Enhancing Cloud Computing Security using Cryptography & Steganography

Dheyab Salman Ibrahim
alnedawy69@gmail.com

Computer Science Dept. / College of Science / University of Diyala.

Abstract:

The large challenge of data stored in “cloud computing“ is confidence and security since the sensitive data saved into data centers in cloud. These critical data may be accessed, retrieved, or edited by unauthorized person(s) or machine(s). In addition, managing, organization of sensitive data may not be secure. Therefore, the security of data is highly interesting. To increase the security of data in data centers of cloud, we have introduced scheme to ensure data security in ‘cloud computing’ by encoding secret data using two levels of encryption are DES & RSA algorithms. And then to enhancing the security we use LSB algorithm to hide these encrypted data inside edges of color images which is called steganography. The fundamental objective of this paper is to avoid data access by opponent users. This scheme hiding encrypted secret data within images and store these encrypted secret data at the data centers of cloud and retrieves data from it when it is wanted.

Keywords: Cloud Computing, Cryptography, DES, RSA, Steganography.
المستخلص

الأمن البيانات المخزونة في السحابة تمثل التحدي الأكبر بالنسبة لمزودي الخدمة والزبونان معاً وذلك بسبب ضعف السياسة الأمنية وجودة الثغرات التي يستغلها الغير مخولين للوصول إلى البيانات لقراءتها أو تعديلها ... الخ. لذلك ظهرت أهمية زيادة أمن المعلومات المتواجدة في مراكز خزن البيانات في الحوسبة السحابية. في هذه الورقة البحثية تم زيادة الأمنية من خلال بناء نظام برمجي يقوم بتشهيّر ثم إخفاء المعلومات الحساسة في صور قبل إرسالها إلى مركز خزن البيانات في الحوسبة السحابية وبالإمكان استرجاعها فقط من قبل الشخص المخول. إن الهدف الأساسي للنظام هو منع الخصم من الوصول إلى البيانات المخزونة في مركز حفظ البيانات في الحوسبة الحاسوبية.

الكلمات المفتاحية: الحوسبة السحابية، RSA ، DES، الكتابة المخفية.

1. INTRODUCTION
The term 'cloud' refers to a network or internet. Cloud Computing refers to manipulating, configuring and accessing the application online. It offers online, data storage, infrastructure, and applications [1].

'Cloud Computing' is defined as a model for enabling convenient, ubiquitous, cheapest access to shared resources (such as servers, networks, storage devices, and services) that can be easily management with minimal effort[2].

Cloud Computing technology is a collection of services on internet. You are use cloud when you store your text, images online instead of your hard drive on computer or when you use e-mail. The big benefits of cloud are minimal cost. It is the combination of computing and services. It believes in
anything –anywhere concept and provides services through internet at single browser [3].

Common benefit of cloud computing is storing; that users can store large amount of data in “Data Storage Centers” of Cloud. "Cloud Computing" model permits to delivery of computing resources over the Internet and allows access to resources, data, and information from anyplace.

Data Storage in "cloud" is an important topic because whole data / information be located within connected resources. The resources allows the data / information to be retrieved by virtual machines. Cloud architecture includes several elements can be listed:

1. Data– It the collection of facts that may be benefit may not.
2. Storage– It is data center that it is saving information and allows access, update and controlling purpose.
3. Client– It include different devices like Smart Phone, I–Phone, Computers, laptops etc.
4. Application– it include programs which are required to execute the task.

Component architecture of cloud computing is shown in figure 1.
The major cloud service providers are significantly investing in their infrastructure and in acquiring customers, big players list include: Google(Gmail), Microsoft (Azore), Amazon(Amazon web services), Cisco(web Ex)[4].

Cloud Computing can much improve the availability of IT resources and owns many advantages over the computing techniques[5]. Cloud Computing moves the application software and data bases to large data centers, where the management of data and services may be not fully trustworthy; this unique attribute poses many new security challenges[6].

