Journal of Electronics and Information Science (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2025.100113
ISSN 2371-9524 Vol. 10 Num. 1

Design of a Cloud-Based Decryption Architecture for Malicious Information

Kunpeng Cao[1], Leyi Zhang[1], Guobing Jiang[2]

[1]State Key Laboratory of Mobile Network and Mobile Multimedia Technology, Shenzhen, 518055, China
[2]ZTE Corporation, Nanjing, 210012, China

Keywords: Encrypted Malicious Information, Cloud Architecture, Decryption As A Service

Abstract: Network security protection focuses on ensuring the confidentiality, integrity, and availability of protected assets. Encryption is always the core technology to protect asset confidentiality, and encryption files can be decrypted mostly by using decryption keys. With the advancement of encryption technologies, attackers also skillfully utilize the inherent characteristics of encryption algorithms, which are difficult to crack. They transmit illegal and malicious information in a concealed manner and spread it extensively across the Internet. Nowadays, the traditional protection means are often misused by attackers to disseminate harmful information. This raises significant concerns about how to mitigate the negative impact of storing and transmitting illegal information on both organizations and society as a whole, which is a pressing issue in the field of cybersecurity. In light of the growing use of cloud computing technology, this paper proposes an architectural solution to efficiently decrypt illegal and malicious information, and interprets the business flow, which provides a new direction for entities to share decryption tools and techniques to the maximum extent.

1. Introduction

Confidentiality, integrity, availability, commonly referred to as CIA, are the basic security attributes of protected assets. For key and sensitive assets, their confidentiality traits often involve significant decisions and interests of individuals, organizations, and even countries. Therefore, the protection demands are relatively high, and encryption frequently becomes the primary method of safeguarding this information. However, encryption is also a double-edged sword. On the one hand, it protects important and sensitive data. On the other hand, it can also enable criminals to conceal or illegally transfer malicious information to avoid security supervision. In 2007, when the US Customs found child pornography on Sebastian Boucher's laptop, the laptop was seized as an evidence and he was charged with transporting the pornography across borders. When examiners tried to access the hard drives of the laptop, they failed due to drive encryption. Boucher refused to give the password on the grounds that it violated the Fifth Amendment right against self-incrimination.

Privacy is publicly considered as one of the unique personality needs of individual citizens. However, in some cases, organizations and societies have to strike a hard balance between individual privacy and public safety, so as to ensure that the legitimate interests of most people are not infringed on. Efficiently decoding encrypted data that is suspected to be or already confirmed malicious to

prevent or intercept imminent crimes poses a significant challenge on cybersecurity.

2. Related Work

Currently, the decryption methods are divided into the following categories:

1) Encryption backdoor

An encryption backdoor is a concealed entry point in an encryption system, aiming to facilitate law enforcement agencies, governments, or other authorized parties to bypass pre-defined identity proofing procedures and access encrypted data when necessary. As mentioned in [1], the Clipper chip developed and promoted by the U.S. National Security Agency (NSA) in 1993 is an example of encryption backdoor. This concept was heavily resisted in the industry, which was never started and disappeared within a few years. However, in the subsequent periods of time, some government officials and law enforcement agencies inside and outside Europe still promoted the so-called encryption backdoors to assist in cybercrime investigation[2]. Actually, encryption backdoors often mean weak cipher technologies, which are very easily cracked and are therefore not recommended.

2) Key escrow

Key escrow is a commonly used technology in community supervision. In accordance with the traditional convention, law enforcement agencies usually retrieve keys from service providers to monitor and handle suspicious communications as required [3]. This process is effective only if the target users use the keys provided by the service provider for their communications [4][5]. However, due to mistrust on the providers, some cautious users may opt for alternative keys that are privately agreed with the peer end for communications. This practice can make it more challenging for third parties to decrypt the encrypted data.

3) Extraction of keys from RAMs

Almost all cipher keys used in communications are stored in RAM, where they are typically stored encrypted and are only decrypted at runtime in RAMs when needed for cryptographic operations[6]. Extracting cipher keys from RAMs is therefore a newly proposed cracking method in digital forensics[7]. However, this method requires additional legal authorization in advance, and needs to intrusively access target devices. Moreover, the allowed operation time is very limited, making it a challenging task. If a large number of community users need to be supervised, the cost-effectiveness ratio is not appropriate.

4) Shared decryption platform

The shared decryption platform mentioned in [8][9] is a novel development arising from the shared economy. Such an innovative decryption platform provides significant support for both Europol in collecting cybercrime evidence and assists various EU organizations in alleviating the challenges posed by Ransomware attacks. The details of its technical implementation have not been released yet.

