Pros and Cons of Key Escrow Agreements in Cloud

Raja Abou[1], Baris Celiktas[1]

1 Isik University

Funding: No specific funding was received for this work.

Potential competing interests: No potential competing interests to declare.

Abstract

Encryption of data at rest, in use, and in transit is a major requirement in the decision of migrating to cloud services. With the usage of encryption, the key management process, which is related to the creation, usage, and storage of the encryption keys had been raised. Dealing with these keys manually exposes enterprises to the risk of losing the encrypted data because of the loose of encryption keys. From that point of view, key escrow or key restore services were needed. In this research, we are going to discuss the key escrow advantages and disadvantages to help the decision makers in taking their decision of using these services or not.

Mhd Raja Abou Harb

Computer Engineering Department

Isik University

Istanbul, Turkey

21comp9001@isik.edu.tr

Baris Celiktas

Computer Engineering department

Isik University

Istanbul, Turkey

brsclkts1@hotmail.com

Keywords: Key escrow services, key restore services, pros and cons of key escrow, encryption in cloud.

I. Introduction

Encryption is a need to protect the data in cloud environments. Data shall be encrypted when it is transferred to cloud

environments and when they are stored or achieved. Encrypting data provides organizations with a level of security to achieve confidentiality and prevent unauthorized access to these data. When encryption was started to use, new risks had been raised for organizations which are the key management processes. Organizations shall have proper methodologies to deal with encryption keys in the creation, storage, and usage of these keys. Improper key management processes may lead to the risk of losing the encrypted data because it is hard or even impossible to reach the encrypted data without having the decryption keys. For example, the key size of Advanced Encryption Standard (AES) is 256 bits, so the brute force to guess the decryption key is by checking 2 to the power 255 of possibilities. Using a computer with quad-core processing with hyper-threading, that equates to 230 bytes per second, and with a calculation to the worst-case scenario, the number of years to reach the data is 27 trillion trillion trillion trillion trillion years [1].

The first solution to handle the encryption keys, that was used by organizations, was human-based handling. This way led to the risk of losing the keys because of human errors, termination of the key holder person or even losing him/her because of death. Also, if we go back to the AES-256 encryption algorithm, we notice that it is hard to memorize 256 bit key or store it manually. From this point of view, having a systematic way to deal with these keys was a need, and that is why key escrow services were invented.

In this work, we are going to spot the light on the key escrow services and the gained benefits from these services along with their pitfalls. This work can be used to help decision-makers in organizations in reducing the risks of key escrow services.

The rest of this paper is organized as follows: in section II, the formal definition of the key escrow services will be shown, section III will show how key escrow services work and it will show one of the first initiatives related to that topic which is Clipper ship. In section IV, we are going to discuss the options the cloud customers may use when they decide to go with key escrow systems. Section V will discuss the advantages of using key escrow systems, while section VI will show the disadvantages. Section VII will show the comments related to the discussed ideas. Lastly, section VIII will show the conclusion of the discussed ideas.

II. Key Escrow Definition

The National Institute for Standards and Technologies (NIST) defined Key Escrow Services as the “deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement.” [2]

In other words, the key escrow service is a methodology for storing the used cryptography keys. Each stored key in the key escrow system is tied to the original user and subsequently encrypted for security purposes. Some resources name key escrow services as key recovery systems, because of the functionality that they provides.

You can see similarities between key escrow systems and the valet or coat check function, where each key is connected

to the user that leverages it, and then returned once queried. Also, there is a similarity between key escrow and when you have to put your home keys with your neighbors in case of emergencies. Key escrow agreements in clouds can be defined as an agreement between business owners (who may be referred to by cloud clients) and a reliable outsider who can provide a solution for safely storing their keys. The provided service can be referred to hardware security module (HSM) as a Service. which ensure that cryptography keys remain protected, not only in storage, but also while in use.

III. Key Escrow Methodology

In this section, we are going to show the simplest way for implementing a key escrow system, knowing that there are several other ways to implement it.

Figure 1 shows the encryption and decryption processes for the normal encryption algorithms and the key escrow systems.

