WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Data Security

Assistant Prof. Ms. Kalpana N. Rode, Ms. Shreya D. Terdale, Ms. Vidya V. Ghatage

Electronics &Telecommunications Engineering Department ,Sharad Institute of Technology College of Engineering, Yadrav, Ichalkaranji, India
vidyaghatage557@gmail.com

ABSTRACT

One of the techniques used in information security is the concealment technique, where the information to be hidden within another information medium to be saved in the process of messaging between two sides without detection. In this paper, an algorithm was proposed to conceal and encrypt data using several means.in order to ensure its preservation from detection and hackers. Wavelettransformer was used to change the shape of a wave of information (one and two-dimensional data) and its different mathematical formulas. Two sets of data were used, the first group used in a hidden process. The second group was considered as a means of both embedding and encryption.The data in the second group is reduced to the extent of sufficient for the modulation process, by extracting its high-value properties and then removing them from the mother's information wave. The process of encrypting of the two sets of data comes together using an exponential function. The result is undetectable information signals. Algorithms were built to hide and encrypt one and two-dimensional data. High-security signals and images were obtained. Decryption algorithms were built to return encrypted data to their original forms, and getting the replica data.

Keywords—Embedding and encryption, exponential function, information security technique, Wavelet transformer.

Introduction

With information and data sharing being an issue of concern for many companies, there has been the call to have secure processes that will ensure that there is better management of information and customer data. Many companies have experienced data breach in the past, the recent victims being Home Depot and Target. It has called for companies to have ways in which to secure the data and policies to ensure that there is better understanding of information that they have stored in their computer systems.

Cryptography and steganography are common methods to secure communications. For the purpose of protection against unauthorized access, confidentiality and data integrity must be observed. Cryptography scrambles a message so it cannot be understood. The Steganography hides the message so it cannot be seen [1, 2]. This research is made to combine both cryptography and Steganography methods into one
system for better confidentiality and security. In this advanced encrypting data hiding method, encrypted data can be embedded and extracted from both encrypted images and signals [3-5].
The data is encrypted using two scenarios. The first was to use a wavelet transformer to change the shape of the signal or image to a different form of the original[6, 7]. In the second stage, the exponential function was used to complete the encoding process to the final form. While the hiding algorithm was built between
the two encryption phases. (Stego-crypto) as a term, goes to attain its importance attributable to the exponential growth and secret communication of potential users over the web [2,3]. In addition, it has become an important tool for data security especially in military applications for example 5 G is more security others wireless communication techniques [5,6]. The proposed work includes: decompose both encrypting data and hiding data, generate the modulated medium, data embedding, data extraction, and data recovery.
Examples of data security technologies include backups, data masking and data erasure. A key data security technology measure is encryption, where digital data, software/hardware, and hard drives are encrypted and therefore rendered unreadable to unauthorized users and hackers.
One of the most commonly encountered methods of practicing data security is the use of authentication. With authentication, users must provide a password, code, biometric data, or some other form of data to verify identity before access to a system or data is granted.

Data security is also very important for health care records, so health advocates and medical practitioners in the U.S. and other countries are working

toward implementing electronic medical record (EMR) privacy by creating awareness about patient rights related to the release of data to laboratories, physicians, hospitals and other medical facilities.

Types of Data Security

Access Controls

This type of data security measures includes limiting both physical and digital access to critical systems and data. This includes making sure all computers and devices are protected with mandatory login entry, and that physical spaces can only be entered by authorized personnel.

Authentication

Similar to access controls, authentication refers specifically to accurately identifying users before they have access to data. This usually includes things like passwords, PIN numbers, security tokens, swipe cards, or biometrics.

Backups & Recovery

Good data security means you have a plan to securely access data in the event of system failure, disaster, data corruption, or breach. You'll need a backup data copy, stored on a separate format such as a physical disk, local network, or cloud to recover if needed.

Data Erasure

You'll want to dispose of data properly and on a regular basis. Data erasure employs software to completely overwrite data on any storage device and is more secure than standard data wiping. Data erasure verifies that the data is unrecoverable and therefore won't fall into the wrong hands.

Data Masking

By using data masking software, information is hidden by obscuring letters and numbers with proxy characters. This effectively masks key information even if an unauthorized party gains access to it. The data changes back to its original form only when an authorized user receives it.

Data Resiliency

Comprehensive data security means that your systems can endure or recover from failures. Building resiliency into your hardware and software means that events like power outages or natural disasters won't compromise security.

Encryption

A computer algorithm transforms text characters into an unreadable format via encryption keys. Only authorized users with the proper corresponding keys can unlock and access the information. Everything from files and a database to email communications can — and should — be encrypted to some extent.

Main Elements of Data Security

There are three core elements to data security that all organizations should adhere to: Confidentiality, Integrity, and Availability. These concepts are also referred to as the CIA Triad, functioning as a security model and framework for top-notch data security. Here's what each core element means in terms of keeping your sensitive data protected from unauthorized access and data exfiltration.

- *Confidentiality*. Ensures that data is accessed only by authorized users with the proper credentials.
- *Integrity*. Ensure that all data stored is reliable, accurate, and not subject to unwarranted changes.

- *Availability*. Ensures that data is readily — and safely — accessible and available for ongoing business needs.

Methodology

1. Secure Your End-Point Access

A hosted QuickBooks solution stores your important data on third-party remote servers. You can access data/files on cloude pc azure anywhere and anytime via the Internet. While this prevents your data from getting misplaced if someone steals your hard drives.

Avoid leaving your screen ON when you exit your workstation.

