Sādhanā Vol. 41, No. 11, November 2016, pp. 1289–1298
DOI 10.1007/s12046-016-0558-8

New approach for ensuring cloud computing security: using data hiding methods

MURAT YESILYURT and YILDIRAY YALMAN*

YY Image Processing Laboratory, Kocaeli, Turkey
e-mail: mr.yesilyurt@gmail.com; yildiray.yalman@gmail.com

MS received 1 April 2015; revised 11 May 2016; accepted 16 May 2016

Abstract. Cloud computing is one of the largest developments occurred in the field of information technology during recent years. This model has become more desirable for all institutions, organizations and also for personal use thanks to the storage of 'valuable information' at low costs, access to such information from anywhere in the world as well as its ease of use and low cost. In this paper, the services constituting the cloud architecture and deployment models are examined, and the main factors in the provision of security requirements of all those models as well as points to be taken into consideration are described in detail. In addition, the methods and tools considering how security, confidentiality and integrity of the information or data that forms the basis of modern technology are implemented in cloud computing architecture are examined. Finally, it is proposed in the paper that the use of data hiding methods in terms of access security in cloud computing architecture and the security of the stored data would be very effective in securing information.

Keywords. Cloud computing; access security; stored data security; data hiding.

1. Introduction

In today's global world, rapidly evolving technology and internet infrastructure require secure communications. As a natural consequence of this, the concept of "information security" has gained great importance in many areas such as banking, e-commerce, e-signature, distance learning, e-government applications, personal and corporate communications, and data storage. Information security aims to prevent access to information by third parties for whatever purpose and is of great importance for all users. In recent years, the rapid change and development experienced in the internet world has also greatly enhanced the field of information security. The main elements constituting information security are given below:

- Confidentiality: Protection of information against unauthorised access.
- Integrity: Completeness, entirety, consistency and accuracy of information.
- Accessibility: Access to information by authorised persons only when required.

In the present study, the current state of information and communication technologies and the increasing daily use of cloud computing are discussed in detail. The importance of utilising data hiding science for the information security elements mentioned above is emphasised. In this context, the paper is organised as follows.

Section 2 elaborates the security issues of cloud computing, which incorporate many innovations in the computer industry and emphasises that the concepts of information security and privacy constitute the most important elements in cloud computing. In section 3, the points to be taken into consideration regarding the security of cloud services providing users with services are examined, and the measures to be taken for ensuring this are detailed. Section 4 covers the conditions necessary to establish information security and the ISO standards and applications which constitute an important standard in this regard are described. Ensuring of cloud computing security through the use of data hiding methods has been presented in section 5 and experimental results of the proposed methods have been given in section 6. Final remarks have been presented in the "Conclusions" section.

2. Security in cloud computing

As a solution to security and privacy in cloud computing, the options may be enumerated as monitoring cloud server services, protection of data privacy, determination of the accuracy of the information, inaccessibility by third parties, protection against unwanted changes and deletions, prevention of malicious content and ensuring uninterrupted access to information [1].

Sun *et al* [2] dwelled on this point and studied security, privacy and confidence concepts in cloud computing. In

*For correspondence

this study, the security concepts containing elements such as accuracy of the information, prevention of unauthorised access, and unauthorised changes to the information are defined as closing any gaps that may occur in the system (e.g. accessibility deficits, virtualization deficits and web application deficits). Lombardi and Di Pietro [3] have focused on the advanced cloud protection system (ACPS), one of the cloud computing security models. They revealed that this system enhances the security of the nodes in cloud computing and provides a complete protection against attacks by following the local and remote users' interaction with cloud computing.

The operating system often used the PaaS platform, the virtual drive platforms and the potential of security levels related in particular to .java and .NET-based application layers (java-based google app. engine (GAE)) were examined in a study [4]. In an analysis by Cloud Security Alliance (CSA) and IEEE, which are included in the PaaS platform and constitute the most known components, it was observed that the sectors have adopted cloud computing and also that interest in cloud computing has further increased. However, along with this adoption, each service's own security issues should be handled separately [5].

Another security requirement for cloud computing is the cases which are of great importance for institutions and where access to a virtual machine is not possible, when it is necessary to replace authentication and authorisation applications for cloud computing [6]. In such a case, cloud service would be interrupted and many users would be negatively affected. Therefore, continuous availability of cloud service providers stands out as an important security issue which to be overcome for cloud computing.

3. Security of cloud computing services

As mentioned above, cloud computing provides services through three basic services (IaaS, PaaS and SaaS). These services provide the user with all infrastructure resources, application platforms and software support. Therefore, the idea of individual evaluation and examination of the platforms and the provision of individual security for each service after their differential evaluation was accepted in the provision of information security [5].

Cloud computing also provides external service providers with a service for storage areas and their presentation. The most obvious example of this is the service level agreement (SLA) which is used to enable the access of users to the applications running in the cloud and must be taken into consideration. The external servers managed by the SLA can provide a system used at the annual rate of 99.9%. However, these services may fail to provide security requirements at a desired level in terms of the principles of information confidentiality and integrity. Cloud computing users principally expect the security of all service providers to be at the same level and the related costs to be determined based on them [6].

In order to increase the security level in a cloud structure defined by SLA Bernsmed *et al* [7] have also proposed the utilisation of other service providers [8]. Furthermore, in this paper, a customer relationship management (CRM) application and a cloud unified communication application sample were presented for customer relationship management.