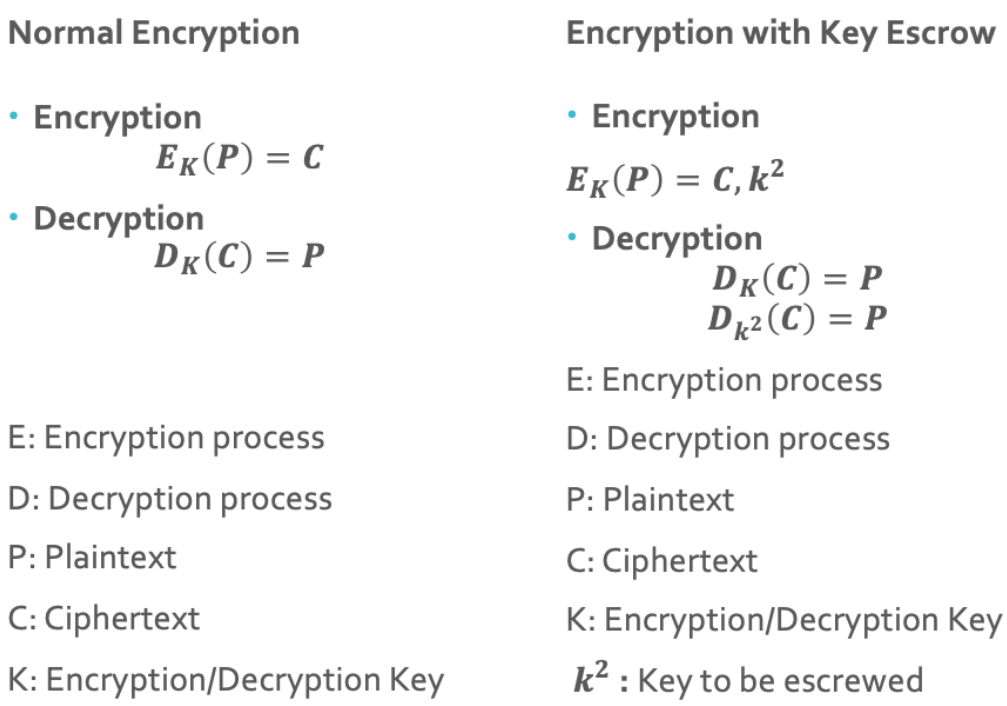

Fig. 1. Encryption and Decryption Processes for Classical and Key Escrow Encryption Algorithms.

In the classical ways of encryption algorithms, the encryption and decryption processes can be done through keys (which may be similar in symmetric encryption algorithms and different in the asymmetric encryption algorithms), while in the key escrow algorithms, the encryption and decryption processes are similar, except having an extra key (or copy from the main keys) in the encryption process. This extra key can be sent to a trusted third party who is offering the key escrow services, and it is used to reach the plain-text using a decryption process [3].

A. Clipper Chip

When the key escrow proposals were initiated, the United States of America (USA) enforced these solutions through several regulations, and one of them was the escrowed encryption standard [4].

The main reason for the concerns of the US government in key escrow systems is having transparency for the encrypted data by having a copy from the decryption key in case of judge warrents. This demand had increased especially after the eleventh of September event. The Clipper chip was part of the proposal inside that standard.

In order to allow encryption in the face of security risks, the chip-set was marketed as an encryption device with a master key that was kept in escrow by the government. By 1996, the contentious Clipper Chip was no longer in use because of the violation of privacy and several cases of abuse, but the idea was transformed into the widely used Pretty Good Privacy (PGP) encryption technology.

The Clipper ship was used for encrypting voice and data messages, and it kept a backdoor for the government to access the encrypted data through a copy of the encrypted key which is held by the federal agencies. It used Skipjack encryption, an encryption algorithm that was invented by the National Security Agency (NSA) and it is classified as national security data which prevents the scientific community from reviewing it, algorithm to encrypt the voice and data messages, and Diffie–Hellman key exchange algorithm for sharing the keys securely. Figure 2 shows how the encryption process in this initiative [5].

