A SMART ENCRYPTION BASED SECURITY KEY MANAGEMENT IN MODERN CLOUD COMPUTING

M. Sutharsan

Department of Electronics and Communication Engineering, Muthayammal Engineering College, India

Abstract

In general, the Cloud Servers in the present modern era have more usage from the peoples. The special feature is that you can easily access data from these clouds. But it is the largest problem that can be accessed by the person who puts Password. That means some talented hacker groups will have those Password data to be simplified. There is also a vulnerable issue of its security features. At this paper, an encryption algorithm, which is based on the input of the key information, has been proposed by its security issues. This protective encryption combines a security code with the inclined plants based on its data. The security code in this link will be registered in the Cloud Server. That code will check and send it to its entries. When the user provides the right inputs in that way, let him out. Thus, security processes are more and more reliable.

Keywords:

Cloud Server, Encryption Algorithm, Security Code, Password Data

1. INTRODUCTION

Today we use all the services of the cloud storage, drop box, Google Drive, One Drive (Micro side) or others, and the fact is that at least well known, the most well-known, usually our data is well protected [1]. Of course, if someone cannot catch us, approach the data, already a multi-time and a long time ago, Apple service to those who use iCloud, iPhones, iPhones, and Mac Books for those who have saved their data for many parties [2]. The problem is that in a server, the security flaws y exhibit our data and we are enhanced with login data. Of course, if we do not use such data carefully (for example when logging in unsafe networks or computers) and if someone receives it, they can access the full control of our account, and of course, if we have the information stored there, it is important to datastore [3].

That is why we are going to show a way to protect the local folders and then synchronize local folders and synchronize them with any cloud service, despite any of the most important institutions, because information is important, because they are important to believe that they will disappear overnight and even guarantees a little more seriousness [4]. All we uploading to the cloud work when doing this work, it cannot be encrypted, but they cannot use it or know what it is. We need to use some of the encryption tool, which we are going to use for the encryption tool, and most Linux distributions are available in the most Linux distributions and it works differently than True Crypt because it is a encrypted container - data itself when we take a encrypted container No-What is done here is to encrypt each file in the folder specified [5]. This folder will be automatically synchronized in another folder and all the information will not be encrypted from the data we store [6].

The Encryption is the process of using a method to transfer information that is unreadable to unauthorized users. This cryptographic system protects important data such as credit card numbers by encrypting and converting information into unreadable cyber text. This encrypted data can only be encrypted or readable with a single key [7]. The symmetric-key and the asymmetric key are the two primary types of encryptions. The Encryption is essential to ensure important information is provided in a reliable and reliable manner [8].

The Symmetric-key encryption uses two secret, often identical keys or codes for computers engaged in messaging. The data packet of each secret key is self-encrypted. The first symmetric encryption algorithm is the Data Encryption Standard (DES), which uses a 56-bit key and is not considered an attack-source [9]. Advanced Encryption Standard (AES) is considered the most reliable because it uses 128-bit, 192 bit or 256 bit key. Asymmetric key encryption, also known as public key encryption, combines private and public keys [10]. The public key is shared with computers trying to securely communicate with the user's computer. This key handle encryption, making the message indescribable in traffic. The unique matching key is unique to the user's computer. This allows the message to be decrypted and read. Pretty good privacy (PGP) is the most commonly used public key encryption system.

The simplest way to interpret Gmail's current encryption is to think of an email message that travels from the sender's computer to the intended email recipient. During transport, digital messages are encrypted via Transport Layer Security (DLS), a protocol that provides security between interacting client / server applications over the Internet [11]. Misconceptions come into effect when the message is at rest to the sender, intermediate servers or recipient. At those points, the message was not encrypted. If the recipient's email program does not accept HTTPS (using TLS) messages, the message is not encrypted. That's why experts say that the current Gmail encryption is not "end-to-end" [12]. Google keeps track of the number of Gmail messages sent and encrypted while being transmitted, as well as the number of messages received by Gmail users.

