# CSPM: Metamodel for Security and Privacy Knowledge in Cloud Services*

Hironori Washizaki, Sota Fukumoto, Misato Yamamoto, Masatoshi Yoshizawa and Yoshiaki Fukazawa
Waseda University
washizaki@waseda.jp

Takehisa Kato
Toshiba Corporation
takehisa.kato@toshiba.co.jp

Haruhiko Kaiya
Kanagawa University
kaiya@kanagawa-u.ac.jp

Shinpei Ogata
Shinshu University
ogata@cs.shinshu-u.ac.jp

Eduardo B. Fernandez
Florida Atlantic University
fernande@fau.edu

Hideyuki Kanuka and Yuki Kondo
Hitachi, Ltd.
hideyuki.kanuka.dv@hitachi.com

Takao Okubo
Institute of Information Security
okubo@iisec.ac.jp

Nobukazu Yoshioka
National Institute of Informatics
nobukazu@nii.ac.jp

Atsuo Hazeyama
Tokyo Gakugei University
hazeyama@u-gakugei.ac.jp

## ABSTRACT

It is important to ensure security and privacy in cloud services. Although there are many security and privacy patterns as well as non-pattern-based knowledge such as practices and principles in cloud services, it is difficult to select and combine the right ones due to the vast volume of such items and the nature of the layered cloud stack. Herein we propose a metamodel called the Cloud Security and Privacy Metamodel (CSPM) to handle security and privacy in cloud service development and operations. CSPM can be utilized to classify and reuse existing cloud security and privacy patterns and practices in a consistent and uniform manner. Moreover, CSPM can also be used to design and maintain cloud service systems incorporating security and privacy. In a case study to model a cloud service, we confirm that CSPM is useful to consistently design services with applications of various security and privacy knowledge over different layers.

## CCS CONCEPTS

•**Computer systems organization** → **Cloud computing;** •**Software and its engineering** → **Software architectures; Design patterns;** •**Security and privacy** → Systems security; Software security engineering;

## KEYWORDS

Cloud computing, security patterns, privacy patterns, software and system architecture

**ACM Reference format:**
Hironori Washizaki, Sota Fukumoto, Misato Yamamoto, Masatoshi Yoshizawa and Yoshiaki Fukazawa, Takehisa Kato, Haruhiko Kaiya, Shinpei Ogata, Eduardo B. Fernandez, Hideyuki Kanuka and Yuki Kondo, Takao Okubo, Nobukazu Yoshioka, and Atsuo Hazeyama. 2017. CSPM: Metamodel for Security and Privacy Knowledge in Cloud Services. In *Proceedings of 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, August 2017 (ARES 2017),* 6 pages.
DOI: 10.475/123_4

*The background and the former version of the metamodel described in this paper were presented at [1, 2]. Here an extended metamodel along with its case study are described.


*ARES 2017, Reggio Calabria, Italy*

DOI: 10.475/123_4

## 1 INTRODUCTION

Because service providers centrally control services and data, which are remotely available and often connected with other services [3], ensuring security and privacy in cloud services is particularly important. However, not all software engineers are experts on security and privacy (S&P) [4], making it is difficult to incorporate a variety of S&P concerns in various software lifecycle stages.

A pattern is an abstraction from a concrete form that recurs in non-arbitrary contexts. Pattern catalogs (and pattern languages as well) should enable the coherent integration and presentation of the relevant background, leitmotif, and metaphors [5]. In the area of cloud computing and

services, many security and privacy patterns have been published [6–11]. Moreover, non-pattern-based knowledge in the form of practices and principles has been well documented to address security and privacy issues in cloud services.

The vast number of S&P patterns and documents describing related knowledge in cloud services makes the selection (and combination) of the right ones difficult. This problem is common to security patterns in general [4, 12, 13], but is more severe in cloud services due mainly to the following two reasons. First, cloud services and their underlying mechanisms are related to various layers in the layered stack of cloud [14] and often integrated over different layers [3]. Second, a variety of devices are connected to cloud computing systems, which may require different deployment models and diverse services, resulting in a highly complex system [15]. This leads to many concerns, including S&P.

