UDC 621.391

MECHANISMS OF ENSURING SECURITY IN KEYSTONE SERVICE

I. KUZMINYKH, M. FLIUSTIKOVA

Kharkiv National University of Radio Electronics,
Blekinge University of Technology (BTH)

Abstract *– User authentication is one of the most important aspects in the area of cloud services, followed by the storing of sensitive information about customers. A number of solutions exist for authentication, security, and privacy provisioning in cloud, while cloud identity management systems aim to simplify and harmonise access. This paper presents an investigation into the security problems associated with cloud identity and access management system (IAMS), using the Keystone identity service within OpenStack as an example. In order to analyse the existing challenges, the paper expands security provisioning into authentication management, authorization management, personal data protection, privacy and confidentiality, as well as logging and auditing and considers the security mechanisms required for any cloud IAMS for each one of these categories. The paper also investigates some of the existing and potential attacks against the Keystone service, then follows with recommendations and mechanisms for enhancing the security. The vulnerabilities in cloud IAMS show that most systems support at most a subset of security provisioning mechanisms or have their own flaws; in addition, there are no unified international standards in this cloud identity systems area for cloud and service providers. The identified list of attacks and the associated mitigation mechanisms will help to provide the identity and access management system with the protection of identity credentials in the cloud system. The provided results can help with further researching mechanisms aiming to ensure personal data confidentiality and integrity.*

Анотація *– В хмарних сервісах автентифікація користувача є одним з найважливіших процесів. Збереження конфіденційної інформації про клієнтів – це другий найважливіший процес. Забезпечення безпеки для цих двох процесів є основним питанням в хмарних технологіях. Автентифікація та збереження облікових даних користувача – завдання для системи управління ідентифікацією в хмарних сервісах. У статті представлено аналіз проблем безпеки, пов'язаних з ідентифікацією в хмарних сервісах та системою управління доступом, використовуючи приклад служби ідентифікації Keystone у платформі OpenStack. Основні категорії забезпечення безпеки були класифіковані як управління автентифікацією, управління авторизацією, захист персональних даних, конфіденційність та довіра, а також реєстрування та аудит. Розглянуто механізми забезпечення безпеки у кожній із категорій, необхідні для будь-якої хмарної системи управління доступом. Також було проаналізовано атаки на службу Keystone, як потенційні, так і вже виявлені, і запропоновано механізми підвищення безпеки служб ідентифікації. Практика та уразливості в системі ідентифікації та управління доступом показують, що більшість систем не підтримують всі основні механізми забезпечення безпеки. Жоден із механізмів не забезпечує всіх функцій безпеки; крім того, ще однією проблемою забезпечення безпеки хмарних сервісів є відсутність єдиних міжнародних стандартів у цій сфері для всіх хмарних сервісів та для постачальників послуг. Отриманий список атак та можливі механізми їх усунення допоможуть забезпечити захист особистих даних користувачів в хмарних сервісах та у системі ідентифікації та управління доступом. Надані результати можуть допомогти у проведенні досліджень щодо удосконалення механізмів, що дозволяють забезпечити неможливість несанкціонованого доступу до персональних даних.*

Introduction

With the growing popularity of cloud technologies, protection of personal users data is becoming a core requirement. User identification is the first step to a safe and successful interaction with a web application, service, or software. Proper authentication and authorisation mechanisms help to protect personal data when a user works with a cloud system.

Different Service providers propose different cloud-based solutions and include cloud computing and cloud storage from different cloud providers, such as Amazon, Alibaba Cloud, Google, IBM, Sun, Cisco, Dell, HP, Intel, Novell, and Oracle. One of the typical choices for provisioning such cloud environments is to construct the infrastructure using the OpenStack technology, an open source software for creating public and private clouds.

Similar to any other critical infrastructure software, OpenStack is regularly updated and improved by its developers, with the associated caveat that the changes may introduce variations in interfacing or functionality with the technology. In order to avoid the pitfalls of adapting to new version, infrastructure managers may prefer reinstallation and redeployment of the cloud infrastructure. If services do not provide updates, the outdated vulnerabilities can be used by attackers or malicious users. As part of the regular updates, individual OpenStack services will have specific patches applied, but addressing all the problems across the entire OpenStack architecture is non-trivial task. In this context, the purpose of this paper is to provide a starting point for the updating process by analysing the vulnerabilities of the identity management service and protection mechanisms using the example of OpenStack, more specifically, the Keystone service.

The paper is organised as follows: sections 1 and 2 discuss the complexity of providing security and privacy in an Identity and Access Management System (IAMS) and give an overview of attacks on cloud services. Section 3 gives an overview of the front- and backend Keystone services, including their main functions as well as the typical most common attacks. Section 4 proposes a taxonomy of mechanisms for applying security in authentication, authorization management, personal data protection, privacy and confidentiality, as well as logging and auditing categories. Section 5 provides a summary of the mechanisms for enhancing the security and identifies a number of additional security tools for OpenStack. Based on the combination of security provisioning and enhancing mechanisms introduced, section 6 aggregates the information in a set of recommendations, then the Conclusions section summarises the achievements and limitations of the study.

