RESEARCH REVIEW JOURNALS
Volume-04
Issue-01
January -2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

A Study of Security of Cloud Using MSB Stegnography

[1]Kamal Kishore and [2]Dr. Jitendra Sheetlani

[1]Research Scholar, Sri Satya Sai University Of Technology & Medical Sciences, Sehore
[2]Associate Professor, Sri Satya Sai University Of Technology & Medical Sciences, Sehore

ARTICLE DETAILS

Article History
Published Online: 20 January 2019

Keywords
Cloud Computing, Data Storage Security, Steganography, Edges of image.

ABSTRACT

Cloud computing is an important issue in data storage security since the whole data is made available through a number of interconnected resource pools which permit the access of data through virtual machines. This transfers the software framework and databases to large data centers where data processing actually takes place. Since the resources pools are distributed in various parts of the world, data and services management can not be completely accurate. Therefore, the confidentiality and protection of data is highly difficult. We proposed an efficient and method to ensure data security in cloud computing by hiding data in the so-called steganography images, in order to ensure the privacy and security of data-at - rest in cloud computing. The article aims specifically at stopping unauthorized users from accessing data from cloud data storage centres. This scheme stores data within the edges of color images at cloud data storage centers and retrieves data if necessary. Cloud is a very common device. Cloud computing is the model for enabling easy access to a shared pool of configurable computer resources (e.g. networks , servers , storage, apps and services) on a shared demand basis, which can be easily supplied and released with minimal effort of interaction between service providers. Cloud computing allows cloud providers to raise or eliminate startup costs. In cloud computing , data security is the biggest challenge.

1. Introduction

In 1499, Johannes Trithemius's Steganography, a cryptographic treatise and steganography masking a book on sorcery, first recorded use of Steganography. The secret messages typically appear to be (or are part of) something else: photos, posts, shopping lists or some other cover text. For example, between the visible lines of a private letter the secret message may be in invisible ink. Some steganography implementations that do not have a common secret are forms of darkness protection, and the concept of Kerckhoffs adheres to key steganographic systems.

The benefit of steganography over encryption alone is that the hidden message is not the object of scrutiny. Clearly readable encrypted messages, however unbreakable they are, can cause suspicion in countries where encryption is illegal and can be incriminating in themselves.

Although cryptography alone is used to conceal the content of a message, steganography attempts to mask the fact that a hidden message is sent and the meaning of the messages is revealed.

The cyber-attack 's history is very old. Around the year 1820, it was the first cyber attack. Cyber-attacks are very common in this modern era: Trozan attacks, DOS attacks, bank account hacking, personal profile hacking and email messaging. By breaching anyone's computer, hackers may use personal data and cause significant losses.

Cyber assault is a illegal act by using a computer. Cyber-attack It's a form of cheating. The hacking of cyber-attacks is very common. Thanks to hacking, a hacker can collect any bank information and transfer money from the victim to his account. The cyber-attack can harm a person to this degree. This cyber-attack problem has spread worldwide. The explanation behind its growing craze is that by hacking someone's account, the criminal can gain a lot of money. The other definition of a cyber-attack is that every person's personal information is readily available. It affects people's personal lives and therefore culture.

Cyber-attacks often occur in non-monetary crimes including virus production and distribution. The virus is very dangerous to laptops , phones, mobiles and so on. Viruses are spread over the internet and connected to a particular file.

When the user attempts to download or clicks on the connection mentioned, the virus attached directly reaches the user's computer or mobile device and can destroy the user's private data. This virus is nothing but a few codes with a secret intent. The severity of the harm depends on the target of the virus. Some viruses such as Trojan can destroy important files and data from the computer or mobile device of the user. Therefore, a major concern for society is the issue of cyber-attacks.

Governments worldwide have started to take proactive steps to counter cyber attacks. In India, cyber law punishes the attacker. In an IT survey, 579 cases have been reported in India. Act. Act. Act. The number of online attacks is growing annually.

Cyber terrorism has also spread at a much higher rate these days. Videos are made by many militant groups such as ISIS and Lashkar. We try to influence the young people to join their party through these videos. The videos are available for download on the internet. Recently, boys and girls working for ISIS at college were discovered in India. You all decided that by seeing your videos on the internet they were inspired by this terrorist group. How very daunting is the problem of cyber-attack for society?

2. Review of related literature

Agarwal et al. (2012)[1] described that Steganophony is the concealment of messages in Voice-over-IP conversations, e.g.

the employment of delayed or corrupted packets that would normally be ignored by the receiver (this method is called LACK — Lost Audio Packets Steganography), or, alternatively, hiding information in unused header fields.