Metamodels or reference architectures that capture the essential concepts related to S&P in the layered stacks of cloud should address the aforementioned problem since engineers can describe security and privacy-related knowledge as well as design systems and services using knowledge consistently over different layers. Although several metamodels [15, 16] and abstract reference architectures [17] address cloud security, none of these addresses privacy in cloud services. Since the relation between security and privacy is complex [18], it is preferable to deal with S&P simultaneously. On the other hand, there are several metamodels and conceptual models to address both S&P [19, 20], but they are generally defined in such a way that makes applying them directly to cloud services difficult.

Thus, we propose a metamodel called "Cloud Security and Privacy Metamodel (CSPM)" to address S&P in cloud services by integrating and extending existing cloud security metamodels together with newly added concepts. Figure 1 shows how CSPM would be used in cloud services development and maintenance. CSPM provides the basis to describe and accumulate security and privacy-related knowledge over different layers, making it easier to select and combine the right patterns and related knowledge to address S&P issues in cloud services. Moreover, engineers and developers can refer to CSPM to design high-level architectures of cloud service systems efficiently and effectively. To confirm the usefulness and feasibility of CSPM, we conducted a case study that models a cloud service with a privacy pattern and related knowledge based on CSPM.

The remainder of this paper is organized as follows. First, we propose our metamodel in Section 2. In Section 3, we describe the case study. Finally, we conclude our work and discuss the future direction in Section 4.

## 2 CLOUD SECURITY AND PRIVACY METAMODEL (CSPM)

Based on the information described in Section 1, we identified the following three requirements for designing the metamodel:

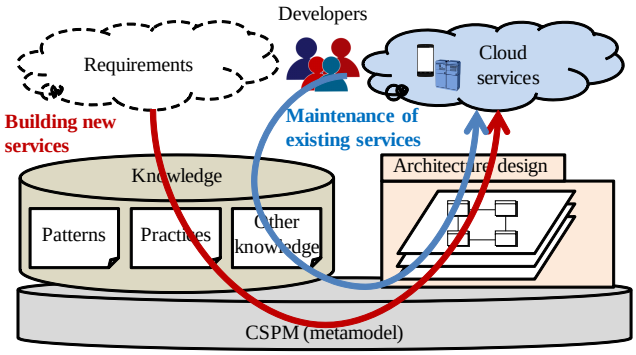


**Figure 1: Overview of the metamodel and cloud services**

- R1. The metamodel must consistently deal with security and privacy-related knowledge over different layers, including the software application layer, the platform layer, and the infrastructure layer. Services corresponding to these layers are SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). From the user's viewpoint, each service is provided at a certain layer; however, the data controlled by the service may be related to any layer [14]. Moreover, cloud services are often integrated over different layers so that careful consideration of security over different layers is important [21]. This is also important for privacy.
- R2. The metamodel has to be mostly consistent with existing cloud security metamodels and reference architectures so that engineers and developers can utilize assets based on our metamodel and those based on existing metamodels (and reference architectures).
- R3. The metamodel allows engineers and developers convenient access to a knowledge base containing cloud-specific and cloud-independent knowledge. For example, there are many S&P patterns that are not specific to cloud services [22, 23], which can be applied to or support cloud service development.

We designed CSPM to consist of seven packages. Its overview is shown in Fig. 3 illustrating six packages with a special package (i.e., "Target") that combines all packages.

Moreover, Fig. 3 describes details of CSPM in the form of UML class diagram. Table 1 describes the outline and major concepts of these packages. The metamodel satisfies the above requirements as follows:

- The problem, bridge, and solution packages capture concepts common to all layers, and organize their relationships. Using these packages as a foundation for all layers yields consistent handling of security and privacy-related knowledge over different layers. This satisfies R1.