In some cases, a person required to store data on remote cloud servers. These gives three sensitive states: transmission of personal sensitive data to the cloud servers, transmission of data from the cloud server to clients computers, and the storage of personal data in cloud. These states are severely prone to security breach that makes the research within security aspects of cloud practice imperative one[7].
Now days, the computer technology is changed. The computer power, storage, and networking technologies are changed a lot [8]. Cloud help to reduce hardware, maintain and installation cost [9]. The major advantage of the “cloud computing” is cost saving. Cloud Computing environment provides two functions:

a. Computing – customers of cloud services can access to their data and finish their tasks by connect to internet.

b. Storage – cloud computing is represent as a large pool.

Benefits of cloud storage are easy access means to your knowledge anyplace, anytime, scalability, resilience, cost efficiency, and high reliability of data. Because these benefits each organization is moving its data to the cloud. So there is a need to protect that data against unauthorized access, modification, denial of services, etc.[10].

Data Security is a main element of services in “cloud computing”. Clients do not use cloud computing tools since the vulnerabilities of security control policy. Cloud security or network security is a not absolute. All security is relative. Security is a balancing act that requires the deployment of “proportionate defenses”. The defenses that are deployed or implemented should be proportionate to the threat[11].
Data stored in "cloud" means user uses the computer to connect to the database by using a web service, user can upload / download his information with help the cloud provider shown figure(2).

Clients of cloud access cloud services through internet by use a web browser. Services do not need to buy any software to get the benefits of software. Example of ‘cloud computing’ is yahoo email, Gmail, Hot mail, etc. [12]. Could computing has several advantages listed below [13].

a. One can access application as utilities, over the Internet.
b. Manipulate and configure the application online at any time.
c. Reduce the cost and complexity of owning, computers and networks.
d. Flexible use.
e. Scalability.
f. Reliability.
Cloud Computing Model is composed of three service models shown in Figure (3).

1. **Software – as – a – Service (SaaS)** - SaaS is software that is owned, delivered, and managed remotely by one or more providers.

2. **Platform – as – a – Service (PaaS)** - In PaaS, an operating system, hardware, and network are provided, and the customer installs or develops its own software and application.

3. **Infrastructure – as – a – Service (IaaS)** - IaaS provides access to main resources such as physical machines. IaaS provides the user the capability to processing, storage, networks, and other main computing resources [14].

![Cloud Service delivery model](image-url)
Cloud Computing Model is composed of four deployment models are:

a. Public Cloud: allows systems and services to be easily accessible to the general public. Examples, e-mail services.

b. Private Cloud: allows systems and services to be accessible within an Organization. It has increased security because of its private nature.

c. Community Cloud: allows systems and services to be accessible by group of organizations.

d. Hybrid Cloud: the hybrid cloud is mixture of public and private cloud.

General example of cloud services is Google apps, provided by Google and Microsoft SharePoint [15]. Famous companies have been provided service on the internet such as) [16]:

1. Microsoft (http://azure.microsoft.com).

2. Amazon (http://aws.amazon.com)

3. Google (http://cloud.google.com.)

There are many factors supporting cloud computing like: virtualization process, distributed storage, fast and inexpensive server, etc.[17].

Organization. The rest of the paper is organized as follows: In Section 2 we present some related works. In Section 3, we present the effects of security factor in cloud computing. Then, we explain use cryptography in cloud In Section 4. In section 5,
we defined Steganography methods. We discuss proposed system in section 6. Finally, we displayed results in Section 7. In section 8, discussed the Conclusion.

In this paper, we propose a good scheme that effective for encrypted sensitive data using DES algorithm and RSA algorithm, then hiding these cipher data in edges of color images by using steganography techniques, to ensure the security of data and information when it is residing in data storage center in cloud computing.