2. RELATED WORKS

In the [1] discussed the convenience and security conflict, convenience usually wins. Currently, setting up email encryption is complicated and a pain to use. Also, until recently, people were not interested in encrypting their email. In [2] expressed the problem with end-to-end email encryption is the need for compatible encryption software for both parties. If the programs are not compatible, the email message will not be encrypted. Therefore, more than the risk of not reading the email, most senders do not bother with encryption.

The author [5] discussed the various data and location. The data goes to unknown, uncontrollable, and increasingly unreliable locations. It occurs in the normal course of the process, through user error or malicious or malicious activity. Because the places

where your data goes are unreliable, you cannot trust the security of your network, device, or application to protect that data.

In the encryption of [7] alone is not enough to protect data. Encryption should be combined with continuous, modifiable access controls, which enable the originator to define the conditions under which a key is issued, and change those controls as circumstances dictate.

There should be comprehensive, comprehensive visibility of who can access protected data, when, and how often. This comprehensive visibility ensures auditing for regulatory requirements and power analyzes, for a broader understanding of application methods and potential issues, which enhances control [9].

For data-centered security to be effective, data must be protected at the point of origin. The first step in the process is to encrypt the data so that wherever it goes, what network it travels to, and ultimately where it lives is secure. Otherwise, it requires every computer, every network connection and every person's trust to do so, leaving that information in the care of the originator, and as long as it or any other copy [10].

3. METHODOLOGY

The proposed Cloud Security key encryption algorithm modules are (CSKEA) shown in Fig.1. It is a symmetrical module cipher with 128-bit volume size and variable-long encryption key, which is one of the most secure encryption protocols in the industry. Cloud Security key encryption is a new way to protect your data using cloud computing technology. This is a safe way to save your data, which is different from other methods because third parties do not need to keep and manage your data.

It can count that it is very safe and your data is safe. Cloud Security key encryption is a new way to protect your data, which is different from other methods because third parties do not need to keep and manage your data. You can count that it is very safe and your data is safe. The Cloud Security key is an innovative encryption protocol, which provides a safe way to save and manage important information such as data and passwords. Cloud Security key encodes your passwords, so they cannot see anyone else and cannot access your data or use anything other than you thought. This means you can have your own encrypted data vault and share it with loved ones. The only way to decrypt the dubish encrypted file is to use the user's personal key created by the file. To do this, the users must have a trusted device (computer, tablet, and phone) that supports the duplicate encryption.

This type of encryption comes in two versions: one requires physical access to the other reliable device (computer) only. Two versions support all operating systems that do not have special software and updates for Windows, Linux, IOS and Android. The Cloud Security key protocol provides advanced features such as anonymous access, encrypting zero knowledge, and 100 percent privacy. Protocol provides fast speed and non-sinful protection for mobile devices and desktop computers. Because the private key stored in Cloud server is completely encrypted, you no longer need to worry about keys or passwords. Using other wallets such as My ether Wallet or Nano wallet can send money to anyone else who uses your friends or wallet.

Using your data to encrypt your data is a new way to protect your data. Using Cloud server technology, you can save your data in the encrypted form using encryption. This means that if someone approaches it, it should encrypt it before they read information. Cloud server technology is built on top of Pit-coin, ie Pit-coupling is the same kind of security and privacy. Because of this, using Cloud Security key encryption to save your data, allows you to use all the benefits such as Cloud server technology, such as the low transaction fees and quick confirmations. You can use this method because you do not need third parties or servers to host or manage your data.

Step 1: To create a folder, preferably in our personal folder, and it’s going to save data without encryption.

Step 2: To create a folder in the local folder, which sync with us preferred cloud service, which will be encrypted data. This folder is created by ENCFS and naturally called 'private'.

Step 3: The password is asked for us, and we have to create and remember that we cannot change access to our data without it.