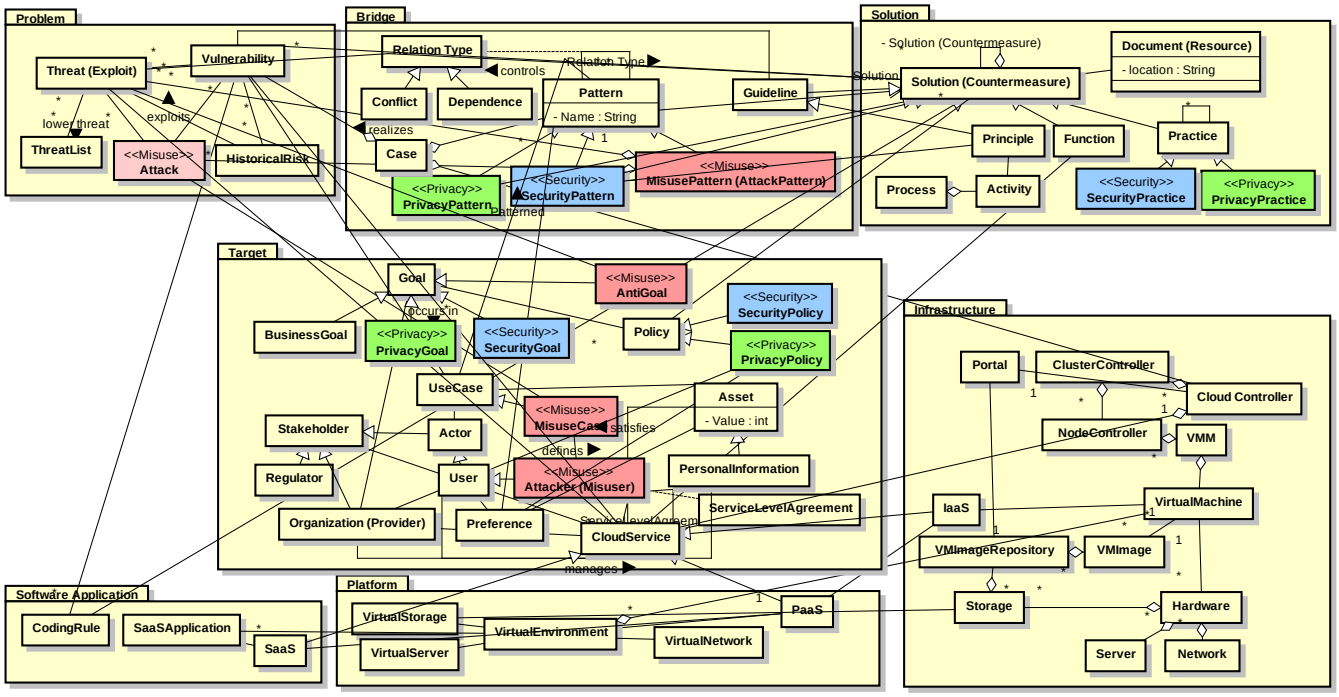


**Figure 3: Details of metamodel**

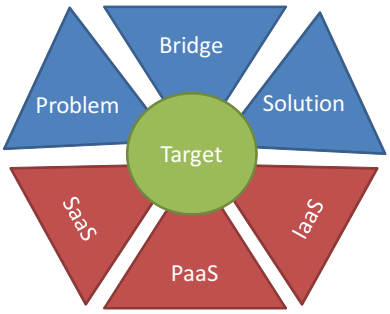


**Figure 2: Overview of metamodel for security and privacy in cloud services**

- The aforementioned common packages incorporate the most of concepts with relationships defined in existing metamodels [15, 16], so that the entire metamodel is mostly consistent with existing metamodels. This satisfies R2.
- By separating general concepts in the problem, bridge, and solution packages from those specific to a certain layer, cloud-specific and cloud independent knowledge is easier to access. This satisfies R3.

**Table 1: Packages in the metamodel**

| Package | Outline | Major concepts |
|---|---|---|
| Problem | Common concepts for problems | Threat, vulnerability, attack |
| Bridge | Concepts on the relationships between problems and their corresponding solutions | Pattern, case, guideline |
| Solution | Common concepts for solutions | General solution (i.e., countermeasure), security function, practice |
| Application | Concepts specific to the software application layer | Application, coding rule |
| Platform | Concepts specific to the platform layer | Virtual environment, virtual storage |
| Infrastructure | Concepts specific to the infrastructure layer | Virtual machine, hardware |
| Target | Concepts specific to the target application | Goal, policy, asset, cloud service |

## 3 CASE STUDY

To confirm the usefulness and feasibility of CSPM, we conducted a case study of modeling a cloud service with applications of various S&P knowledge over difference layers. Let's assume that the service provider has a privacy goal of "protecting the confidentiality of personal information" and has established a corresponding privacy policy. Regarding the goal and the policy, developers could specify a misuse case (i.e., actions to harm the system) as "unauthorized access to personal information". Figure 4 shows the structure of the problematic design of the service without any security function based on CSPM, while Fig. 5 shows its corresponding behavior.