2. RELATED WORK

- Brian Hay et. Al [18] have focused on data authentication, data integrity, querying and outsourcing the encrypted data. Their research says that, the risks can arise at operational trust modes, resource sharing, new attack strategies. In operational trust modes, the encrypted communication channels are used for cloud storage and do the computation on encrypted data which is called as holomorphic encryption [19].
- Pallav Sharma et.[20]; suggested a solution for data security problem by combining RSA algorithms with the other Symmetric Key Cryptographic algorithms. This hybrid approach made the encryption and decryption process stronger. RSA algorithm with 1024 bit key used with a block cipher algorithm provided more complex encryption method.
- RSA and Advanced Encryption Standard (AES) algorithms.[21] are used as an integrated approach where data was encrypted with AES and private key can be encrypted with RSA algorithm. This lead to the increase in performance and compared with other techniques. The parameters like
throughput, response time, overheads etc., were used as a performance measure. There exist many variants of RSA. One among them is Multi-prime RSA.

- Nasrin Khanezaei et. al.[22] used a combination of asymmetric and symmetric encryption techniques (i.e., RSA and AES encryption methods) to achieve the assurances of cloud data security.

3. SECURITY ISSUES IN CLOUD COMPUTING

Most of the data travel over the internet and it becomes difficult to make data secure[23]. “Cloud “ can save an Organization’s time and money, but trusting the system is more important because the real asset of any organization is the data which they share in cloud to use the needed services by putting it in data base through an application[16]. The major issues in cloud computing is the protection security and it reduce the growth of the cloud computing[24].

One of the critical threats facing cloud users is the unauthorized access by the insiders(cloud administers) or the justification of location where the cloud providers operating[25]. Challenges are the most significant of security and privacy are ensuring authorized access to user data and both Cloud Provider and its Customer should share responsibility for privacy and security [4]. Types of threat related with cloud such as [26]:

1. Information (data) may be attacked by an opponent person.
2. Information (Data) can be altered by third party though transmitting the data. There are two basic types of attacks:
a. Active attacks: the data integrity is broken, the data can be modified by the third party and it sent back to the user.

b. Passive attacks: the data is confidentially is broken, the third party only can access your data but cannot do any modification in the data[8].

Through the access to the data and computing, the consumers do not know where data are kept and which machines achieve the computing jobs. Data security are main factors for customer's trust.

There are particular areas of the cloud shown figure (4)[27].

1. Security of data at rest.
2. Security of data in transit.
3. Authentication of user / applications /processes.
4. Robust separation between data to different customers.
5. Cloud legal and regulatory issues.

Fig. 4: Areas of Cloud Computing
The threats to the cloud service and data are authentication, inappropriate use of system, eavesdropping, network intrusion, denial of service attacks, and session hijacking[28]. Although Cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human’s lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception [29].

Once the client host data to the cloud there should be some guarantee that access to that data. Will only be limited to the authorized access. The cloud seeker should be assured that data hosted on the cloud will be confidential [30].

4. CRYPTOGRAPHY

Employers normally want to keep, send or get data in safe. Common way to do this is to convert the data into a different forms. Information can be known only the one who can convert it to its original form. This process is named as Encryption. Encryption used to protect secret data on communication network by using cryptographic algorithms. Cryptographic Algorithms divided into two classes are:

1. Symmetric–key algorithms that use the same key for encryption and decryption Such as DES(digital encryption standard) and AES(Advanced encryption standard ).
2. Asymmetric-key algorithms (also called public-key cryptography) that use two keys one for encryption and the other for decryption such as RSA(ravest–shamir–Addeman). RSA is one good method use public-key encryption.

There are a number of existing techniques used to implement security in cloud storage. Some of the existing encryption algorithms which were implemented in research work are as follows:

1. Data Encryption Standard (DES) Algorithm: The Data Encryption Standard (DES) is a symmetric-key block cipher. At the encryption process, DES takes a 64-bit plaintext and creates a 64-bit cipher text, at the decryption process, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm as shown in figure 5.
DES performs an initial permutation on the entire 64 bit block of data. It is then split into two, 32 bit sub-blocks, L0 and R0 which are then passed into what is known as Festal rounds [10]. Each of the rounds are identical and the effects of increasing their number is twofold – the algorithms security is increased and its temporal efficiency decreased. At the end of the 16th round, the 32 bit L15 and R15 output quantities are swapped to create what is known as the pre-output. This [R15, L15] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit cipher text. The function f is made up of four sections:
a. Expansion P–box

b. A whitener (that adds key)

c. A group of S–boxes

A straight P–box.d

2. RSA Algorithm: The RSA algorithm named after Ron Rivest, Adi Shamir, and Leonard Adleman. It is based on a property of positive integers. RSA uses modular exponential for encryption and decryption. RSA is an algorithm for public key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The process is shown in figure 6.
RSA uses two exponents, e and d, where e is public and d is private. Let the plaintext is M and C is cipher text, then at encryption
\[ C = M^e \mod n \]