Step 4: All we want to protect and move to the folder from step 1, copy or create.

Step 5: NCF takes care of automatically synchronization, encryption and cloud service with the folder created in Step 2.

The Coding involves the use of a code to convert the original data into a format that can be used by an external process. The type of code used to convert characters is called the American Standard Code for Information Interchange (ASCII), the most commonly used encryption scheme for files containing text. ASCII contains both uppercase and lowercase letters, symbols, punctuation, and printable and non-printable characters. Some characters are assigned a unique number. The standard ASCII scheme has only 127-character levels from zero; 128 to 255 is not defined. The problem of undefined characters is solved by Unicode encryption, which assigns a number to each character used worldwide. Other types of codes include Pin hex, Unicode (Unix to Unix encryption) and Multi-Purpose Internet Mail Extensions (MIME).

The Encryption is also used to reduce the size of audio and video files. Each audio and video file format has a corresponding coder-decoder (codec) program that uses it to encode the appropriate format and then decode it to playback. Not to be confused with encryption that encodes content. Both techniques are widely used in the fields of networking, software programming, wireless communication and storage.

Cloud Security key encryption is a safe way to save data. Whenever you want, it allows you to access your data from everywhere you want and any device. Cloud server technology operates this technology is based on the open-source protocol of Pit-code. It has become one of the most popular forms of Pit-code's digital currency, because it is fast, cheaper and easy to use. Cloud Security key encryption is more than a decade, but it is recently popular, because third parties act without having to keep and manage your data. Cloud Security key encoding people provide the opportunity to use their favorite cryptograms or without paying fees or charges charged by NFT intermediaries-traditional financial systems today.

4. RESULTS AND DISCUSSION

The proposed Cloud Security key encryption algorithm (CSKEA) was compared with the existing RC6 encryption algorithm (RC6EA), Homomorphic encryption method (HEM), hybrid symmetric encryption algorithm (HSEA) and RSA magic square algorithm (RSAMS)

4.1 BIG DATA MANAGEMENT

This is the technology you need if you want to save your data in Cloud server. The dubish encryption uses the algorithm to change the data as encrypted form. Then decode the system encrypted data and saves it safely into the database, changing it to its original form. There are information about all data transactions and "smart contracts" (programs) that are done between users in the database. These smart contracts are used to provide additional security measures for data stored in Cloud server. Therefore, no one can read any part of your data stored in this database.

Table.1. Comparison of Big data Management

Instruction	RC6EA	HEM	HSEA	RSAMS	CSKEA
1000	59.83	64.5	88.63	76.79	92.59
2000	58.16	63.37	85.7	75.53	90.12
3000	56.21	63.02	84.16	73.64	89.32
4000	54.22	61.07	82.13	72.44	88.12
5000	51.64	60.3	81.23	80.88	87.48
6000	49.65	59.92	79.26	69.13	86.22
7000	47.63	58.79	77.79	68.2	85.22

4.2 SMALL DATA MANAGEMENT

Cloud Security key encryption is a safe data storage solution for all sized businesses. This allows you to save electronics and safe information without any cost in cloud computing. Currently, it is only available for private customers, but sooner, it is available in public.

Table.2. Comparison of Small data Management

Instruction	RC6EA	HEM	HSEA	RSAMS	CSKEA
1000	58.24	70.57	87.38	77.43	91.42
2000	56.61	68.83	85.8	76.01	90.13
3000	56.13	66.49	83.6	74.75	89.12
4000	54.84	65.68	81.97	72.76	88.23
5000	52.73	63.39	80.83	70.29	87.86
6000	51.24	61.46	78.63	68.85	86.22
7000	49.43	59.73	77.48	67.13	85.85

4.3 CLOUD DATA MANAGEMENT

Cloud Security key encryption is a safe way to save your data, which is different from other methods because third parties do not need to keep and manage your data. The best part? It's free. So you do not have to pay for expensive storage solutions or do not have to worry about leaving the information you need. Make sure the service provider has a good security registry, and they will give you an encrypted file.