By referring to existing knowledge sources such as S&P pattern catalogs, developers find that a privacy pattern of "encryption with user-managed keys" [11] can protect the service from the misuse. The application of the pattern requires developers to consistently adopt a set of necessary knowledge and elements over different layers such as "encryption" as a security function, "generating a strong encryption key" as a guideline and code for generating the key as a coding rule. Figure 6 shows the structure of the design of the service with the application of the pattern and the related knowledge as instances of concepts in CSPM, while Fig. 7 shows its corresponding behavior. Fig. 6 and 7 are shown in the form of standard UML class diagram and sequence diagram, respectively.

These figures show that the confidentiality of personal information is protected by encryption and decryption. Moreover, we confirmed that the necessary elements involved in the pattern and their relationships over different layers can be clearly and consistently modeled by instantiating CSPM. Using CSPM, developers and engineers can easily recognize when and how to avoid misuse.

## 4 CONCLUSION AND FUTURE WORK

We proposed a metamodel, CSPM, to address security and privacy in cloud services and implemented a simple case study. We plan to conduct more complex case studies such as integrating many S&P patterns, designing cloud service architectures based on CSPM, and implementing them; these cases will be comprehensive and span from requirements to implementation.

## ACKNOWLEDGMENTS

This work was supported by JSPS KAKENHI Grants Number 25330091, 15H02686 and 16H02804, IISF SSR Forum 2015 and 2016.

## REFERENCES

[1] H. Washizaki, et al., "A Metamodel for Security and Privacy Knowledge in Cloud Services," Proc. 12th IEEE World Congress on Services (SERVICES 2016), pp.142-143, 2016.
[2] H. Washizaki, et al., "A Metamodel for Handling Security and Privacy in Cloud Service," Proc. Computer Security Symposium 2015. (in Japanese)
[3] R. F. El-Gazzar, "A Literature Review on Cloud Computing Adoption Issues in Enterprises," IFIP Advances in Information and Communication Technology, Volume 429, 2014, pp 214–242.
[4] N. Yoshioka, H. Washizaki and K. Maruyama, "A Survey on Security Patterns," Progress in Informatics, No.5, pp.35-47, 2008.
[5] D. Riehle and H. Zullighoven, "Understanding and Using Patterns in Software Development," Theory and Practice of Object Systems, Vol.2, No.1, pp.3-13, 1996.
[6] K. Hashizume, N. Yoshioka and E.B. Fernandez, "Misuse Patterns for Cloud Computing," 2nd Asian Conference on Pattern Languages of Programs (AsianPLoP'11) , 2011.
[7] K. Hashizume, N. Yoshioka and E.B. Fernandez, "Three Misuse Patterns for Cloud Computing," in "Security Engineering for Cloud Computing: Approaches and Tools," IGI Global, 2013.
[8] T. Reimer, P. Abraham and Q. Tan, Federated Identity Access Broker Pattern for Cloud Computing, 16th International Conference on Network-Based Information Systems (NBiS), 2013.
[9] E.B. Fernandez, N. Yoshioka, H. Washizaki, Patterns for Security and Privacy in Cloud Ecosystems, 2nd International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE 2015), 2015.
[10] E.B. Fernandez, N. Yoshioka and H. Washizaki, "Cloud Access Security Broker (CASB)," 4th Asian Conference on Pattern Languages of Programs (AsianPLoP 2015), 2015.
[11] N. Doty and M. Gupta, "Privacy design patterns and anti-patterns," Trustbusters Workshop at the Symposium on Usable Privacy and Security, 2013.
[12] K. Supapporn, N. Prompoon and T. Rojkangsadan, "An approach: Constructing the grammar from security pattern," 4th International Joint Conference on Computer Science and Sofware Engineering (JCSSE2007), 2007.
[13] K. Yskout, R. Scandariato and W. Joosen, "Do security patterns really help designers?," International Conference on Software Engineering (ICSE), 2015.
[14] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, Vol.34, No.1, pp.1–11, 2011.
[15] E. B. Fernandez, et al, "Building a security reference architecture for cloud systems," Requirements Engineering Journal, Jan. 2015.
[16] A. Hazeyama, "Survey on Body of Knowledge Regarding Software Security," 13th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD 2012), 2012.
[17] NIST Cloud Computing Security WG, "Cloud computing security reference architecture," 2013
[18] V. Katos and A. Patel, "A partial equilibrium view on security and privacy," Information Management & Computer Security, Vol.16, No.1, pp.74-83, 2008.
[19] C. Kalloniatis, E. Kavakli, S. Gritzalis, "Addressing privacy requirements in system design: the pris method," Requirements Engineering, Vol.13, No.3, pp.241–255, 2008.
[20] R. Tesoriero, et al. "Model-Driven Privacy and Security in Multimodal Social Media Uis," International Workshops MSM 2011.
[21] A.A. Almutairi, M.I. Sarfraz, S. Basalamah, W.G. Aref, A. Ghafoor, "A Distributed Access Control Architecture for Cloud Computing," IEEE Software, Vol. 29, No. 2, pp.36-44, 2012.
[22] E.B. Fernandez, N. Yoshioka, H. Washizaki, et al., "Using security patterns to develop secure systems", in "Software Engineering for Secure Systems", IGI Global, pp16-31, 2010
[23] L.L. Lobato, E.B. Fernandez and S.D. Zorzo, "Patterns to support the development of privacy policies", International Conference on Availability, Reliability and Security (ARES'09), 2009.

