile phone).
- Uses virtualization technology that allows servers and storage devices to be shared and utilization to be increased. Applications can easily be migrated from one physical server to another.

2.4 Cloud Computing Threats

Security and privacy are the challenges associated with cloud computing, which is related to storing and securing data, monitoring the use of the cloud by the service provider. New threats avenues are introduced. When an organization moves its critical data and applications to a cloud storage server, new approaches for securing data in the cloud must be implemented. Top seven security threats to cloud computing are listed below [2]:

- Abuse and nefarious use of cloud computing.
- Insecure interfaces and Application Programming Interface (API).
- Malicious insiders.
- Shared technology issues.
- Data loss and leakage.
- Account and service hijacking.
- Unknown risk profile.

3. Steganography

Steganography is the art and science of hiding information into covert channels so as to conceal the information and prevent the detection of the hidden message. Steganography is defined as hiding information with the existence of a noise. It is considered as a way to enhance but not to replace encryption. It is used to prevent the existence of encrypted data from being detected. Both steganography and cryptography are used in the data hiding techniques [15]. The cryptography is the practice of scrambling a message to an obscured form to prevent others from understanding it. However, the steganography is the study of obscuring the message so that it cannot be seen.

Steganography messages may first be encrypted. Then a cover message is modified to contain the encrypted message, resulting in stego text. Only those who know the technique used can recover the message and, if required, decrypt it.

3.1 Steganography Techniques

Information hiding techniques are receiving much attention today. The main motivation for this is largely due to fear of encryption services getting outlawed, and copyright owners who want to track confidential and intellectual property copyright against unauthorized access and use of digital materials such as music, film, book and software through the use of digital watermarks.

There are many ways to hide information. We look at the following approaches [16]:

- Least significant bit insertion.
- Masking and filtering.
- Algorithms and transformations.
- Each of these techniques has varying degrees of success.

3.2 Steganalysis

Steganalysis is the process of detecting steganography by looking at the variances between bit patterns and unusually large file sizes [17]. It is the art of discovering and rendering useless covert messages.

3.3 The Challenges of Steganalysis

Some of the challenges of steganalysis are listed below [18]:

- The suspect information stream, such as a signal or a file, may or may not have hidden data encoded into them.
- The hidden data, if any, may have been encrypted before inserted into the signal or the file.
- Some of the suspected signals or files may have noise or irrelevant data encoded into them (which can make analysis very time consuming).
- Unless it is possible to fully recover, decrypt and inspect the hidden data, often one has only a suspect information stream and cannot be sure that it is being used for transporting secret information.

3.4 Types of Attacks

Attacks and analysis on hidden information may take several forms: detecting, extracting, and disabling or destroying hidden information. An attack approach is dependent on what information is available to the steganalyst (the person who is attempting to detect steganography-based information streams) [19].

- **Steganography-only attack:** Only the steganography medium is available for analysis.

- **Known-carrier attack:** The carrier as the original cover and steganography media are both available for analysis.
- **Known-message attack:** The hidden message is known.
- **Chosen-steganography attack:** The steganography medium and tools (or algorithms) are both known.
- **Chosen-message attack:** A known message and steganography tools (or algorithms) are used to create steganography media for future analysis and comparison. The goal in this attack is to determine corresponding patterns in the steganography medium that may point to the use of specific steganography tools or algorithms.

Known-steganography attack: The carrier and steganography medium, as well as the steganography tool or algorithm, are known.

4. The Proposed System

The proposed system provides techniques on how to hide the data through security pipeline channel. This is used to provide protected access control to the data in Software-as-a-Service of cloud computing system. By using steganography, the data will provide safety, dependability, performance, integrity and confidentiality to the communication system in SaaS cloud when exchanging data. It is based on hiding the data with all text properties when data is requested and displayed. Steganography scheme is designed to keep the safety and integrity of the data and prevent unauthorized user to access the data in SaaS cloud. This steganography scheme uses all text properties to hide the data when requested, processed and displayed. Text properties includes: manipulating fonts, font metrics, font styles, color and their RGB values, and the x, y location to display data.