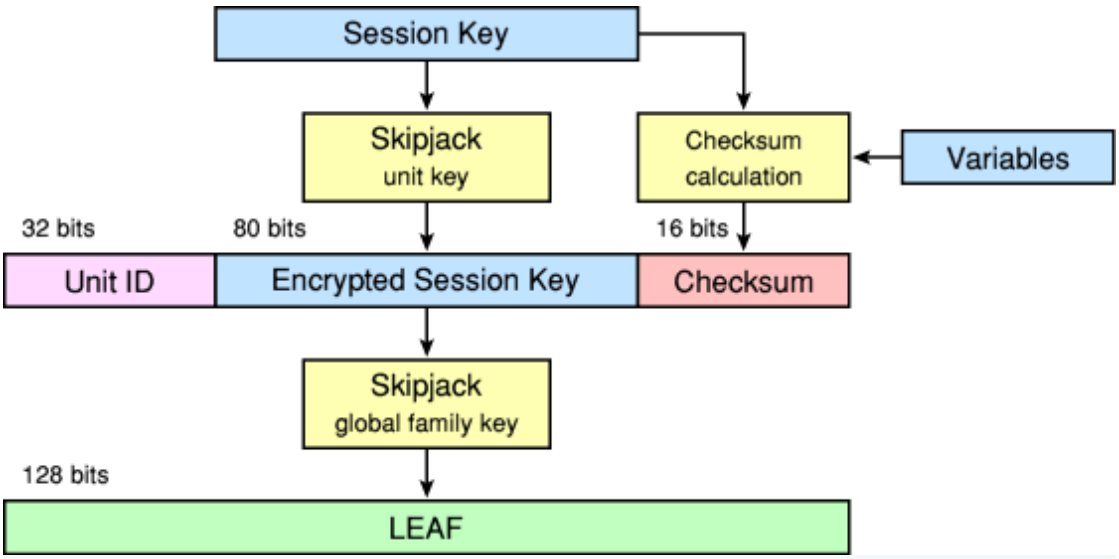

Fig. 2. Encryption Process in Clipper Chip Initiative. [6]

IV. Key Escrow for Cloud Users

When cloud customers want to protect their encryption keys, several ways should be taken into consideration by decision-makers:

- **Cloud-Based Encryption:** The Cloud Service Provider (CSP) generates, manages, and stores the keys used to encrypt and decrypt data.
- **Bring Your Own Key (BYOK):** The customer generates and manages encryption keys, but the CSP has access to the keys and can use them to encrypt and decrypt data.
- **Hold Your Own Key (HYOK):** The customer generates, manages, and stores encryption keys in its own environment. The cloud provider does not have access to the keys and is blind to the contents of encrypted files.

Some businesses address all sensitive data using the HYOK method. These businesses only use the Cloud as a place to store data. Sensitive data is stored on cloud servers, but it can only be decrypted and utilized within the company network or by approved third parties.

For at least some of their sensitive data, the majority of enterprises need to use additional cloud capabilities (online collaboration, online search, and cloud Data Leakage Prevention (DLP) scanning).

With cloud-based encryption, HYOK encryption can be used. To enable the full spectrum of cloud services, data that an organization deems appropriate for cloud-based use can be encrypted using keys that the cloud provider maintains. Data that needs the highest level of security can be encrypted using company-owned keys, making the cloud provider unable to decrypt it.

When the cloud services are used 2 main processes based on the data phases shall be encrypted, which are data in transit and data at rest. In the case of data in transit, encryption is relatively straightforward. Transport Layer Security (TLS) or other trusted techniques are almost always used to encrypt data as it travels (between data centers, or between servers and consumer devices). On the other hand and with data at rest, While CSP can encrypt data on its servers, the cloud providers must maintain control over the keys used to encrypt and decode the data in order to enable indexing, online reading, online collaboration, or other services.