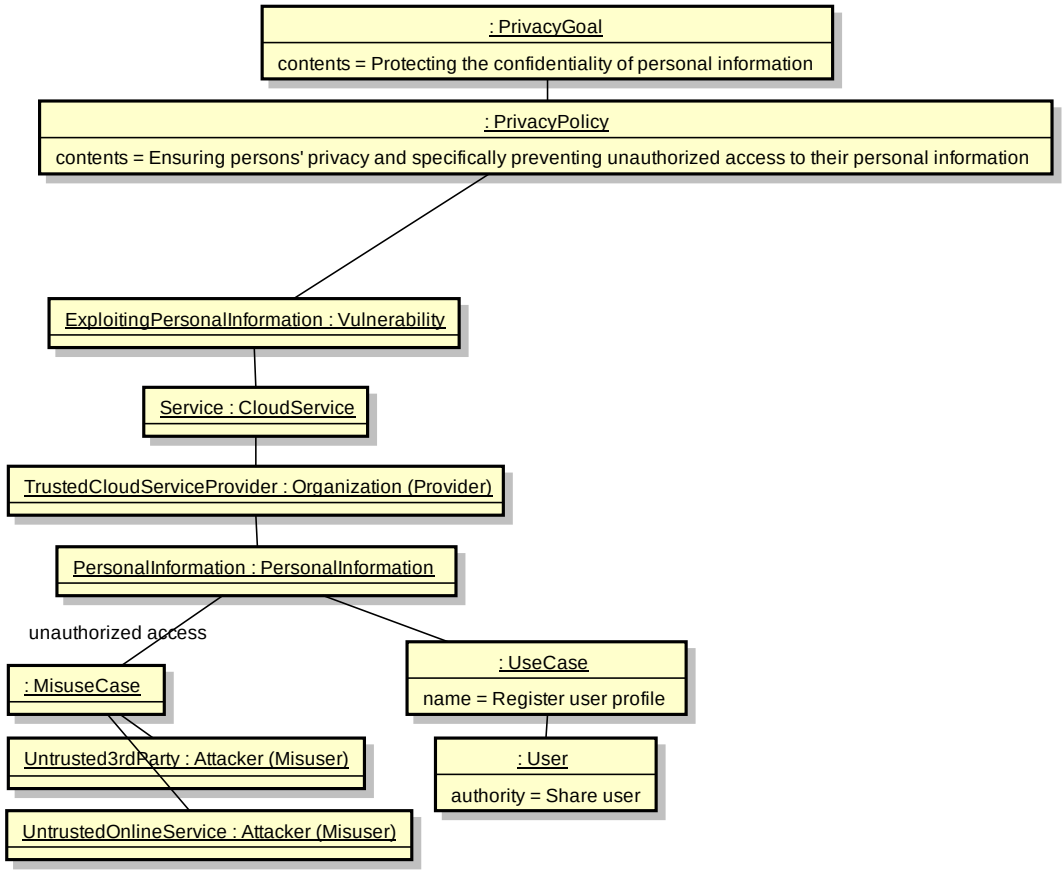


**Figure 4: Structure of a problematic service**

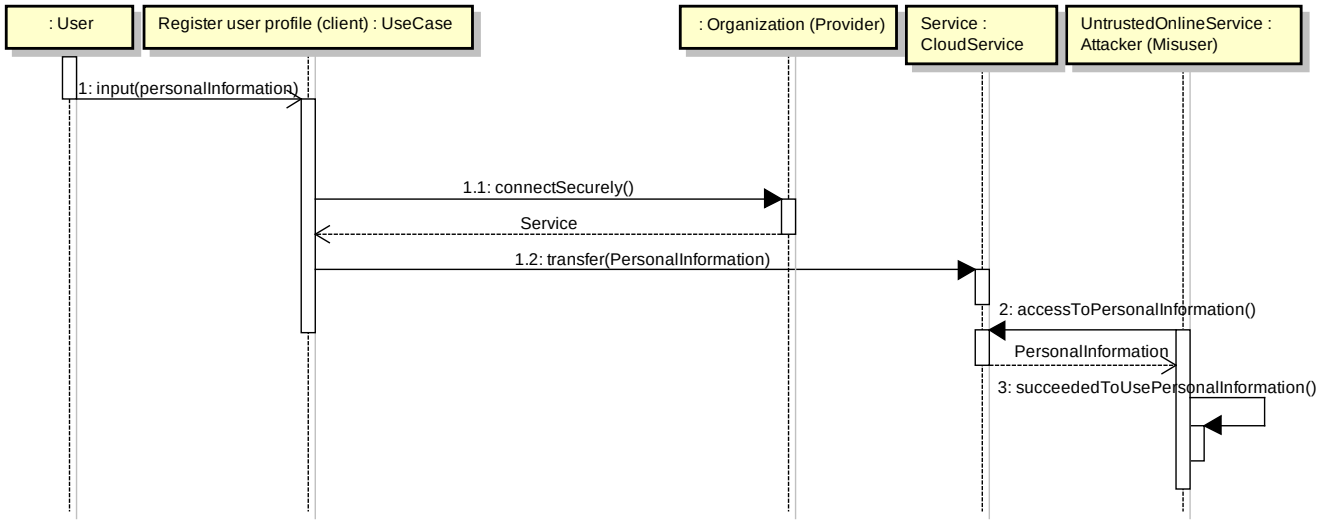