4.1 The Proposed Steganography Scheme Architectural Model

We also propose Steganography Architecture in cloud computing as illustrated in Figure 1. It contains the following layers:

- **Physical Layer:** Network Infrastructure Layer represented by the general purpose internet infrastructure and dedicated network infrastructure.
- **Data Layer:** Data centers and computing resources/facilities.
- **Security Layer:** Hiding the data through security pipeline channel that includes: manipulating fonts, font metrics, font styles, color and their RGB values, and the x, y location to display data.

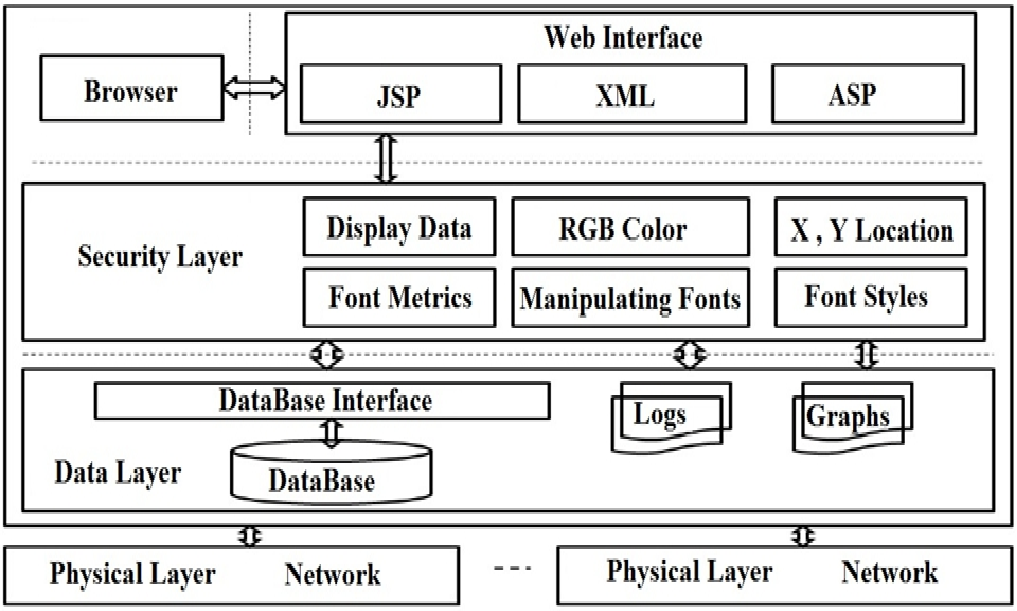

Figure 1: The Proposed Steganography Scheme Architectural Model

Figure1 above illustrates the process of concealing data in the Cloud Computing system. The process consists of two files: the **first file** is called java class. It contains all the steps, which will be programmed and implemented as designed inside this (class). The **second file** is known as Hyper Text Markup Language (HTML). The first file is embedded within the second file. The HTML file can send any number of (parameters) to the Class file. This requires implementation to show hidden data, as follows:

```
<PARAM NAME=fontVALUE=TimesNewRoman>
<PARAM NAME=Style VALUE=Bold>
<PARAM NAME=Size VALUE=14>
 <PARAM NAME=xpos VALUE=10>
<PARAM NAME=ypos VALUE=10>
<PARAM NAME=rcolor VALUE=255>
<PARAM NAME=gcolor VALUE=200>
<PARAM NAME=bcolor VALUE=0>
```

The method code is

```
private void HideData()    {
   public String font = "TimesNewRoman";
Other parameter Style,Style,Size,xpos,ypos,rcolor,gcolor and bcolor
        String fontParam = getParameter("font");
      if ((fontParam == null) || !fontParam.equals(font))  {
throw new SecurityException("Developing Secured Interoperable Cloud Computing
Services");
 } }
```

5. Conclusion

This paper discussed security problems in cloud computing systems and how they can be prevented by using protected access control to hide data. This is used to protect the data in the cloud computing system by exploiting text properties including: manipulating fonts, font metrics, font styles, color and their RGB values, and the x , y location to display data. In our future work, we will extend the proposed scheme to support encrypted data with steganography in cloud computing.

References:

[1] Demchenko, Y., Makkes, M., Strijkers, R., Ngo, C. and de Laat, C. (2013) “Intercloud Architecture Framework for Heterogeneous Multi-Provider Cloud based Infrastructure Services Provisioning”, The International Journal of Next-Generation Computing (IJNGC), 4(2), July, 2013.