Lorrie et al. (2011) [2] highlighted that Detecting physical steganography requires careful physical examination, including the use of magnification, developer chemicals and ultraviolet light. It is a time-consuming process with obvious resource implications, even in countries that employ many people to spy on their fellow nationals.

Henry et al. (2012) [3] described that people need to be more aware about cyber attack. This is not a simple thing. People and Government have to tackle it seriously otherwise it may cost a lot to the society.

Jain et al. (2012) [4] described that the youngsters need to be more aware towards cyber terrorism. We should not watch any video which is not for our purpose. If any anti-nation video is found then inform to the police.

Neilson et al. (2011) [5] described that in the year 2005, 167 cases were registered under IT law and in the year 2010, 354 cases were registered. Hence, the problem of cyber attack is increasing year by year.

Moore et al. (2013) [6] reported that cyber attack is harming almost each and every business industry. Sometimes, hackers leak the confidential information of an industry leading to a lot of financial loss for that particular industry/company.

Williams et al. (2012) [7] described that WLAN Steganography is the transmission of steganograms in Wireless Local Area Networks. A practical example of WLAN Steganography is the HICCUPS system (Hidden Communication System for Corrupted Networks)

Steel et al. (2011) [8] described that downloading pirated video or audio file also comes under the category of cyber attack. School and college going youngsters be a part of it so often as they love to watch or listen any latest video or audio file. So youngsters need to be aware about it and should download only authorized video or audio files.

Gordon et al. (2012)[9] described that there are a lot of harmful viruses spread all over the internet. These viruses are attached to some specific files. If the user tries to download that particular file then virus attached to it comes in victim's device which may damage important files of the victim.

Rebovich et al. (2011)[10] highlighted that online gambling is very popular these days and it is also a part of cyber attack.

Haantz et al. (2012)[11] described that child pornography is also spreading among the youngsters which is a part of cyber attack as well.

Rantala et al. (2012)[12] described that small and medium industries have to suffer a lot due to cyber attack and their confidential data is leaked during tendering.

Richardson et al. (2013)[13] described that e-banking has also been damaged by cyber attack as the hackers can access the victim' s account and can transfer desired amount of money.

Rushinek et al. (2013)[14] described that due to increasing trend of cyber attacks, people now feel unsecured while using e-banking. So this cyber attack is the biggest challenge for the banking sector and its services.

Williams et al. (2013)[15] described that these cyber criminals often work in a group and work according to a plan to cheat any person or business.

Goodman et al. (2014)[16] described that students should be taught regarding cyber attack and its evil effects from the school days so that they cannot be a part of it unintentionally.

Simpson et al. (2012)[17] reported that organizations should use the technology of steganography so as to hide their confidential information so that no hacker can access that.

Thompson et al. (2012)[18] described that the procedure to find out the cyber criminal is same as that is followed for the other criminals. But the difference is that in case of cyber attack, the technology component needs to be found.

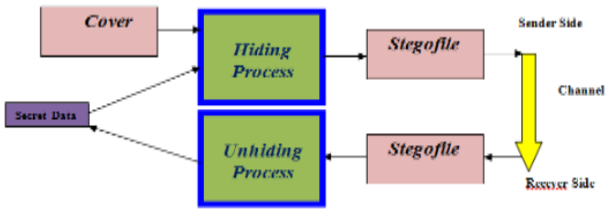
Feeny et al. (2014)[19] described that Government of all nations need to be united to eliminate the problem of cyber attack. Otherwise, it will damage every nation economically and socially.

Lee et al. (2013)[20] described that these hackers can be of any age. They can be youngsters or an old men. So it is very difficult to recognize the hackers as they look like a common person. So this threat is very challenging to overcome this problem of cyber-attack.

3. Cloud Computing & Information Hiding

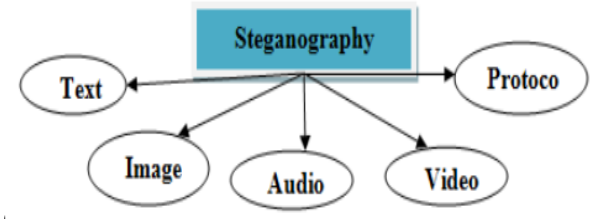
We plan to make information present in the cloud more private, confidential and accessible. Web users often have private information to store, send or receive. The most common way is to convert the data into various forms. Only those who know how to return data to its original form will understand the resulting results. This information protection method is referred to as encryption. Cryptography is a method of encrypting and decrypting data using mathematics. It allows you to store or transfer confidential information through vulnerable channels or networks (such as the Internet) so that none of you can read it other than the intended recipient.