**Figure 5: Behavior of the problematic service**

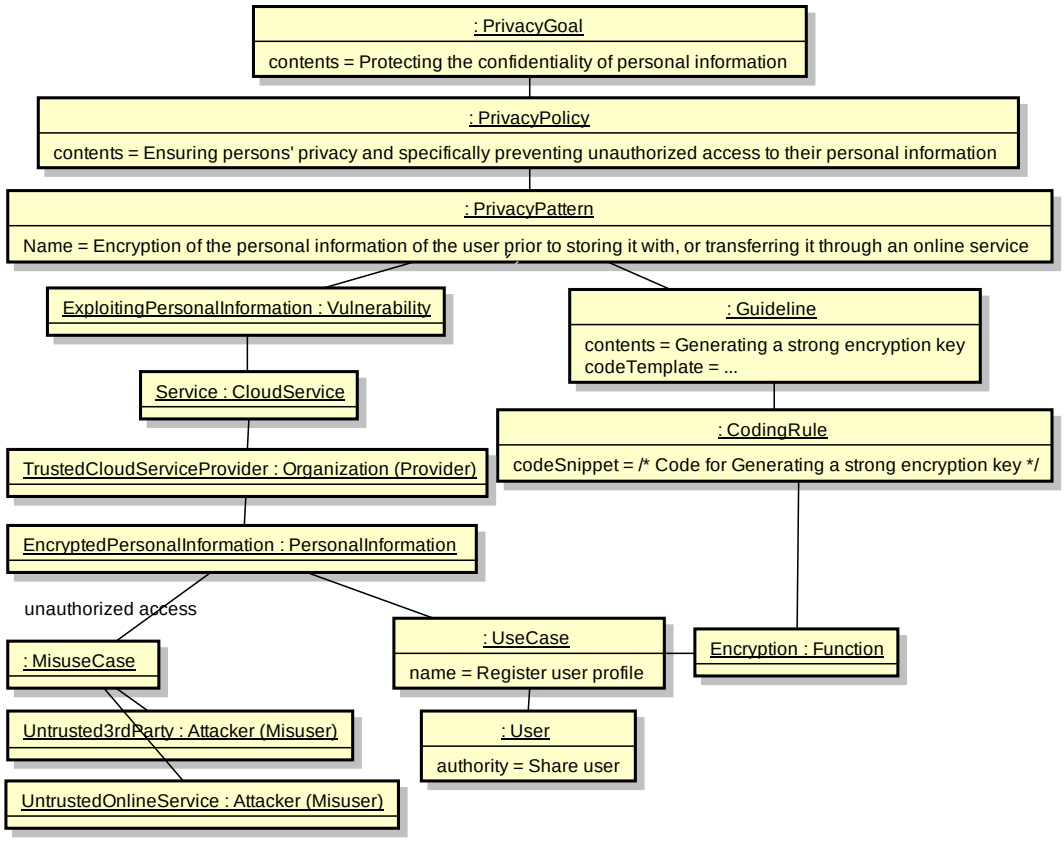


**Figure 6: Structure of the service with encryption