Two main examples of where key escrow systems are Full Desk Encryption (FDE) and public keys of Secure Shell Protocol (SSH). When organizations go with FDE protection for the data at rest, they can access the encrypted data through the credentials of the authorized users or through recovery keys which are special, difficult passwords linked to the encrypted drives. When a user needs an SSH key pair to access their cloud infrastructure (such as Amazon Web Services (AWS®)), a public and private key are generated in the public SSH keys. The service that a user uses to log in with their public key manages their private key. SSH keys are frequently more difficult to remember than regular passwords because they tend to be longer and more complicated. Therefore, IT companies might be less concerned about their users losing their SSH key pairs and, as a result, their access to vital, protected resources by employing a key escrow mechanism for the system-stored public keys [7].

When Organizations want to go further with key escrow services, the chosen framework shall consider the following[8]:

- Provide benefits to legitimate users,
- Be public and unclassified,

- Use well known techniques,
- Support all forms of communications,
- Compatible with different laws and regulations,
- Provide access under warrant, and
- Not require to deal with other third parties.

V. Pros of key Escrow Services

From what was shown before, the main advantage of key escrow systems is the recovery of the encrypted data when the keys were lost. The independence of human interactions in key recovery processes when the key escrow systems were used reduces the risks of human errors that may occur. Key escrow systems may lead to an increase the national security by having transparency to the encrypted data, which may be used from the side by criminals and terrorists to hide their malicious behaviors.

VI. Cons of Key Escrow Services

As we all know there is no perfect solution in the information technology world. In this section, we are going to talk about the pitfalls of key escrow services. Trustworthy third parties must provide client information as mandated by law because they operate inside the regulatory framework. It is similar to bank laws in that banks are required to provide the tax authorities with proof of certain financial transactions. The Key escrow agreements could be the weakness that thieves utilize to conceal their nefarious actions.

For the following reasons, it is challenging to implement in multi-domain frameworks (despite being simple for a single domain): For each domain, one escrow agent, various regulations in each domain, and insufficient faith between the realms.

Lack of confidence in the structural escrow arrangement's security is another disadvantage of using key escrow systems. Moreover, they may expose businesses to new dangers. The following points are some of the new risks that arise when organizations decide to go with key escrow solutions.

- Improper disclosures of keys. As you know we lose any secret if we share it with more than two people.
- Theft of valuable key information even in storage on these solutions' infrastructure or in transit of these keys.
- Failure to comply with law enforcement demands.
- Insider abuse to the stored keys from the side of key escrow service providers.
- As we mentioned before, governments may access to these data, and because of corruptions and abuse of powers protected data can be be compromised, which leads to security violations for individuals, companies, or even the entire nations.
- going with key escrow solutions lead to new kind of attacks:
    - Theft of recovery agent’s own private keys may lead to broader array of communications,

- Key recovery infra is a valuable targets for attackers.

Beside the mentioned risks, we shall not forget that escrow solutions are cloud based systems, which means that risks of migrating to cloud solutions exist. The following points are some of the risks of migrating to cloud solutions [9]:

- Risks of private clouds such as personnel risks, natural disasters, external attacks, non compliance to regulations and malware infections.
- Vendor lock-in. when it is not feasible to move to another CSP because of technical or nontechnical restrictions.
- Vendor Lock-out. when the CSP go out the market.
- Risks of Software as a Service (SaaS) service models, such as property formats, virtualizations, and web application security.
- Other threats such as escalation of previledges, internal/external threats, contractual failures, theft/lost of devices, loss of policy controls, loss of physical control, lack of audit access, and rogue admin.
- Risks of improper key destruction on the cloud.

Nevertheless, new open issues may arise when organizations decide to go further in key escrow services. One of these issues is increase in operational, product design, government oversight, and even user costs. In designing such a solution, the highly scalability shall be taken into considerations since [5]:

- More than 800 encryption product,
- Thousands of agents all over the world,
- About 17,000 different local, state, and federal law enforcement,
- Millions of users, and
- Tens of millions (or more) public-private key pairs.

VII. Comments about the Shown Information

In this section, comments about the shown information in this paper are going to be shown.