All these show that cloud computing offers services through its service oriented architecture (SOA) that are directly related to and integrated with each other. In such a model, each service must be dealt with individually to ensure security and privacy [9].

3.1 *IaaS and security*

This IaaS platform offers mainly basic-level services and infrastructure services. In the first gate position, the IaaS plays a role as the basic security provider of tools such as firewalls, load balancing the system by creating a "shield of protection" as if it is outside the "cloud" [10].

In the IaaS platform, the security vulnerabilities that may occur in virtualization management are less common compared to the other platforms and this process is better controlled [11]. On the other hand, the other important factor is that different techniques are applied to ensure maximum privacy and security, in addition to the virtualization applied due to the storage of data in a physical structure [12]. Due to differences between cloud service models, in order to ensure information security the service providers are required to apply different techniques. For instance, elastic compute cloud (EC2) offered by Amazon in 2010 not only ensures physical security, but also provides environmental security, virtualization security and management of the security criteria [13].

In this regard, another application which is used as the security protocol in the IaaS platform and has many benefits in providing cloud computing services is security content automation protocol (SCAP). It is emphasized that it is important to develop SCAP as a universal security standard. It has many uses in providing cloud services through applications, such as user authorisation, determination of the information security method and content control applications [14].

3.2 *PaaS and security*

The PaaS is a platform where there are applications and development tools for users within cloud computing. This platform offers storage, management, and virtual application development tools needed by the users.

The virtual machines included in the PaaS must necessarily be protected against harmful software such as malware and trojans. Data privacy protection ensures that the integrity of content in the applications developed does not deteriorate and facilitates data transfer between reliable networks. In addition, it must also ensure that the profile validation checks are performed in a complete and safe way.

Another point to take into consideration is to perform examinations at regular intervals to prevent malicious applications from penetrating the cloud architecture.

3.3 *SaaS and security*

SaaS platform is a service through which cloud computing offers software services to its users. There are a number of ready-to-use software programs for processing safely stored information.

While SaaS service provides the user with some basic functions such as authentication for safe communication, authorisation control and secure data storage, it may also connect to the users of different services. For example, to provide a variety of solutions for e-health services, electronic health records or a medical software installed on the virtual machines (EHR, electronic health record), such applications can be opened via the user interface and the HTTPS protocol [15].

In addition, many IT departments and government agencies use SaaS platforms. The most important point is the security level of the servers where the user's information is stored. The fact that highly confidential information of a State, special personal data, or a company's customer information are stored in the same servers is an issue to be extremely careful in terms of information security and privacy. Otherwise, access to confidential information by unauthorised persons will be possible. If the information accessed constitutes top secret documents or information directly belonging to government agencies. This situation will lead to legal problems or cause data hacking and espionage. For this reason, it is very important to keep information secure in the SaaS platform.

4. Information security requirements and cloud computing

'Security' will confront us as the most important factor in cloud computing architecture in the near future, where necessary applications and software will be provided and which will include many data centres. The important parameters and developments in cloud computing security and the advancements in this regard have been the main subject of many studies [13, 16, 17].

The components required for the provision of information security in the world are covered by the ISO 7498-2 standard [18]. To render information security in cloud computing as an effective solution for IT applications, innovations are introduced through changing technology. Therefore, the 27001 standard is included within the ISO 27000 standard used in this field and determines the security standards and all the requirements needed for an information security management system (ISMS) [19]. These requirements involve issues such as ISMS policies, assessment and management of possible risks, monitoring, and control of information security. Public awareness of the ISO 27001 standard will increase day-by-day. While 19,620 certificates were obtained in 2012, this number increased to 22,293 in 2013 [20].

The schematic representation illustrating the information security requirements in the case of combining cloud computing with application models and deployment models was created by Eloff *et al* [21]. According to this scheme, the features "Identification and authentication, authorisation, confidentiality, integrity, non-repudiation, availability" among the information security requirements should be examined separately in the services of each delivery model.

In Eloff's scheme, mandatory and optional requirements are shown in different cloud deployment models [21]. However, this table was created based on an old IT infrastructure and such requirements as well as the ISO 27001:2013 standard, were updated and the security level was improved. The most important of these security requirements are shown in figure 1.

- Audit: Authentication and authorisation sections are determined based on the deployment models. This requirement ensures identification of user names and passwords on the users' profiles and safe implementation of verification processes.
- Confidentiality: Information confidentiality includes the confidentiality of data stored in databases, the confidentiality of user profiles and authorisation, and all other information of the user.
- Integrity: Data integrity (robustness, accuracy, integrity, etc) is the important requirement for each platform in cloud computing and is one of the basic requirements of the security information to be provided.
- Availability: In addition to the delivery model, availability is emerging as a key factor in the decision-cloud model. The availability level is of great importance between cloud computing servers and users. Therefore, ISO encourages a complete fulfilment of information security requirements.