By combing the philosophy of the shared decryption platform with the cloud computing technology, this paper innovatively proposes an operating architecture for decryption and explains working processes with the aim of maximizing the sharing of advanced decryption technologies, tools, and knowledge across the industry. This approach successfully explores a new direction for individuals and organizations to access decryption services in a secure and efficient manner.

3. Cloud-Based Decryption Architecture Solution

3.1 Design Logic

Decryption as a Service (DaaS) is designed to provide secure, reliable, and instant decryption for multiple tenants. It virtualizes a specific number of physical decryption machines to create Virtual Decryption Machines (VDMs), which are logically infinite and can be dynamically allocated based on

the principles of “product sharing, resource pooling, and virtual allocation”, see Fig. 1. For the DaaS, tenants receive decryption services from one or more VDMs through the decryption service platform. Each VDM operates independently from each other.

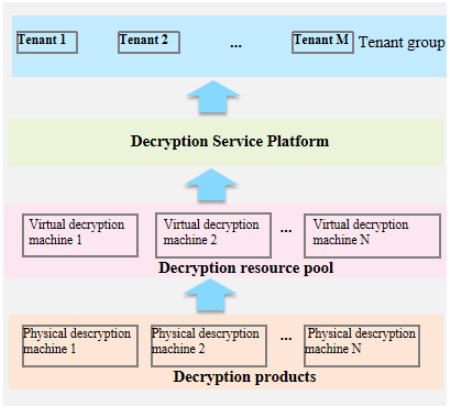

Fig. 1. DaaS Logic

3.2 Overall Architecture

Fig.2 shows the overall architecture of DaaS, which consists of four sub-layers: the infrastructure layer, the resource layer, the service layer, and the presentation layer.

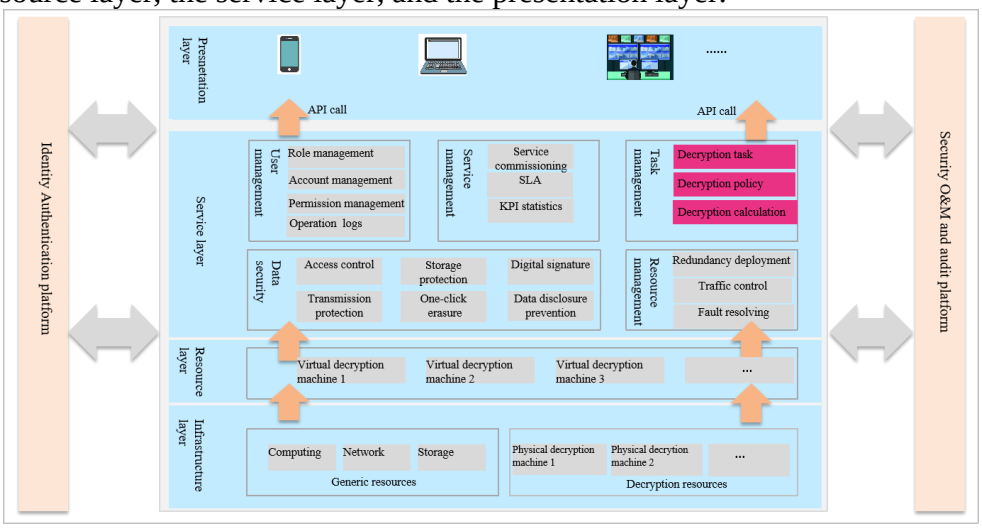

Fig. 2. DaaS Architectu

1) Infrastructure layer

It includes essential computing resources, network resources, storage resources, and physical decryption machines running the core decryption function.

2) Resource layer

Multiple VDMs operate by utilizing the hardware facilities at the infrastructure layer. When a tenant subscribes to the decryption service and applies for the first time, one or more dedicated VDMs are created for it. After the decryption service ends, the VDMs are permanently released once the tenant confirms or logs out. If the tenant exits during the decryption process, the VDMs enter sleep mode and can be re-activated after the tenant logs in again.

3) Service layer

It consists of five modules: user management, service management, task management, data security, and resource management. The user management module is responsible for role management, account

management, permission management, and management of operation logs which record all actions take by administrators, operators, and tenants. The service management module covers decryption service provisioning, SLA settings, and KPI statistics related to service quality. The task management module serves as the core of the service layer, including the setup of decryption tasks, customization of decryption policies, and decryption calculation. The data security module focuses on access control and storage protection for originally encrypted data and decrypted data, digital signatures including timestamps for decrypted data, transmission protection for originally encrypted data and decrypted data, and one-click erasure and data disclosure prevention. The resource management module ensures the business continuity of the decryption service, including redundant deployment of key functions, traffic control for data upload and download, and fast recovery upon faults.