Table.3. Comparison of Cloud data Management

Instruction	RC6EA	HEM	HSEA	RSAMS	CSKEA
1000	68.13	66.47	87.22	76.42	93.42
2000	66.64	64.5	84.8	74.22	91.43
3000	65.84	63.37	84.39	73.42	90.23
4000	63.51	62.16	82.79	72.75	89.75
5000	62.5	61.79	80.47	71.32	88.32
6000	61.86	60.26	79.22	70.23	87.16
7000	61.2	59.76	76.49	69.75	86.39

4.4 DIGITAL DATA MANAGEMENT

To use Cloud security key encryption, you need to install the app on your computer. This will allow you to send encrypted messages between the two devices already connected to the same network. Digital property is the file, image or video. All data can be stored in a smart deal, which can read and send it to another device through Apps.

Table.4. Comparison of Digital data Management

Instruction	RC6EA	HEM	HSEA	RSAMS	CSKEA
1000	59.50	62.83	79.82	68.99	92.16
2000	59.17	61.33	79.23	67.12	91.12
3000	57.83	60.22	78.25	66.29	90.99
4000	56.69	59.84	77.04	65.38	90.03
5000	55.64	58.83	75.90	64.46	90.46
6000	54.71	57.76	75.04	63.21	90.17
7000	53.69	56.81	74.04	62.13	89.30

4.5 ECONOMIC DATA MANAGEMENT

Cloud security key encryption makes great impact on business. This is not only to protect your data from external threats. This is the ability to protect your data from the threats inside. For example, if you store important information on the laptop or mobile device, the hacker can easily steal that information using the cloud security key Encryption. To make it valuable for businesses, it will help protect their data and make them more secure. The technology is cheaper and easy to use.

Table.5. Comparison of Economic data Management

Instruction	RC6EA	HEM	HSEA	RSAMS	CSKEA
1000	67.26	71.25	88.92	73.01	95.84
2000	67.59	72.75	89.51	74.88	96.88
3000	68.93	73.86	90.49	75.71	97.01
4000	70.07	74.24	91.70	76.62	97.97
5000	71.12	75.25	92.84	77.54	97.54
6000	72.05	76.32	93.70	78.79	98.40
7000	73.07	77.27	94.70	79.87	98.84

4.6 DATA CENTERED SECURITY

The principle of data-centric security is simple: data is protected if a network is compromised, or if the mobile device is lost or stolen. Those companies that embrace this paradigm shift have realized the need to add control and visibility to data security by looking beyond traditional solutions. Adopting this evolving vision of data-centric security enables companies at all levels to secure sensitive data, regardless of where that data is.

Table.6: Comparison of Data centered security

Input Instructions	RC6EA	HEM	HSEA	RSAMS	CSKEA
1000	58.63	67.61	81.52	65.58	90.58
2000	60.12	69.58	83.94	67.78	92.57
3000	60.92	70.71	84.35	68.58	93.77
4000	63.25	71.92	85.95	69.25	94.25
5000	64.26	72.29	88.27	70.68	95.68
6000	64.9	73.82	89.52	71.77	96.84
7000	65.56	74.32	92.25	72.25	97.61

Data-centric security solutions have traditionally been inward-facing and focus on securing data within the company's domain as they are collected and stored. However, data moves away from the center of the organization, not towards it, and mega trends such as cloud and motion accelerate the process. An Effective Data-Center Security Protects data from being shared and consumed then that are moving away from the organization's hub. This includes temporary relationships across domain boundaries, enabling secure communication with clients and partners.