5. Proposed approach: use of data hiding methods in cloud computing security

Cloud computing is a model with extreme limits that are capable of integration with each other. To access the numerous data sets in different capacities within such a model and maintaining the integrity of such data sets is regarded as the most important security requirements. The main point emphasized in this paper is security of users'

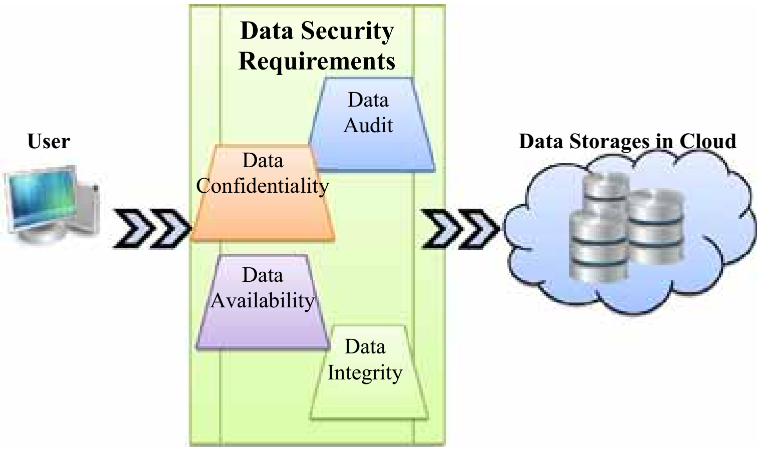

Figure 1. Information security requirements of cloud computing.

information. Access with audit and data integrity demonstrates an approach that successfully allows this. Among the most important security features are inaccessibility of personal or corporate data stored in cloud computing by unauthorised persons, fully ensuring the integrity of the data i.e. full protection of information, preventing any change, division, deletion, replacement, and inhibiting any unauthorised backup or update. Therefore, this paper focuses on information access security and an active use of data hiding methods to maintain the integrity of the information being accessed.

Another important point in cloud computing is the use of mobile devices for access (tablet PC, smart phone, etc.). Thanks to their ease of use, the use of mobile devices is increasing day by day and provide easy access to all over the world. Thus, data hiding techniques must be used for connections between mobile devices and cloud computing as a factor to improve security too.

Data hiding methods have always been a factor in increasing the existing security for all applications in which they are used. Thus, security is ensured against possible attacks. Likewise, a robust method against any attack can be created by hiding the user name and password used for access to data by the method of watermarking in any media (text, images, videos, etc.) to render it resistant against attacks. As the importance of information security increases, studies on this subject have gained momentum and research conducted within the scope of data hiding science have contributed to the solution of security problems. Thus, the overall security level of data has been increased, and an improved security level may also be ensured for private data. In other words, data hiding techniques aim to protect data against malicious users and attacks in a secure way.

Data hiding techniques can be divided into three main categories: steganography, watermarking and cryptology. Steganography comprises the method of hiding data in a multimedia tool (images, videos, etc.) to prevent it from being recognised by third parties. Watermarking is widely used for unauthorised copying and copyright issues in general, and the hidden data is expected to be robust against attacks. Third parties are aware that the data are stored through an invisible watermarking method; however, since this method is robust against any external intervention aimed at accessing this data, the data is preserved. Cryptology involves converting the information using an encryption algorithm. The data will be prevented from being read by unauthorised users. However, although the related data is not read by the third parties, there is risk of it being removed or replaced. For these reasons, benefiting equally from these three techniques that have many areas of use in the literature, cloud computing is expected to achieve success in the security and confidentiality of information and in the solution of the associated problems.

There are some basic features to be supplied for the use of data hiding techniques. These features are capacity, robustness and security, as shown in figure 2. Capacity is expressed as the amount of data that can be hidden. Robustness and security represent, respectively, the resistance of hidden data to attacks and the set of measures preventing the data from being obtained by third parties. In the case, where one of these requirements is missing, some vulnerability occurs in the method to be employed and this leads to weaknesses in information security. Figure 2 emphasises the phases of the data hiding methods aimed at ensuring security in cloud computing.

In addition to these valuable methods mentioned above, encryption and data hiding methods can be easily used to increase the security level altogether.

5.1 *Use of data hiding in access security*

Given that data storage units within cloud computing receive data in various sizes and types from many different regions and via many different networks, increasing the access security through data hiding methods will gain more importance. The use of the data hiding method is very important for both to ensure protection against various

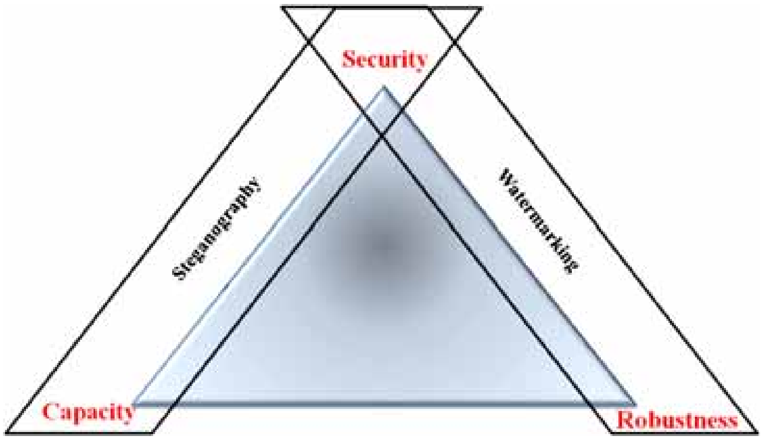

Figure 2. Basic requirements triangle in data hiding.

possible attacks during access by users, to prevent any vulnerabilities in the identity profiles of users and also to ensure disclosure of such data only to authorised persons by maintaining the confidentiality and integrity of information.