Similarly, while working from home, always provide your end-point devices are locked and cannot be accessed using a saved password. It would benefit if you also deactivated old devices that you no longer use.

2. Implement Password Management Policies

A password is your first line of security against unauthorized data access. It would help if you mandated organization-wide password management policies. Avoid using personal data as your password. Someone near to you may exploit it and illicitly access your system.

Please make a strong password that combines different alphanumeric characters and symbols. Furthermore, it activates multi-factor authentication for signing in. This adds another layer to your safety.

3. Avoid Storing Data Locally

The whole point behind hosting your QB is to avoid storing your sensitive data on-premises. Your local device may not have the required security measures for protecting your data. So, a hacker has a more useful chance of accessing it. This will infect your system and acquire access to your files. So, like this quote says, "Prevention is better than cure"—avoid protecting data on your local devices and let it remain secured in your cloud environment.

4. Invest in Quality Security Tools

Having top-rated security tools in your hosted QB environment is a make-or-break for your data privacy. Without them, your sensitive data could be smoothly compromised. You can either deploy quality tools yourself or avail yourself of a hosted solution from a reputed quick books cloude hosting provider.

Cloud providers implement a special security framework with the latest available technologies. Their hosted environment is secured with modern anti-malware and antivirus software, advanced AI surveillance, and numerous software/hardware-based firewalls.

Most cloud providers deploy an IDP system for swiftly detecting and preventing any data breach. Their data servers are even secured by network filters for filtering out malicious IPs and preventing hackers from carrying out a DDoS attack.

5. Use a Safe Network Connection

A highly secured hosting environment can resist a direct hacking attempt. But what if they intercept your important data while in transit? For this, you must use a secure internet connection while logging into your hosted QuickBooks. Avoid using public Wi-Fi when you are handling any sensitive data. Most cybercriminals use open Wi-Fi sources for luring individuals into using them. Once done, they can easily hack into your device and acquire access to your data. To prevent this, use the Internet just from verified sources.

Data Security Technologies

While compliance will keep you in good standing with regulatory agencies, a more complete approach will help keep threats at bay. The following technologies should be a part of every company's data security strategy.

Data Encryption

Encryption is viewed as one of the most reliable ways to keep your data confidential at rest, in transit, or when processing real-time analytics. Data encryption uses algorithms to encode data into an unreadable format that needs an authorized key for decryption. But cryptographic processing can be vulnerable to side channel attacks and can affect performance.

The latest technologies can speed up encryption and boost security without affecting performance.

User Authentication and Authorization

To help keep unauthorized users from accessing sensitive data, you'll need to have the right user authentication methods in place. But strong passwords aren't enough. The most-secure methods use hardware security features such as biometrics, built-in two-factor authentication, and secure enclave technology built into the processor itself.

Hardware-Based Security

As hackers have become more sophisticated, they've made their way down the stack, increasing attacks at the hardware level. That's why you need to protect your data at every layer of the IT infrastructure—not just the software. Intel's hardware-enabled security capabilities include protections built right into the silicon, creating Trusted Infrastructure, which helps secure hardware, firmware, operating system, applications, networks, and the cloud.

Data Backup

Data backup solutions can help you restore your company and customer data in the event of a storage failure, breach, or disaster. By creating an exact copy of your data and storing it in a secure location that can be accessed by authorized administrators, you can minimize the risk of a primary data failure. However, for better data integrity and security, you'll need protections for that backup, both while that data is being sent to its backup location as well as when it's stored to assist in spotting anomalies or threats early. A documented data backup policy can help you comply with various security regulations as well as establish a consistent, reliable data recovery process.

Conclusion

You require to take cautious steps to prevent data loss and theft. Apps4Rent is an intuit authorized QuickBooks hosting provider which assists thousands of customers from small to big-sized companies all over the United States. They even specialize in providing IT consultation to companies that require assistance in migration services like Exchange Online Mailbox Migration into business processes.

REFERENCES

[1]O. Abikoye, K.Adewole, and A. Oladipupo, "Efficient data hiding system using cryptography and steganography," 2012.

[2]P. P. Aung, T. M. J. I. J. o. I. T. Naing, Modeling, and Computing, "A novel secure combination technique of steganography and cryptography," vol. 2, no. 1, pp. 55-62, 2014. https://doi.org/10.5121/ijitmc.2014.2105

[3]N. Rashmi and K. Jyothi, "An improved method for reversible data hiding steganography combined with cryptography," in 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 81-84: IEEE. https://doi.org/10.1109/icisc.2018.839 8946

[4]C. Anuradha, S. J. I. J. o. A. R. i. C. S. Lavanya, and S. Engineering, "Secure and authenticated reversible data hiding in encrypted image," vol. 3, no. 4, 2013.

[5]H. Alrikabi, A. H. Alaidi, and K. J. I. J. o. I. M. T. Nasser, "The Application of Wireless Communication in IOT for Saving Electrical Energy," vol. 14, no. 01, pp. 152-160, 2020. https://doi.org/10.3991/ijim.v14i01.11538

[6]G. Bhatnagar, Q. J. Wu, and B. J. I. S. Raman, "Discrete fractional wavelet transform and its application to multiple encryption," vol. 223, pp. 297-316, 2013. https://doi.org/10.1016/j.ins.2012.09.053

[7]H. T. S. J. W. J. o. E. S. ALRikabi, "Study the Matching of the Level of Electromagnetic Radiation Emitted by Communication Towers in the Kut City with the International Health organization criterion," vol. 4, no. 1, pp. 101-111, 2016.