4) Display layer

Decrypted data is called through APIs and is displayed in accordance with the user-defined style, such as APPs, terminals, and supervision screens.

In addition to the sub-layers, the identity authentication platform provides a centralized login portal and authentication service to implement identity authentication on administrators, operators, and tenants. It also assigns corresponding permissions based on user roles and responsibilities, effectively managing the access and use of cloud decryption resources. The security operations and maintenance (O&M) and audit platform monitors and alerts important indicators, such as network traffic and device status, in real time, It also regularly audits user operations and file access records. Both the unified identity authentication platform and security O&M and audit platform collaborate with the core components of the architecture to provide tenants with a secure and reliable DaaS.

3.3 Technical Principles of VDM

In DaaS, the core decryption process is executed by multiple VDMs virtualized from physical decryption machines. Fig. 3 shows the composition of a VDM. Each VDM consists of six modules: sandbox, identity proofing, decryption policy management, decryption task/operation unit, decryption information management, and decryption knowledge base. Although VDMs are isolated from each other, they simultaneously share hardware resources of the physical decryption machines. After a tenant is successfully registered and gets the decryption permission, DaaS dynamically provides one or more dedicated VDMs for the tenant in accordance with the number of files to be decrypted, decryption policy, and expected deadline. Throughout the entire service period, DaaS ensures the protection of decrypted information..

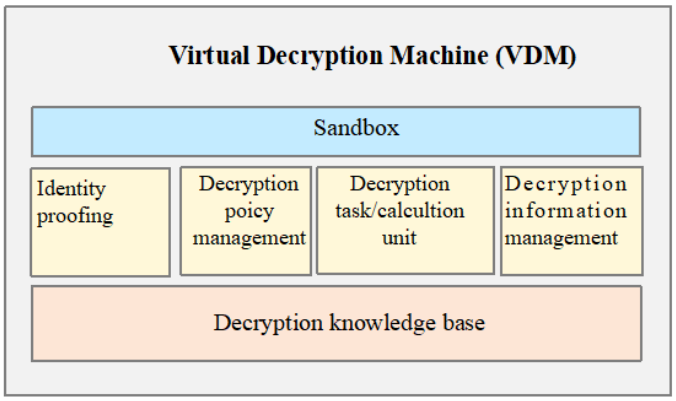

Fig. 3. VDM Composition

1) Sandbox module

Encrypted files from known or unknown external sources may contain viruses or other malicious

programs. To prevent internal programs of DaaS from being infected, the original encrypted files are transferred to sandbox for isolation after uploading. Follow-up decryption operations are all executed in the sandbox.

2) Identity proofing module

This module authenticates the validity and authenticity of tenants by using the Multi-Factor Authentication (MFA) technology. Once authentication is successful, VDMs are allocated in accordance with tenant requirements. A tenant, once successfully logging in to one VDM, can perform operations across multiple associated VDMs running at the same time. If one VDM has no activity within the specified period, the tenant needs to be re-authenticated upon the second login to the VDM.

3) Decryption policy management module

It provides various decryption policies for tenants, including brute-force cracking, bypass cracking, feature- or encryption source-based matching of known decryption keys, and other special methods. These decryption policies may also include customized or default configurations, and can be updated periodically.

4) Decryption task/calculation unit module

As the core module of DaaS, the decryption task/calculation unit module receives decryption instructions, creates decryption tasks, performs decryption, and produces decryption results, directly determining the decryption speed, quality, and performance. Additionally, this module supports the running of multiple processes at the same time, and visualizes the decryption process and status.

5) Decryption information management module

To prevent sensitive information from being disclosed or tampered with during decryption, the decryption information management module provides security protection for decrypted information by using various means like access control, encryption, data masking, and digital signatures.

6) Decryption knowledge base module

This module stores available decryption technologies and information that have been reliably retrieved from legal and authorized channels, so as to maximize the reuse of industry-wide historical decryption knowledge. For example, when dealing with a file encrypted due to Ransom infection, the virus type (such as AES_NI Ransom and Aura Ransom) can be roughly identified in accordance with the suffix or other known features of the encrypted file, and the publicly known decryption key is further searched in the decryption knowledge base module for accurate cracking [10].

3.4 Business flow

1) Step 1-2: The user initiates an authentication request. The identity authentication platform of DaaS matches the identity information carried in the request against that stored in the database, and returns the authentication result.

2) Step 3-5: If the authentication is passed, the identity authentication platform further sends a request to the permission management module, asking for permissions including decryption. After assessment, the permission management module returns the permission enabling result (success or failure).

3) Step 6-8: If the decryption permission is enabled, the user can configure the decryption policy in accordance with his or her personalized requirements to initialize decryption parameters.