And at decryption side
\[ M = C^d \mod n. \]

Where n is a very large number, created during key generation process.

The RSA scheme is the most widely accepted and implemented to public-key encryption. It is block cipher with plaintext and cipher text. RSA are integer between 0 ---- n-1 from some n. The size of n is 1024 bits that is less than \(2^{1024}.\)

The Encryption M and Decryption C are the following form [11]:
\[ C = M^e \mod n \quad \text{(Encryption Algorithm)} \]
\[ M = C^d \mod n \quad \text{(Decryption Algorithm)} \]
\[ = (M^e)^d \mod n \]
\[ = M^{ed} \mod n \]

RSA has two keys (e) for encryption and (d) for decryption.
n is large integer that produce two large prime number p, q.

Encryption key e chosen randomly between 1 and n that relatively prime to \((p-1) * (q-1)\).

Decryption key d can be computed from condition \(d * e = 1 \mod (p-1)(q-1)\)

Both sender and receiver must know the value of n.

The user knows the value of e.

The receiver knows the value of d.

The public –key is PU \((e, n)\).

The private –key is PR \((d, n)\).

Rashmi Nigoti et.al[31], uses DES algorithm and RSA algorithm for providing security to cloud storage. In existing systems only single level encryption and decryption is applied to Cloud data storage. Hackers can easily broke single level encryption. Hence we propose a system which uses multilevel encryption and decryption to provide more security for Cloud Storage.

5. STEGANOGRAPHY

Weakness of encryption is that the information is not hidden. A good solution to this is Steganography. Steganography is the science that hide data into suitable cover to conceal the data and prevent the detect it. Show the figure (7).
In figure 7, shown that secret message file hidden into cover produce stego-cover. All digital files formats can be used for steganography, but the formats that are more suitable which has high degree of redundancy [31]. The good covers for steganography must have two features; it should be popular and modification of the cover should not be visible to opponent[32]. LSB Algorithm is the most common method are used in steganography. And the color images are the best cover which used in steganography.

In this paper, we use both cryptography and steganography to increase the security of secret information in “cloud computing” through using two algorithms: DES, RSA and Steganography. Secret information may first be encrypted.
then select appropriate cover to keep the encrypted information.

6. OVERALL DESIGN OF PROPOSED WORK

Nowadays Cyber Criminals can easily access data storage. In Private Cloud Storage significant data, files and records are entrusted to a third party, which enables Data Security to become the main security issue in Cloud Computing. In Cloud Storage any organization’s or individual’s data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected resources authentication of stored data becomes a mandatory task.

In our proposed effort we provide great security to our secret information in cloud computing through using two cryptographic algorithms DES and RSA with Image Steganography together. figure (8) Shows the implement Three layers of security in cloud computing:
A. Proposed System Design:
The proposed system is designed to maintain security of text files only. This proposed system uses DES & RSA & Steganography algorithms to create the encryption and the hiding when user uploaded the text files in Cloud Storage.

And inverse Steganography algorithm & inverse DES algorithm & inverse RSA algorithm to generate decryption when user download file from Cloud Storage, for increasing security.

The proposed system is designed to maintain security of text files only. The proposed system design focuses on the following
objectives which are helpful in increasing the security of data storage.

**First Process: – For Encryption of text files:**

a. Implementing the DES algorithm of Encryption to generate first level encryption.
b. Implementing the RSA algorithm of Encryption to generate second level encryption.
c. Apply LSB algorithm in steganography to generate third level of security.
d. Upload Text file.
e. Store Cipher Text into Database.