- Dealing with the encryption keys manually is a bad decision that cloud users may take, because of the high probability of losing access to the encrypted data because of the inability to recover the lost keys. From that point of view, key escrow services shall be used to save the recovery keys of the companies.
- National security for countries is important but using key escrow services to access the encrypted data of users in case of suspicion of malicious behaviors is not the solution, the keys shall be protected by the key escrow services, and if there is a suspicion of any criminal behavior, the disclosure shall be by judge order and with notifying the user about this disclosure. From that point of view, extra efforts about the regulations shall be done to insure the protection of the privacy of users with this transparency.
- Before going further in any agreement related to key escrow services, compliance with the standards between the two parties shall be studied to avoid the risk of non-compliance with the standards that each party follows.

- Similar to any participation in cloud services, several issues shall be taken into consideration. For example, ensuring favorable contract terms for portability, avoiding propriety formats, ensuring no physical limitations to moving, and checking for regulatory constraints to avoid vendor lock-in risks. Other things shall be taken into consideration which are provider longevity, core competency, jurisdictional suitability, apply chain dependencies, and legislative environment for avoiding or reducing the risks of vendor lock-out.
- In the contractual phase between the customers and key escrow services, all the processes of key handling shall be documented; such as transmitting the keys to the service providers, the ways to store these keys on the local infrastructure, the ways to destroy these keys in case of expirations, and the ways to handle the keys for authorities and notifying the customer about that behavior.
- Since encryption keys are considered highly sensitive data regular audit activity shall take place from the side of the service provider, and System Organization Control (SOC) version 3 type 2 shall be provided to their customers, to confirm compliance with the security controls based on the availability, processing integrity, confidentiality, and privacy principles.
- Avoiding storing the encryption keys with the encrypted data in the same cloud environment is important to reduce the probability of unauthorized access to the encrypted data. This is similar to having protection gates to the houses but keeping the keys on these gates.

VIII. Conclusion

In this work, we studied one of the new solutions that came with the need to encrypt the data with the usage of cloud solutions, which are key escrow solutions. Key escrow solutions can reduce the probability of losing access to the encrypted data because of losing the decryption keys. However, the main concern with these kinds of solutions is the abuse of these solutions which may lead to critical data disclosure. There shall be a tradeoff between the privacy and protection of the population against serious crimes, and also a tradeoff between security and trusted third parties to store the encryption keys.

Cloud customers are the only ones legally responsible for protecting their customers’ data that they have, so before going further in any key escrow arrangement they have to heavily check the key escrow providers.

Regulatory requirements that key escrow providers shall be checked before going further in any agreement, since these regulations may expose the customers' data to authorities that may not be preferable to be exposed based on the customers' regulations.

Acknowledgements

Many thanks to Prof. Baris Celiktas for his efforts in teaching Security in Cloud subject.

References

1. ^*scrambox. How long would it take to brute force aes-256? [Online]. Available: https://scrambox.com/article/brute-force-aes/*
2. ^*W.P.D.R. Kuhn, V. Hu and S.Chang,"Sp800-32.introduction to public key technology and the federal pki infrastructure." 2001.*
3. ^*J. Moses, "Key escrow encryption: Would it have saved the day?, global information assurance certification paper," SANS Institute, vol. 1.2f, 2005.*
4. ^*M. Smid, "Escrowed encryption standard, federal inf. process. stds. (nist fips), national institute of standards and technology, gaithersburg, md," NIST, 1994.*
5. a, b*S. B. J. B. M. B. W. D. J. G. P. N. R. R. J. S. H. Abelson, R. Anderson and B. Schneier, "The risks of key recovery, key escrow, and trusted third-party encryption." O'Reilly & Associates, Inc, 1997.*
6. ^*cryptomuseum. Clipper chip, cryptographic key escrow. [Online]. Available: https://www.cryptomuseum.com/crypto/usa/clipper.htm*
7. ^*Z. DeMeyer. (2019) What is key escrow? – store cryptographic keys – jumpcloud. [Online]. Available: https://jumpcloud.com/blog/key-escrow*
8. ^*P. M. Hoyle and C. Mitchell, "On solutions to the key escrow problem," Springer, pp. 277–306, 1998.*
9. ^*B. Celiktas, "Lecture notes of security in cloud subject (domain 5)," Isik University, 2022.*