and related knowledge**

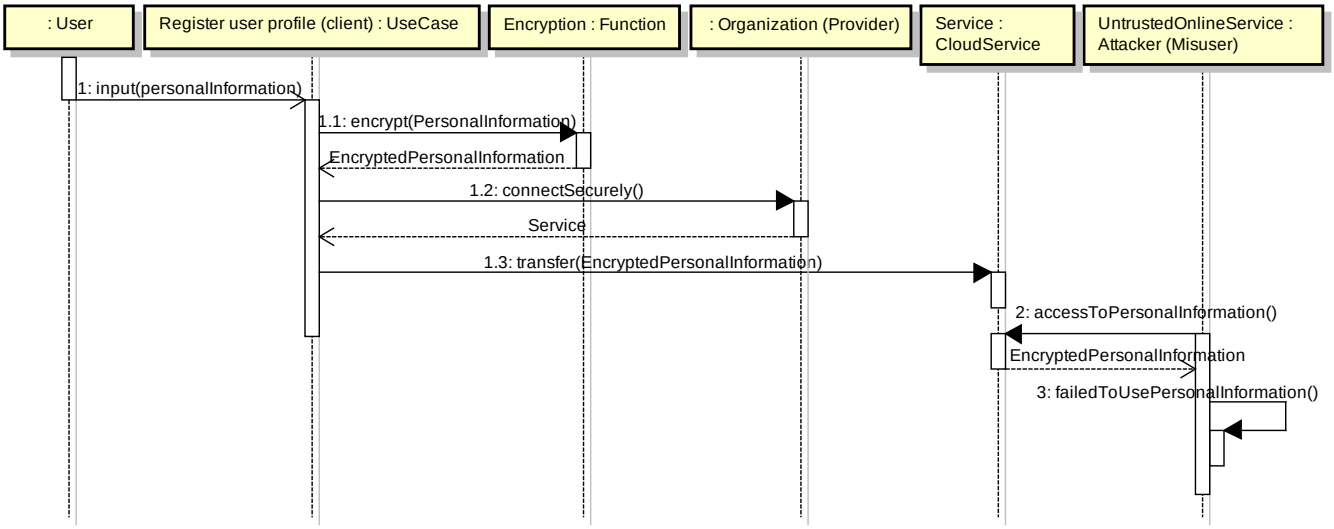


**Figure 7: Behavior of the service with encryption and related knowledge**