Some researchers have conducted studies on this issue and they have supported our prediction by using the methods developed [22, 23]. In some studies, however, in addition to the use of a new encryption method, the use of trusted third parties (TTP) software is also proposed to fix some of the security vulnerabilities in cloud computing and to protect the CIA (confidentiality, integrity and authentication) of data at the same time [24]. The vulnerabilities can be in all software (closed or open source code). On the other hand, TTP software with an open source code is likely to have more unknown vulnerabilities and these are likely to lead to weaknesses in the security. Even if encryption is a secure method, while ensuring access in the case of any attack to the TTP employed, a vulnerability will arise in the system and this might lead to some problems in information confidentiality and integrity. Therefore, there is no need to use any other TTP software for access security.

As stated above, two of the most preferred data hiding methods are digital watermarking and encryption. The most important phase in which the use of such data hiding methods are required is the phase of access to information by the user, namely the first phase. This phase constitutes the access phase called 'User Audit' in which identification, authorisation, and authentication steps are taken (figure 3).

L is the length of the audit (a) information to be embedded and $1 \leq j \leq L$. "a_j" is "j." of bits a information to be embedded in cover object. a and key information (key) are subjected to an encryption function as described in Eq. 2 and "$\mathcal{E}a$" information is obtained. Here, the "f" function, both key and a_j is also a function of the cover object. The "$\mathcal{E}a$" information is hidden in the carrier (i.e. an image) by data hiding function $\mathcal{H}$ (Eq. 3) and covered data (I_C) is obtained. The $\mathcal{H}$ function algorithm mentioned herein can, according to the data hiding method, be varied (figure 3).

$$\mathcal{E}a = f\left(a_j, key_j\right) \tag{1}$$

$$I_C = \mathcal{H}(I, \mathcal{E}a). \tag{2}$$

In this section, which can also be called the first gate, increasing the security level will also remove many security weaknesses that may occur during the transition to the other layers. Verifying the identity profile of the user, using the access and creating an authorisation model for such user is an important security step. It is also of great importance to prevent any penetration in to private information by obtaining the user name and password without permission. This constitutes the classic authentication elements and obstructs any violations of data confidentiality, data integrity and authentication rights CIA. To accomplish this, using a combination of invisible digital watermarking and symmetric/asymmetric encryption algorithms (RSA, AES, etc.) will secure all necessary information to access the user data.

Thanks to this approach, a secure user access will be ensured by hiding the user's identity profile information (user audit) using a watermarking method identified by a cover file after its encryption as well as resulting in a new covered audit. Since a safe area will emerge through this resulting "covered audit", access security will be provided against external attacks that could be committed during access to the storage area within the cloud.

5.2 *Use of data hiding in the security of stored data*

Another section in which top-level security must be ensured is the section where the servers in which the data are stored are available. In the present study, another security approach is recommended. This section is located within the public cloud and constitutes the most intense platform in terms of the number of users. It is known that using data hiding methods to ensure security of private information stored in the database, both on the server where they are

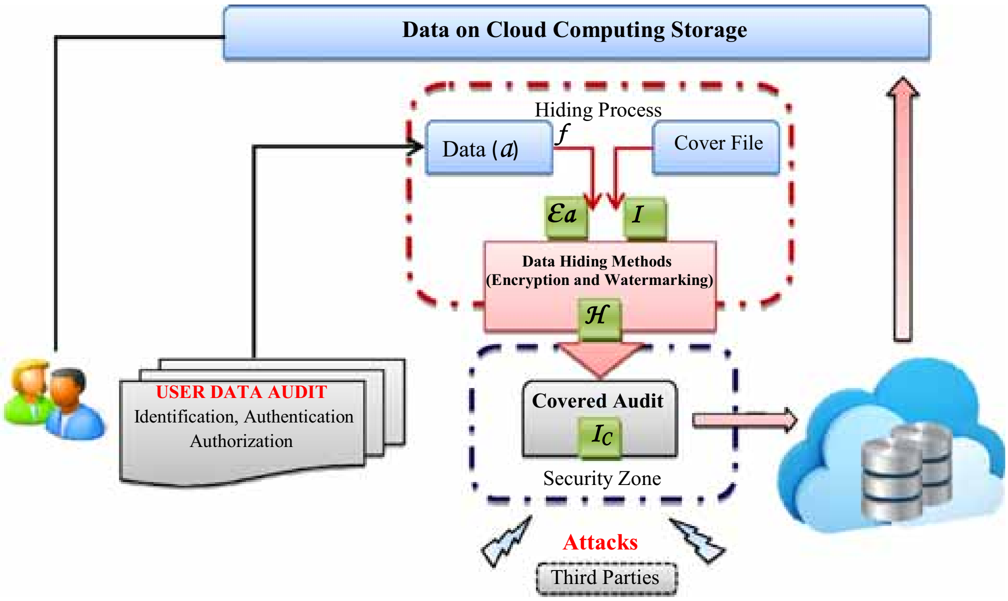
Data on Cloud Computing Storage
Hiding Process
f
Data (a)
Cover File
Ɛa
I
Data Hiding Methods (Encryption and Watermarking)
ℋ
USER DATA AUDIT
Identification, Authentication Authorization
Covered Audit
I_C
Security Zone
Attacks
Third Parties

Figure 3. Proposed approach: use of data hiding methods for access security.

kept and during the period until it reaches the user from the server, is of critical importance.