**Second Process: – For Decryption of text files:**

a. Read Cipher Text from Database.
b. Implementing the inverse algorithm of LSB steganography to generate first level of Decryption process.
c. Apply the inverse RSA algorithm to generate second level of decryption process.
d. Implementing the inverse DES algorithm to generate Plain text.
e. Display Plain Text to User.
B. Proposed Algorithm:
We have suggested a grouping of three different security algorithms to reduce the security challenges of Cloud Storage. We have taken a combination of algorithms like: DES and RSA and LSB steganography. DES (Data Encryption Standard) is a symmetric key algorithm, in which a single key is used for both encryption/decryption of data. Whereas RSA is an asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes. But steganography is a secrecy method to hide data/information file in another file.
A user can upload Text file in Cloud Storage. When uploading file DES, RSA and LSB colour image steganography Encrypting and Hiding schemes are used to encode data.

**Embedding Algorithm**
The LSB algorithm inserts secret message data in cover image through handling the cover by using Robinson Compass filter to detect edges of the color image and selected these edges in array as pixels. And we using another array to select these pixels in randomly which used in Embedding Process will be described by the following steps and by algorithm1:

**Step 1:** Read the secret data.

**Step 2:** Determine the size of secret data file, and give the length of secret message as bytes.

**Step 3:** Load the cover image.
Step 4: Copy the first 54 bytes (header) of cover image and write it in a new stego file.

Step 5: Find the edges of image by using Robinson Compass filter specially to select edges of image.

Step 6: Compute the number of pixels of selected edges. And store the positions of these pixels in array(x,y). And

Step 7: Create new Random array corresponding the array of the positions of pixels.

Step 8: Select the position of edges according to the random array.

Step 9: While not end of secret message file: Read secret message file bytes sequentially. And convert to binary form.

Step 10: Hide first character(byte) of message into a pixel of edges of cover which selected by random array; Put first 3-bits of message byte instead 3− LSB of red color byte, and Put next 3−bits of message byte instead 3− LSB of green color byte, and Put last 2−bits of message byte instead 2− LSB of blue color byte in sequentially.

Step 11: Repeat step 8 until while condition is satisfied.

Step 12: Take the complete cover file as a stegocover file.
Algorithm (1) Embedding Process

```
{ 
    While not end of secret message file
    { 
        Read secret message file byte sequentially
        Convert to binary form
        { 
            While not end of cover file
                Read edges of cover file as pixels
                Put pixels in array
                Create random array of position.
                Read an edges pixels as a bytes sequentially.
            
            Put first 8 bits of secret data instead last of 3-bytes of first pixel
            according to random array of position.
        } 
        Repeat until while is satisfied.
        Take complete cover file as a stegocover file.
    }
}
```

Extracting Algorithm

Extracting Process will be described by the following steps and algorithm (2):

Step 1: Read the stego file. Compute the length secret message.

Step 2: Find the edges of stego file by using the Robinson compass filter that is used in hiding process.

Step 3: Create array of random numbers that used in hiding process.

Step 4: According to the size of secret data, the length of Extracting process will be performed by reading the sequence
bytes from stego file and extracting the secret data according to the random positions that are stored in array.

Step 5: Save the data of message in a new file.

Algorithm (2) Extracting Process

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong>: Stego file</td>
<td></td>
</tr>
<tr>
<td><strong>Output</strong>: Secret message</td>
<td></td>
</tr>
<tr>
<td><strong>Step 1</strong>: Read stego file.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong>: While not end of secret data file Do</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong>: Cut the last bits from each byte of edges of stego data according to the random positions that are stored in array and the length of secret message.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong>: Collection these extracted bits in bytes.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong>: Convert the secret data bytes into ASCII code. Then convert each ASCII code to characters.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong>: Display the extracted string as a file.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong>: End.</td>
<td></td>
</tr>
</tbody>
</table>

The Block Diagram of proposed work at multilevel encryption is shown in following figure 9.
As Shown in figure 9, the steps of Multi-level encryption will be as follows:

Upload the text file:

1. Now implementation of DES Algorithm takes place. The Data Encryption Standard (DES) is a block cipher. It encrypts data in blocks of size 64 bits each. That is 64 bits of plain
text goes as input to DES, which produces 64 bits of cipher text. The actual key used by DES algorithm for encryption is 56 bits in length. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds.