The greatest downside of encryption is that the data does not exist. Information encrypted but still unreadable, if enough time has been given, can be unencrypted by anyone. Steganography[8] is a solution to this problem. Steganography is the art and science of hiding information in secret networks so that information is dissimulated and the message is not identified.



Details are covered in details in Steganography. It works by replacing unused bits of data (redundancy) with secret message figure bits in the computer files (such as graphics , sound, text , video, etc.). Steganography is the safest way to store, send, and secretly provide information, since it hides the hidden message and gives greater certainty[6]. All digital file formats can be used in steganography, but those of a high redundancy are the most appropriate formats. Redundant parts of an object may be altered without simple detection of an alteration[3]. Steganography is seen as a way to boost encryption but not to replace it[4]. The Steganograph message

can be encrypted first, and then an encrypted message cover file is changed which causes stegocopy. The message can be interpreted and deciphered only by those who know the technique used.



The best carries for steganography must include two features; it should be popular and modification of the carrier related to inserting the secret data should not be visible to third party[13].

There are several approaches in classifying steganography techniques. The classification according to the cover modifications are:

Substitution Techniques: These methods range from LSB coding. Basic substitution systems try to encode secret information by substituting insignificant parts of the cover by secret message bits. The receiver can extract the secret information if the positions secret information is acknowledged.

Transform Domain Techniques: These methods are represented by Discrete Cosine Transform (DCT) , Discrete Wavelet Transform(DWT), or others. In DWT, the standard technique of storing in the LSB is still applied, but the only difference is that the information is stored in the wavelet coefficients of a cover, instead of changing bits.

Statistical Techniques: The statistical approach is based on a pseudo random, statistical process that takes advantage of the human weakness to luminance variation. This method is more robust to image processing such as cropping and rotating.

Substitution Techniques: These methods range from LSB coding. LSB is One of the most popular amplitude modification methods is known as Least Significant Bit (LSB) insertion , it is common and easy to apply in both steganography and watermarking. As the name states, the information is encoded into the least significant bits of the cover file. In this technique LSB of binary sequence of each sample of digitized cover file is replaced with binary equivalent of secret message.

4. Security Issues In Cloud Computing

The majority of security issues in the cloud are: control loss, lack of confidence and multi-tenancy. Although these problems mainly occur in models of 3rd party administration, self-managed clouds still have security problems, but not the above. Consumers do not have control over data, software, and supplier resources, and so they must rely on their supplier to ensure data security and privacy, resource access, and services / resources monitoring and repair [2]. Chiles and McMakin (1996) define trust as raising the vulnerability of others who are unable to be managed by their actions if the costs of losing trust are greater than the advantages of maintaining trust [bible]. Confidence management is a major problem in the maintenance of cloud security. Cloud architecture is multi-faceted by a wide variety of different users sharing the same framework. The aggressor may then be legally on the same physical machine as the target. Cloud computing has all the Internet-related vulnerabilities. The Web has primarily been designed to be durable, has not been designed to be stable, and its attack surface is much greater than a close-knit application on the local area network. Seven major cloud threats [16-3] have been listed by the Cloud Security Alliance:

- 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.

Security in Cloud Deployment Models

The company may manage its infrastructure or delegate it to another party in a private cloud environment either in the physical or off-site location [1,8]. The internal cloud infrastructure can be controlled and no additional confidence mechanisms are required. Although there are several questions about a third-party provider operating the private cloud [8]. To increasing the level of security, users follow a private cloud implementation. A secure private virtual network is the alternative of isolating a third-party private cloud. The implementation of the public cloud is a model for a third-party service provider providing public services on a pay-per-use basis. Compared with private clouds, secure use of the rising public cloud is more difficult. To that end, the public cloud is more open or less insecure. In the article [8] the authors said trust is an essential issue for public clouds, hence third-party management. In [18], a trustworthy third-party auditor (TPA) is proposed for the resolution of public cloud confidence issues. Within the public / community cloud, organizations can maintain sensitive data only in a relatively small private cloud [1, 8] without compromising the security of basic information. The remaining less sensitive data could be used to allow a better use of resources in a public or a community cloud. The vulnerabilities of the hybrid cloud model in hybrid clouds are that. The possibility of integration points between the different cloud models is still possible.