The security zone created by data hiding methods to be applied to the data stored in the databases of cloud computing, the algorithm to extract the desired information whenever needed, and presentation of such information to the user is shown in figure 4.

Data hiding methods can ensure data confidentiality and integrity against both the unlimited power of cloud service providers on data and any problems that can occur in the connection between the virtual machines of the cloud and the users' IT systems. Combined use of encryption and watermarking methods can definitely improve the security level. This will be possible to ensure user information in the data storage is accessed only by authorised persons, through public or private keys generated with symmetric and asymmetric encryption algorithms, which are the most commonly used among encryption methods. Some methods are available to increase the security of the stored data, such as multiple encryption of data, generation of two different keys, and use of a different encryption method each time or individual encryption of the data through dissection. In this regard, there are some studies conducted through different encryption tables and algorithms in the literature [25–28].

L is the length of the stored data (S) information to be embedded and $1 \leq j \leq L$. "S_j" is "j" of Bits a information to be embedded in cover object. S and key information (key) are subjected to an encryption function as described in Eq. (5). and "$\mathcal{E}$s" information is obtained. Here, the "f" function, both key and S_j is also a function of the cover object. The "$\mathcal{E}_S$" information is hidden in the carrier (i.e. an image) by data hiding function $\mathcal{H}$ (Eq. 3.) and covered data (I_{SC}) is obtained. The $\mathcal{H}$ function algorithm mentioned herein can, according to the data hiding method, be varied (figure 4).

$$\mathcal{E}s = f\left(\mathcal{S}_j, key_j\right) \tag{3}$$

$$I_{SC} = \mathcal{H}(I, \mathcal{E}s). \tag{4}$$

During the process of data extraction, the embedded encrypted data is removed from cover object(s) and extracted information is decrypted by using key(s).

On the other hand, only the portion of the data where processing will be carried out must be downloaded during the access to information, for information security. If the data is encrypted or stigmatized, only the security measure on the data to be processed must be removed and following the change, only the processed part must be re-encoded without the need for re-encryption of all the uploaded data. A study which supports this was conducted by Khan *et al* [29] in the form of a coding-based and sharable encryption algorithm. However, it should be noted that, in the case that the stored data is multimedia data (image, video, audio, etc.), the security must be ensured by means of a digital watermarking method and the areas where connection speed and bandwidth are sufficient to provide access to such information must be preferred. Thus, the data integrity will remain undamaged during access. Otherwise, when high-capacity multimedia data is downloaded to a mobile device, problems may occur depending on the packet loss and this will weaken the security and integrity of the information. In addition, watermarking methods both protect the user's copyright and also become very important in the protection of data against unauthorised reproduction.

Using invisible watermarking methods in cloud computing will also be very useful. In this method, since the colour

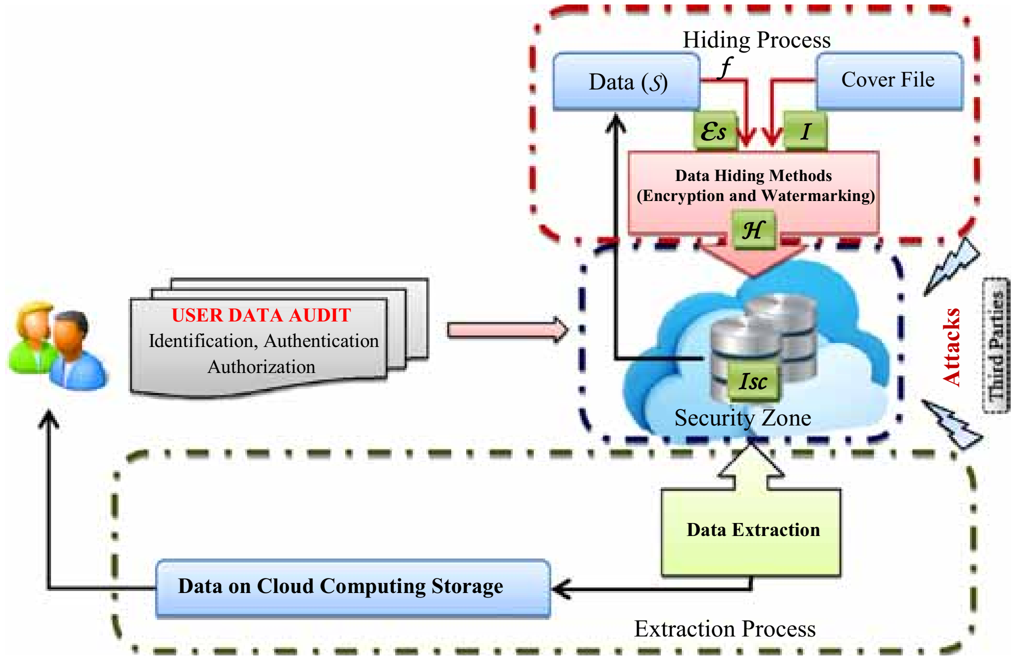

Figure 4. The proposed approach: use of data hiding methods for the security of stored data.

structure in multimedia products (RGB, YUV, YCbCr, etc.) is of great importance, watermarking performed using colour and pixel values of digital images or frames stored in virtual machines within the cloud (any digital signature or knowledge of a user may also be hidden there) will greatly contribute to the provision of information integrity and its verification [30, 31]. Thanks to this method, which may be used for all multimedia tools, resource consumption and costs will also be greatly reduced [32, 33]. As in all other methods, various open source-coded third party software or ready-to-use codes are employed in the watermarking and the results are analysed through another ready-to-use application [34]. However, since the use of any external application may lead to security vulnerabilities, such applications should be avoided as far as possible. It is clear that if data hiding methods are efficiently used there will be no need to use external applications.