2. DES has 16 rounds, means the main algorithm is repeated 16 times to produce cipher text. As number of rounds increases, the security of system increases exponentially.

3. The first level encryption is generated using DES algorithm.


5. In RSA algorithm public key is used for encryption. RSA is a Block Cipher in which every message is mapped to an integer.

6. LSB algorithm is used to hide the secret data file into edges of colour images by using steganography science.

7. Once the data is hiding into image using LSB algorithm, it will be stored in Database of Cloud Storage.

And when downloading file, now inverse Steganography, RSA and DES algorithms are used to unhide/decrypt data. The Block Diagram of proposed work at multilevel unhide / decryption is shown in following figure 10.
As Shown in figure 10, the steps of Multi-level decryption will be as follows;

1. Inverse Steganography Algorithm which is called Extracting Process or Un-hiding Process to extract the encrypted data from cover image.

2. Inverse DES and RSA algorithms are used to decrypt data.
   a. First apply the Inverse RSA algorithm (decryption scheme) using private key. This algorithm will generate first level decrypt data.
b. Now apply the DES decryption algorithm on first level decrypt data.

c. DES decryption algorithm uses the same 56 bit length key for decryption.

d. DES algorithm of decryption will generate Plain text.

Now Plain Text will be displayed to the User… e

In Our proposed System, implementation of the DES algorithm takes place to generate first level encryption. And then we apply the RSA algorithm on the encrypted output of DES algorithm to generate second level encryption. And apply LSB steganography on the encrypted output of RSA to generate third level for security by hiding the output of RSA within edges of color images and saved into data centre of cloud. And using the same algorithms for decryption using inverse steganography and inverse DES and RSA algorithms. Means we applied multilevel Encryption and Decryption to provide security for cloud storage data.

7. Results

Result analysis contain security analysis. The security analysis consists of analysing several security characteristics such as:

1. Data Confidentiality— is analysed by comparing it with another data encrypted by DES , AES which uses the
one key to encrypt/decrypt data. Use RSA only, or LSB. In our proposed system, do not have any access to personal data in cloud, do employed three levels of security. The one know the key for three algorithms and is only know to the data owner which ensures the data confidentiality.

2. Authentication – is performed with help of the password set by the user through registration.

3. Integrity – ensures that data integrity into the cloud.

4. Hybrid method made the encryption and decryption process stronger.

5. RSA and DES are used as an integrated approach where data was encrypted with DES and private key can be encrypted with RSA algorithm. This leads to increase in performance compared with other techniques.

6. The combination of symmetric and asymmetric encryption techniques (such as DES and RSA) leads to ensure the security in the cloud computing.

8. Conclusion

Security is the large difficult of cloud computing. It is significant of data storage system. Increasing the security of data into cloud storage become very necessary. We proposed a good method to enhance security on data center and over transmission. This method is used DES & RSA to encrypt secret data and then hide these encrypted data within
images by using techniques of steganography to produce new image file called stego-images which are stored in the cloud data Centre. Now, our data have high secure from any attacks by opponents.

References
4. Tariq Ahmed1, Abdulla Aljumah2; "Cloud Computing and Steganography—attack Threat Relation”, BMAGNT Research Report( ISSN,1444-8939).College of computer Engineering & Sciences, Salman Bin Abdulaziz University, KSA.
8. Bohar Singh, Poonam, Aruna Rani, “To enhance the Reliability and security in cloud environment using RSA algorithm and image


http://dx.doi.org/10.1155/2014/190903.


33. Wojciech Mazurczyk, Krzysztof Szczypiorski; 'Is Cloud Computing Steganography–Proof?'; Institute of Telecommunications, Warsaw University of Technology Warsaw, Poland.