5. Conclusion

Steganography protects secret concealment in machine files. Electronic communications in digital steganography may include steganographic coding within a transport layer, for example a file document, image file, program or protocol. Due to their large scale, media files are suitable for steganographic transmission. For example, a sender can start with an unsafe image file and change color to a letter in the alphabet every 100 pixels. The transition is so subtle that it is impossible that anyone who is not specifically looking for it will recognize it. Cases such as credit card fraud and online money laundering are currently on the increase. The current dangers of e-banking have also been revealed by cyberattack. The most prominent forms of cyber-attack in all countries include zenophobia, hate mailing and cyberterrorism. False spam, online breaches of music and apps often affect cyber-attacks. False malware scams. As every company operates in online mode around the world, all sectors are also vulnerable to cyber attacks because

the majority of its work is carried out via Internet pages. Cyber Attacks often impact companies of all sizes, as almost all organizations are present online and take advantage of rapid technological advantages but pay more attention to their safety risks.

The technical and infrastructural basis for tomorrow's computing have been cloud computing. The pay-as-you-go model is a service-based machine which provides all things in the service. The service offers features such as the sharing of resources, pooling of resources, availability of services on demand, multiple-tendency services, elasticity, security and privacy. Electronic service expansion and development demands continuous infrastructural change. Cloud Computing offers both hardware and software a fairly low-cost scalable alternative to internal infrastructure. Although it is necessary to benefit from being able to use the computing in a diverse range of industries, safety aspects are at the heart of the cloud-based computing world. Cloud computing approach security challenges are a little complex and comprehensive. Cloud computer security is critical to data place. The sharing of resources is another major security concern with the cloud computing model. Trust is another security issue for the use of cloud service because it is directly related to the integrity of cloud providers and their authenticity. Esteem building could be the key to a successful cloud computing environment. We think it is difficult to achieve end-to - end encryption due to the complexities of the cloud.

References

1. Agarwal, Communications Fraud Control Association. 2012 global fraud loss survey.
2. F. Lorrie, editor. “Proceedings of the Anti-Phishing Working Groups”, 2nd Annual e-Attack Researchers Summit 2011, Pittsburgh, Pennsylvania, USA, October 4–5, 2011, vol. 269 of ACM International Conference Proceeding Series. ACM, 2011.
3. Henry, “Machine learning to classify fraudulent websites”. 3rd Year Project Report, Computer Laboratory, University of Cambridge, 2012.
4. Jain, Microsoft Inc. Microsoft security intelligence report, volume 9, 2012.
5. Neilson Ratings. (2011). Top ten global web parent companies, home and work. Retrieved February 24, 2012.
6. N. Leontiadis, T. Moore, and N. Christin. “Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade”. In Proceedings of USENIX Security 2013, San Francisco, CA, August 2013.
7. Phil Williams, Organized Attack and Cyberattack: Synergies, Trends, and Responses, Retrieved December 5, 2012.
8. Steel. C. (2011), Windows Forensics: The Field Guide for Corporate Computer Investigations, Wiley.
9. Gordon, LA, Loeb MP, Lucyshyn W, Richardson R. 2012 CSI/FBI Computer Attack and Security Survey. Computer Security Institute, 2012.
10. Gordon, GR, Hosmer, CD, Siedsma, C, Rebovich D. Assessing Technology, Methods, and Information for Committing and Combating Cyber Attack. 2011.
11. Haantz, S. WCC Issue: Computer Attack: Computer as the Instrumentality of the Attack. National White Collar Attack Center. September 2012.
12. Rantala, RR. Cyberattack Against Business. Bureau of Justice Statistics. March 2012.
13. Richardson, R. 2013 CSI/FBI Computer Attack and Security Survey. Computer Security Institute, 2013.
14. Rushinek, A, Rushinek, SF. “Using Experts for Detecting and Litigating Computer Attack”
15. Williams, WP. The National Cyberattack Training Partnership. http://www.wjin.net/Pubs/3417.htm (accessed 22 November 2013).
16. Goodman, M. “Making Computer Attack Count”
17. Simpson, Doug. “Feds Find Dangerous Cyber stalking Hard to Prevent”. 12 June 2012.
18. Thompson, David. “2012 Computer Attack and Security Survey”.
19. Feeny, Peter. Personal interview. 1 December 2014.
20. Lee, Allen Lt. Personal interview. 19 November 2013.