Figure 5 shows the implementation scheme recommended for security practices. User audit information is embedded into cover image by data hiding methods. So the user's confidential data is on guarantee, access security is ensured. In the same way, data hiding methods are used for information in the data storage. Data security can be ensured those information into a cover image.

6. Experimental results: assessment of the proposed security approaches

This section presents the survey results obtained to evaluate the proposed approaches (use of data hiding in the security of the stored data and in access security) in terms of security contributions and validity. In this work, the classical least significant bit (LSB) technique has been used for data hiding processes. The survey was performed with 50 senior engineers during demo applications of the presented approaches in Turkey. As seen in table 1, engineers were asked seven questions graded using a five-point scale (excellent = 5, very good = 4, good = 3, fair = 2, very poor = 1) similar to a Likert scale. The results are shown in figure 6.

The first four questions were about application-based answers. The average number of positive answers given (excellent, very good and good) was 45, equal to 90% of the population (figure 6). This result shows that the proposed cloud computing security approaches are useful as information security tools. It can be seen that only 20 engineers gave the most positive (excellent) answers for the fourth question, which was about working and response time of the interface. As users have to wait for a few seconds to get the embedding results, this caused some displeasure. One of the main reasons for this situation is the communication delay between the client and the server. The fifth and sixth questions asked are for feedback and technical opinions about the approaches. The average number of positive answers (excellent, very good and good) given to these questions by engineers was 47, equal to 94% of the population.

The seventh question was about overall success. According to results, 45 engineers or 90% of the population thought that the proposed approaches are useful and successful for ensuring cloud computing security. Considering the proposed and realised demo applications mentioned above, some advantages are listed below:

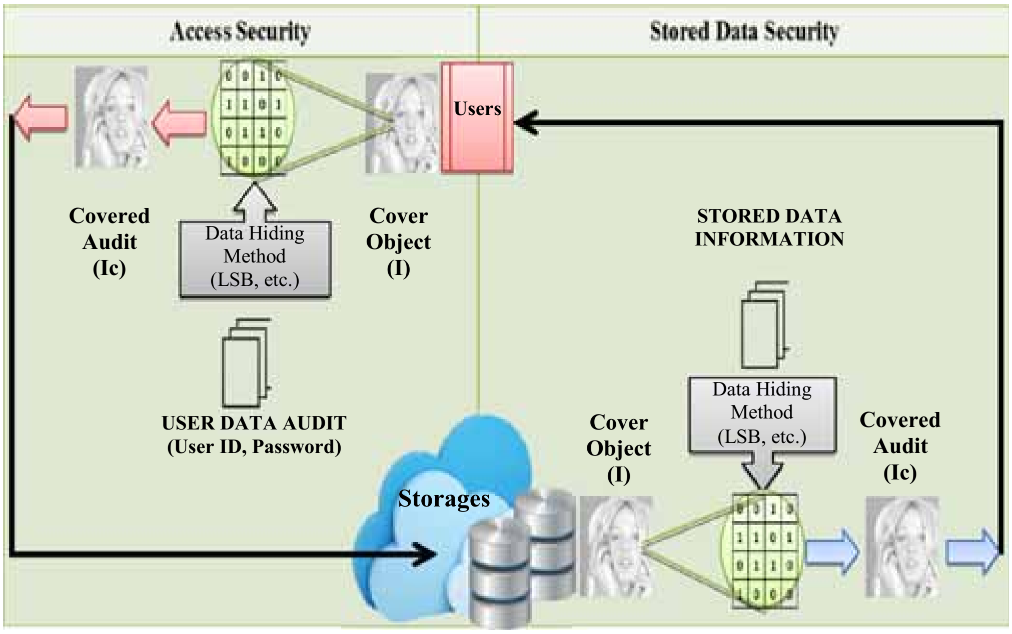

Figure 5. Access and stored data security implementation scheme.

Table 1. The survey questions.

Number	Question
1	Increase of security level
2	Easy and efficiency of usage
3	Flexibility and freedom for users
4	Working and response time of the demo applications
5	Intelligibility of the proposed approaches versus existing methods
6	Contribution of the proposed approaches to assist security needs
7	Overall success of the proposed security approaches

- The approaches have a user friendly concept.
- It is an extremely easy, fast and economical way of ensuring cloud-computing security.
- They can be easily designed for servers which have critical file savings by using more complex data hiding techniques.
- The proposed approaches can be developed easily by adding new features.
- There is no identical or similar security system that performs the work done by the system developed in the literature.