5. CONCLUSION

The data-centric security solution can protect data wherever it goes. As the first fact tells us, data and many of its naturally created copies go to many places, including mobile devices, personal devices and the cloud. An effective solution is to protect data independent of the device, application or network. That data must be protected regardless of its format or location, whether it is dormant, in motion, or in use. It should extend beyond the perimeter immediately and be capable of protecting temporary conversations. It would be useful to consider the many point-and-function-specific data-center security solutions available in the market. By their very nature, these solutions create pitfalls of security because - as the first important fact commands - the data will reside somewhere outside of their operational period. Since these solutions are nowhere near as secure, agencies and businesses are forced to set up multiple pits. Despite the best attempts at many of these pits, the results are predicTable.but the data will still fall between the gaps. These gaps are precisely where external enemies and malicious individuals are waiting to exploit vulnerabilities and steal data. Furthermore, each silo refers to the task of obtaining, implementing and supporting the relevant solution and the operational load to manage multiple solutions.

REFERENCES

[1] Neha Agrawal and Shashikala Tapaswi, "A Trustworthy Agent-based Encrypted Access control Method for Mobile Cloud Computing Environment", *Pervasive and Mobile Computing*, Vol. 52, pp. 13-28, 2019.

[2] Cheng-Chi Lee, Pei-Shan Chung and Min-Shiang Hwang, "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments", *International Journal of Network Security*, Vol. 15, No. 4, pp. 231-240, 2013.

[3] Voundi Koe Arthur Sandor, Yaping Lin, Xiehua Li, Feng Lin and Shiwen Zhang, "Efficient Decentralized MultiAuthority Attribute based Encryption for Mobile Cloud Data Storage", *Journal of Network and Computer Applications*, Vol. 129, pp. 25-36, 2019.

[4] Xinwen Zhang, Joshua Schiffman, Simon Gibbs, Anugeetha Kunjithapatham and Sangoh Jeong, "Securing Elastic Applications on Mobile Devices for Cloud Computing", *Proceedings of International Workshop on Cloud Computing*, pp. 1-6, 2009.

[5] Merve Bayramustaa and V. Aslihan Nasirb,"A Fad or Future of IT?: A Comprehensive Literature Review on the Cloud Computing Research", International Journal of Information Management, Vol. 36, No. 4, pp. 635-644, 2016.

[6] S. Wang, K. Guo and Y. Zhang, "Traceable CiphertextPolicy Attribute-Based Encryption Scheme with Attribute Level User Revocation for Cloud Storage", *PLOS ONE*, Vol. 13, No. 10, pp. 1-12, 2018.

[7] J.K. Liu, T.H. Yuen, P. Zhang and K. Liang, "Time-Based Direct Revocable Ciphertext-Policy Attribute-Based Encryption with Short Revocation List", *Proceedings of International Conference on Applied Cryptography and Network Security*, pp. 516-534, 2018.

[8] Xuanxia Yao, Zhi Chen and Ye Tian, "A Lightweight Attribute-based Encryption Scheme for the Internet of Things", *Future Generation Computer Systems*, Vol. 49, pp. 104-112, 2015.

[9] Umashankar. "A Review on Attribute Based Encryption (ABE) and ABE Types", *International Journal of Computer Science and Mobile Computing*, Vol. 5, No. 5, pp. 142-146, 2016.

[10] Balamurugan and P. Venkata Krishna, "Extensive Survey on Usage of Attribute Based Encryption in Cloud", *Journal of Emerging Technologies in Web Intelligence*, Vol. 6, No. 3, pp. 263-272, 2014.

[11] Yinghui Zhang, Xiaofeng Chen, Jin Li, Duncan S.Wong, Hui Li and IlsunYou, "Ensuring Attribute Privacy Protection and Fast Decryption for Outsourced Data Security in Mobile Cloud Computing", *Information Sciences*, Vol. 379, pp. 42-61, 2017.

[12] Maha Tebaa and Said El Hajii, "Secure Cloud Computing through Homomorphic Encryption", *International Journal of Advancements in Computing Technology*, Vol. 5, No. 16, pp. 1-12, 2013.