4) Step 9-12: Decryption begins, and the corresponding information is searched and matched in the decryption knowledge base. After a series of decryption calculation, the decryption result is returned to the user over encrypted connection, and is then displayed using the pre-defined style.

Fig. 4 demonstrates the whole business flow of DaaS.

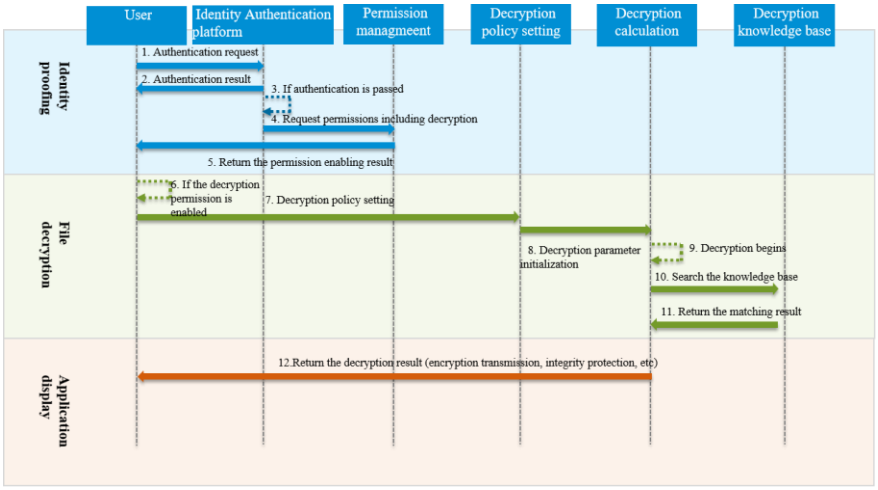

Fig. 4. Business Flow of DaaS

4. Conclusion

This paper designs a cloud-based decryption architecture solution, aiming to enable unified decryption resource management through the virtualization and dynamic scheduling of decryption resources, so as to efficiently provide professional on-demand decryption services for users. It can be foreseen that, as malicious information becomes increasingly concealed due to the emergence of diverse and complex network attack technologies, decryption demands arising from legal supervision may become urgent. Consequently, developing advanced decryption technologies and methods that can be accessed by users across countries and regions will be crucial for the efficient sharing of knowledge of global cybersecurity experts. This will become an important exploration direction for the future evolving of DaaS.

References

[1] J. Liu, M. D. Ryan and L. Chen, "Balancing Societal Security and Individual Privacy: Accountable Escrow System," 2014 IEEE 27th Computer Security Foundations Symposium, Vienna, Austria, 2014, pp. 427-440, doi: 10.1109/CSF.2014.37.

[2] https://www.databreachtoday.asia/strong-crypto-policing-eu-again-debates-encryption-a-15392

[3] S. Yoon, J. Jeong, H. Jeong and Y. Won, "Lawful Interception Scheme for Secure VoIP Communications Using TTP," International Symposium on Computer Science and its Applications, Hobart, TAS, Australia, 2008, pp. 149-152, doi: 10.1109/CSA.2008.31.

[4] P. Bharadwaj, H. Pal and B. Narwal, "Proposing a Key Escrow Mechanism for Real-Time access to End-to-End encryption systems in the Interest of Law Enforcement," 2018 3rd International Conference on Contemporary Computing and Informatics (IC3I), Gurgaon, India, 2018, pp. 233-237, doi: 10.1109/IC3I44769.2018.9007301.

[5] G. Ungaro, F. Ricchitelli, I. Huso, G. Piro and G. Boggia, "Design and Implementation of a Lawful Interception Architecture for B5G Systems Based on Key Escrow," 2022 IEEE Conference on Standards for Communications and Networking (CSCN), Thessaloniki, Greece, 2022, pp. 207-207, doi: 10.1109/CSCN57023.2022.10050895.

[6] Christian Lindenmeier, Andreas Hammer, Jan Gruber, Jonas Röckl, Felix Freiling,Key extraction-based lawful access to encrypted data: Taxonomy and survey, Forensic Science International:Digital Investigation,Volume 50,2024,301796,ISSN 2666-2817,https://doi.org/10.1016/j.fsidi.2024.301796.

[7] K. Hausknecht, D. Foit and J. Burić, "RAM data significance in digital forensics," 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2015, pp. 1372-1375, doi: 10.1109/MIPRO.2015.7160488.

[8] https://www.tandfonline.com/doi/full/10.1080/14782804.2021.1995707?scroll=top&needAccess=true#abstract

[9] https://www.europol.europa.eu/media-press/newsroom/news/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-ransomware

[10] https://www.nomoreransom.org/en/decryption-tools.html