The LSB data hiding method is the process of adjusting the LSB pixels of a cover image. It is a simple method for hiding message into the image. The LSB insertion varies according to the number of bits in an image. For an 8 bit image, the LSB i.e., the 8th bit of each byte of the cover image is changed to the bit of secret message. The colours of each component like RGB (red, green and blue) are changed when colour image is used. The LSB method is effective in using BMP images since the compression in BMP is lossless. There are many methods available for hiding the data within an image: one of the simple LSB hiding approaches is "optimum pixel adjustment (OPA) procedure" [35]. The simple algorithm for OPA explains the procedure of hiding the sample text in an image:

Step 1: A few least significant bits (LSB) are substituted with in data to be hidden.
Step 2: The pixels are arranged in a manner of placing the hidden bits before the pixel of each cover image to minimize the errors.
Step 3: Let n LSBs be substituted in each pixel.
Step 4: Let $d =$ decimal value of the pixel after the substitution
$d1 =$ decimal value of last n bits of the pixel.
$d2 =$ decimal value of n bits hidden in that pixel.
Step 5: if $(d1 \sim d2) <= (2n)/2$ then no adjustment is made in that pixel.
else
Step 6: if $(d1 < d2)$ $d = d - 2^n$
if $(d1 > d2)$ $d = d + 2^n$.

This 'd' is converted to binary and written back to pixel. This method of substitution is simple and easy to retrieve the data and the image quality better so that it provides good security.

The LSB-based OPA procedure explained above has been used for implementations. These implemantations allowed that access security and stored data security is ensured in an effective way. However, the storage and transmission times, up to critical data (bit) × 1 byte

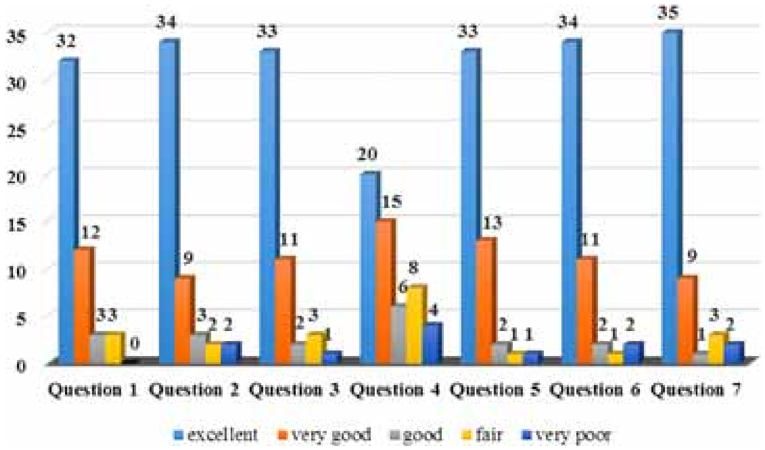

Figure 6. Assessment results.

Table 2. Detection of data hiding results.

Covered image[a] (512 × 512)	Stegdetect results 0.1 bpp	0.2 bpp	0.3 bpp
Ic_1	–	–	–
Ic_2	–	–	–
Ic_3	–	–	–

– Indicates that the result is negative.

[a] All covered images have coded by LSB-based OPA procedure.

additional space has been needed. In addition, Matlab® R2013b platform has been used for data hiding and image database creation.

In addition, robustness is examined using an application named as Stegdetect for the proposed access security approach [36]. The output from the StegDetect (outguess) lists either the data hiding systems found in cover images or "negative" if no steganographic content could be sensed. Final outcomes for the three covered well-known gray-scale images (Ic_1 (Tiffany), Ic_2 (F16), Ic_3 (Peppers)) are all acquired as negative (table 2). Thus, these result also verify the use of the proposed approaches and their reliability.

7. Conclusions

Cloud computing is one of the largest innovations provided by internet technology. This model, which is addressed to all users in the world and provides access to information in each geographical area and environment, requires top-level security for any information, applications and software. To this end, it is very important to use security-enhancing methods. One of the most important things to ensure is that the methods of data hiding used cover an extremely wide area. These methods fix an important vulnerability, thanks to both the security they provide during the access to information and the robustness they will provide against any attacks on the integrity and confidentiality of the data stored in the cloud.

The combined use of encryption and watermarking among the data hiding methods are of great importance, both in the access phase and in terms of the provision of security of the information contained in the information storage centres. In this study, the vital importance of the combined use of encryption and watermarking methods in the database are described in detail. Whatever the data capacity and the content, data hiding methods should be used as a factor to enhance the security of cloud computing services as the utlizationuse is increasing day-by-day and access is often with mobile devices. All of these studies indicate that the security level will increase through the application of encryption and watermarking methods to the data stored in the cloud and, thus, the user will be provided with a more reliable service. Experimental results show that the proposed approaches are secure enough.

Acknowledgements

The authors would like to thank the anonymous reviewers and the associated editor for their valuable comments and suggestions for better presentation of this work.

References

[1] Avizienis A, Laprie J C, Randell B and Landwehr C 2004 Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Depend. Secure Comput.* 1(1): 11–33

[2] Sun D, Chang G, Sun L and Wang X 2011 Surveying and analyzing security, privacy and trust issues in cloud computing environments. *Proc. Eng.* 15: 2852–2856

[3] Lombardi F and Di Pietro R 2011 Secure virtualization for cloud computing. *J. Netw. Comput. Appl.* 34: 1113–1122

[4] Rodero-Merino L, Vaquero L, Caron E, Muresan A and Desprez F 2012 Building safe PaaS clouds: A survey on security in multitenant software platforms. *Comput. Security* 31: 96–108

[5] Kanduriki B R, Paturi V R and Rakshit A 2009 Cloud security issues. *IEEE International Conference on Services Computing*, pp. 517–520

[6] Rong C, Nguyen S T and Jaatun M G 2013 Beyond lightning: A survey on security challenges in cloud computing. *Comput. Electr. Eng.* 39: 47–54