1. Problem Statement

The concept of cloud identity management aggregates a broad set of tasks, with inherent open security issues, with access and theft of personal data, openness, elevated privileges, confidentiality and integrity of data, or trust management representing typical examples [1]. Currently, applications and service providers are either in the process or have already finalised the migration of their infrastructure to cloud structures, with recent years having witnessed a wide range of cloud service/infrastructure/application providers. Depending on their individual requirements, businesses may prefer to deploy their service on a commercial basis, others deploy the cloud themselves on paid or free resources, some prefer an all-inclusive solutions from the leaders of providing cloud technologies, another companies trust their business to little-known providers with a dubious reputation: there are many solutions. While the size, strength, or reputation of the customer and provider may vary, some of the problems faced by cloud infrastructure are common across the en-

tire range of companies, relating to the common backend technologies that they use for the infrastructures, the lack of standardisation (unification and availability of protocols, specifications, data formats). Standardisation is critical, that is why, in the future, such standards should be developed to ensure scalability and interoperability.

The attacks discussed in the next section demonstrate the level of vulnerability of cloud services, and of the Internet in general, including IAM systems. The pattern of intrusion differs slightly from a standard network attack, as the points of entry tend to be linked to gaps or unprotected access in cloud services. Given the level of exposure and risks, both providers and clients of cloud services must be more considerate towards their security measures to avoid potential loses. In this context, understanding of the weaknesses and security mechanisms in identity and management services is critical step in corporate security provisioning.

2. Literature Review

Almost every company is more or less subject to the attempts of unauthorized access, for a wide range of reasons, from defacement and fun to cybercriminal activities. Typical attacks on cloud services have a wide range of mechanisms and aims: compromise of the authorization process, data theft, authentication keys or encbypassing, encryption hacking; attacks on services in the cloud; attacks on the software, such as virus, backdoor, malware, malicious updates.

Cybersecurity threat reports, IT security reports, business risk reports of different companies such as Nexia [2], Cisco [3, 4], Willis Towers Watson [5], McAfee Labs [6], Ponemon Institute LLC [7, 8], Symantec [9], Kaspersky Lab [10, 11] show that cloud services are the most popular attack surface.

Last report of Ponemon Institute LLC [8] says that the average financial consequence of a cyberattack in 2017 reached $11.7M. The most harmful attacks for enterprises remain malware, web-based and DoS attacks. Kaspersky Lab reports [10] that in 2016 over a third of businesses (38%) have been affected by viruses and malware causing a loss of productivity, and experienced inappropriate IT resource use by employees (36%). One in five (21%) has experienced data loss or exposure due to targeted attacks.

In addition, except direct damage from cyberattack there exist costs to resolve the consequences of the cyberattack like business disruptions, loss of information, loss of revenue and damage to equipment. According to report [8] the information theft remains the most expensive consequence of a cybercrime (43%).

Attackers hack both large and small companies. The goals of unauthorized access to confidential information are different: it can be either personal motives or attempts to earn money. Hacking of large companies, as noticed before, can bring a damage of more than one billion dollars to the organization. Examples of some attacks are listed below.

Cloud Hopper attack is a famous phishing attack in 2017 targeted on service providers with the theft of the customer databases of these service providers, mainly the corporate sector [12, 13].

Drown attack against encryption. The disadvantages of old encryption technologies that have not been fixed by network administrators lead to vulnerabilities and irreparable loss to various companies. Drown attack allows to decrypt the client's TLS traffic, can negatively impact on sites that use a secure https connection for communication. Yahoo, BuzzFeed, Flickr and Samsung.com could be compromised just like a large number of the top 10000 sites in the world. Credit card information, passwords and other information processed by these websites can be disclosed [14, 15].

Bypassing of the authentication. Authentication, including two-factor authentication, is considered to be a reliable way to ensure the security of user data. In 2014 the researchers at the Amsterdam Free University found a vulnerability that allows to bypass two-factor authentication upon condition that the user has a smartphone running on Android or iOS. The attacker intercepted the access confirmation code that came to the user's phone using a spyware application which is a trojan that attacks the smartphone. Trojan sends a request to Google Play to install the application on the user's device and do not require any confirmation, the software is installed and the interception of the access code is performed (the code is redirected to the server of the attacker) [16].

Elevation of privileges. In 2018, the attackers hacked the cloud storage of Tesla company, and then they gained access to internal information from the car manufacturer. In addition, attackers used cloud resources to implement the cryptocurrencies mining [17].

Attacks on the client's databases. The client's databases are of the most interesting type of data for an attacker; therefore, many companies are under threat. An example is the hacking of the WADA (anti-doping organization) database in order to compromise some athletes. Such kind of attack gave damage of about $20 thousand [18, 19].