[2] Sharon, I., Kumar, C., Andrew, W., and Jeevakumar, J. (2013) “A Survey on Security Threats and Vulnerabilities in Cloud Computing”, International Journal of Scientific and Engineering Research, 4(3), ISSN 2229-5518, March, 2013.

[3] Mayank, P. (2013) “Online Java Compiler Using Cloud Computing”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2(2), ISSN: 2278-3075, January, 2013.

[4] Aniruddha, S. and Chaudhari, D. (2013) ”Cloud Computing: Infrastructure as a Service”, International Journal of Inventive Engineering and Sciences (IJIES), 1(3), ISSN: 2319–9598, February 2013.

[5] Ateniese, G., Fu, K., Green, M. and Hohenberger, S. (2005) “Improved proxy re-encryption schemes with applications to secure distributed storage”, in *Proc. of NDSS’05*, 2005.

[6] Ravij, K., Nishant, S . and Sutaria, K. (2013) “Ameliorate Security Policy Using Mediated RSA and Identity Based Cryptography in Cloud Computing”, Journal of information, knowledge and research in computer engineering, 2, ISSN: 0975 – 6760, pp. 389, October, 2013.

[7] Ankur, M., Mathur, R., Jain, S. and Singh, J. (2013) “Cloud Computing Security”, International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), 1(1), ISSN 2321 – 8169, pp. 36-39, Jan, 2013.

[8] Yuri, D., Ngo, C., Makkes, X., Strijkers, R., Laat, C. (2012) “Defining Inter-Cloud Architecture for Interoperability and Integration”, University of Amsterdam, System and Network Engineering Group, Cloud Computing, France, July, 2012.

[9] Selvn, M., Subbiah, S. and Ramkumar, T. (2013) "Enhanced Survey and Proposal to secure the data in Cloud Computing Environment", International Journal of Engineering Science and Technology (IJEST), 5(1), ISSN: 0975-5462, January 2013.

[10] Steve, G. (2013) "Cloud Computing, Oxford University, England", International journal of Innovative Research in Engineering and Science, 1(1), ISSN 2319-5665, July, 2013.

[11] Malpani, G. (2013) "Cloud Computing: Key to Business Fitness", Paripex - Indian Journal of Research, 3(4), ISSN - 2250-1991, May, 2013.

[12] Singh, H. and Bansal, B. (2010) "Analysis of security issues and performance enhancement in cloud Computing", International Journal of Information Technology and Knowledge Management, 2(2), pp. 345-349, December, 2010.

[13] Khaja, S., Khamruddin, M. and Krishna, K. (2012) "An Overview of Data Security in Cloud Computing", International Journal of Advances in Computer, Electrical and Electronics Engineering, 2, ISSN: 2248-9584, December, 2012.

[14] Lavania, K., Sharma, Y. and Bakliwal, C. (2013) "A Review on Cloud Computing Model", International Journal on Recent and Innovation Trends in Computing and Communication, 1(3), ISSN 2321 – 8169, March, 2013.

[15] Ssec, I. (2004) "Cryptography, Encryption and Stenography". [online] Available at http://www.infosyssec.org/infosyssec/cry2.htm, Accessed on 23 June 2004.

[16] Johnson, N., Jajodia, F. and Steganalysis, S. (1998) "The Investigation of Hidden Information", the Proceedings of the 1998 IEEE Information Technology Conference, Syracuse, New York, USA, September 1st - 3rd, 1998.

[17] Radcliff, D. (2013) "Steganography: Hidden Data, Quick study by Computer world", [online] available at http://cirworld.com/index.php/ijdns/article/view/487, accessed on 26 October 2013.

[18] Vennice, M., Rao, T., Swapna, M., and kiran, J. (2012) "Hiding the Text Information using Stegnography", International Journal of Engineering Research and Applications (IJERA), www.ijera.com, 2(1), ISSN: 2248-9622, pp.126-131, Jan-Feb, 2012.

[19] Sharma, V. and Kumar, S. (2013) "A New Approach to Hide Text in Images Using Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, 3(4), ISSN: 2277 128X, April 2013.