[7] Bernsmed K, Jaatun M G, Meland P H and Undheim A 2011 Security SLAs for federated cloud services. *Sixth International Conference on Availability, Reliability and Security (ARES)*, pp. 202–209

[8] Karin B, Gilje J M and Astrid U 2011 Security in service level agreements for cloud computing. *1st International Conference on Cloud Computing and Services Science (CLOSER 2011)*

[9] National Institute of Standards and Technology 2009 *The NIST definition of cloud computing*, Information Technology Laboratory

[10] Kuyoro S O, Ibikunle F and Awodele O 2011 Cloud computing security issues challenges. *Int. J. Comput. Netw. (IJCN)* 3(5): 247–255

[11] Gajek S, Liao L and Schwenk J 2007 Breaking and fixing the inline approach. *ACM Workshop on Secure Web Services*, pp. 37–43

[12] Descher M, Masser P, Feilhauer T, Tjoa A M and Huemer D 2009 Retaining data control to the client in infrastructure clouds. *IEEE International Conference on Availability, Reliability and Security*, pp. 9–16

[13] Subashinin S and Kavitha V 2011 A survey on security issues in service delivery models of cloud computing. *J. Netw. Comput. Appl.* 34: 1–11

[14] Harauz J, Kaufman L M and Potter B 2009 Data security in the world of cloud computing. *IEEE Computer and Reliability Societies*, pp. 61–64

[15] Berndt R-D, Takenga M C, Kuehn S, Preik P, Sommer G and Berndt S 2012 SaaS-platform for mobile health applications. *9th International Multi-Conference on Systems, Signals and Devices (SSD)*, pp. 1–4

[16] Rasheed H 2014 Data and infrastructure security auditing in cloud computing environments. *Int. J. Inform. Manag.* 34: 364–368

[17] Yunchuan S, Junsheng Z, Yongping X and Guangyu Z 2014 Data security and privacy in cloud computing. *Int. J. Distrib. Sensor Netw.* 2014: 1–9

[18] ISO, I.S. 7498-2 1989 Information processing systems open systems interconnection basic reference model. Part 2: Security Architecture, ISO Geneva, Switzerland

[19] ISO/IEC 2009 Information technology—Security techniques—Information security management systems—Overview and Vocabulary. ISO/IEC 27000, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

[20] ISO Web Page: https://www.iso.org/iso/iso_survey_executive-summary.pdf

[21] Eloff J H P, Eloff M M, Dlamini M T and Zielinski M P 2009 Internet of people, things and services—the convergence of security, trust and privacy. *3rd CompanionAble Workshop—IoPTS*, Novotel Brussels, Brussels, pp. 8

[22] Boopathy D and Sundaresan M 2014 Data encryption framework model with watermark security for data storage in public cloud model. *International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 903–907

[23] Sudha M and Monica M 2012 Enhanced security framework to ensure data security in cloud computing using cryptography. *Adv. Comput. Sci. Appl.* 1(1): 32–37

[24] Zissis D and Lekkas D 2012 Addressing cloud computing security issues. *Future Generat. Comput. Syst.* 28: 583–592

[25] Arora R and Parashar A 2013 Secure user data in cloud computing using encryption algorithms. *Int. J. Eng. Res. Appl.* 3(4): 1922–1926.

[26] Huang K and Tso R 2012 A commutative encryption scheme based on ElGamal encryption. *IEEE 3rd International Conference on Information Security and Intelligent Control (ISIC)*, pp. 156–159

[27] Kaur A and Bhardwaj M 2012 Hybrid encryption for cloud database security. *J. Eng. Sci. Technol.* 2: 737–741.

[28] Zhao G, Rong C, Li J, Zhang F and Tang Y 2010 Trusted data sharing over untrusted cloud storage providers. *IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom)*, pp. 97–103

[29] Khan A N, Kiah M L, Khan S U, Madani S A and Khan A R 2013 A study of incremental cryptography for security schemes in mobile cloud computing environments. *IEEE Symposium on Wireless Technology and Applications (ISWTA)*, pp. 62–67

[30] Yesilyurt M, Yalman, Y and Ozcerit A T 2013 A new DCT Based watermarking method using luminance component. *Electron. Electr. Eng.* 19(4): 47–52

[31] Yesilyurt M, Yalman Y and Ozcerit A T 2015 A robust watermarking method for Mpeg-4 based on Kurtosis. *Comput. J.* 58(7): 1645–1655

[32] Ren Y, Xu J, Wang J, Fang L and Kim J 2014 Watermark-based provable data possession for multimedia file cloud storage. *Adv. Sci. Technol. Lett.* 48: 103–107

[33] Singh N and Singh S 2013 The amalgamation of digital watermarking & cloud watermarking for security enhancement in cloud computing. *Int. J. Comput. Sci. Mobile Comput. (IJCSMC)* 2(4): 333–339

[34] Lin C H, Lee C Y and Chien S P 2013 Digital video watermarking on cloud computing environments. *The Second International Conference on Cyber Security, Cyber Peace fare and Digital Forensic (CyberSec2013)*, pp. 49–53

[35] Amirthanjan R, Akila R and Deepikachowdavarapu P 2010 A comparative analysisof image steganography. *Int. J. Comput. Appl.* 2(3): 2–10.

[36] OutGuess Steganography Detection Tool [Online]. Available: http://www.outguess.org/detection.php