In addition, because of the attack on the client database, the McDonald's company was damaged when the names, phone numbers, electronic and mail addresses of clients that were participants of promo company were stolen. Thas happened in 2010 [20].

Hackers also stole the database of the largest US company Epsilon which is engaged in researching the Internet market. The mail server was hacked, as a result, the company's customers were exposed to spam mailing [21]. The same story happened with Amazon [22].

Data theft. The storage of information on cloud services does not give 100% guarantee of privacy of this data. The lists of login/password pairs from the DropBox service were published on Internet by one of the hackers. The hacker is ready to provide 7 million pairs of account data for bitcoins [23].

One more example of data theft is the theft of personal photo and video of celebrities. The data was in the Apple iCloud storage which was hacked and the information was published on the Internet [24, 25].

There are the commercial applications that allow hacking the iCloud storage and then transfer the available information to another cloud (DropBox or Google Drive). The price of such programs is 200-400 $. One of them is Elcomsoft Phone Password Breaker. Hacking is carried out as follows: the program selects the user's password, and then you

can select the data required for viewing. Two-factor authentication is not provided here, and the data is transmitted in an unencrypted form [26].

Keystone identity management service contains one of the most interesting types of data for an attacker, so it is a center of unauthorized access and a key risk factor. Therefore, security mechanisms are required to be in a place to access and administer data in Keystone. These include encryption, identification, authentication, access control policy, dedication of privileges, etc.

In addition, the problem lies even in the principle of cloud functionality itself. The resource providing in the cloud should support multi-threading and multi-servicing, and, from cloud point of view, identity management service is just one of the services along with others. In other words, it is easier for service providers to set up the principle of least privilege as an access policy to Keystone and continue using a workflow mechanism for other services. Thus, many deployments of identity management systems today provide excessive provision of effective access rights to users who do not even require these access rights. Such over provision of access leads to many critical security problems including unauthorized access to information, theft of personal data, customer data fraud.

Another most important aspect of identity management is access control to privileges. A frequent problem in conducting business and providing services in the corporate environment is the mismanagement of roles or the violation of the division of responsibilities. Access to privileges should also be a management mechanism. In addition, there should be appropriate reporting and audit of events which is important for detection of unauthorized access.

The heterogeneous nature of the cloud provides access to the services from many different devices and applications. This leads to the increased number of connected points which, with high probability, will be under the risk of unauthorized disclosure of personal data (loss of confidentiality). Similarly, with the growing number of access points and system objects, the integrity of the identity data stored in the Cloud is being under threat risk and shows one more important issue in security [27].

In addition to the above-mentioned problems, the management of trust between the IAMS provider and the consumer of the service should be mentioned. This is one of the main problems that cloud-based IAMS is dealing with today. Trust is a subjective and reputation-dependent parameter that makes it even more difficult to choose an IAMS provider with fully trusted identity services [28].

A lot of attacks on reputation are implemented against global services such as airline companies, government websites and cloud providers. In 2017, the British airline was forced to delay their flights for several hours due to disruptions in the work of the software and had to cancel a large number of flights around the world. This is not the only airline that has faced such a problem. Over the last year, United Airlines, Delta, JAL, All Nippon and Southwest Airlines were forced to cancel flights for the same reason [29].

Global service provider Yahoo also had to admit a serious lack in the security system. In December 2016, it became known about the breaking of a billion accounts that took place in 2013. Before, in September 2016, Yahoo officially announced that during the hack-

er attack in 2014, at least 500 million users of the company's services were stolen. These two attacks are the largest known hacking the network of one company. Initially, Verizon Communications Inc. asked for a discount of $ 1 billion but then the discount was reduced to $ 350 million [30].

Government websites remain popular target for attackers to provide the reputation losses. Breaking of websites of the Ministry of Energy and Coal Industry of Ukraine [31], Ministry of Social Policy of Ukraine [32], Kirovograd Regional State Administration [33], website of Ukraine Parliament Commissioner for Human Rights [34], etc. are the latest examples of website disclosure.

Such kind of attacks in cloud occurs very often due to the large number of vulnerabilities in cloud services, IAM system and the Internet in general. Hackers easily find gaps that can be used to attack any system. Therefore, it becomes relevant to review existing vulnerabilities and security mechanisms in IAMS to ensure security at all possible levels provided that the company does not want to face damage and losses.

Understanding the methods of authentication and authorization process in Keystone as well as functionality of cloud access management service will help us in identifying possible vulnerabilities. Also, considering the components of the service allows to assess the attacks and methods of protection deeper.

3. Keystone Architecture and Attack Surface

The Keystone service architecture is quite simple. Keystone handles all API requests and provides the ability to use services such as Identity, Token, Catalog, Policy (Table 1). Keystone consists of a group of front-end services that are provided through a network API [35, 36].

Table 1. Description of the provided services

Service	Description
Identity	The service validates the authentication credentials and provides all associated metadata
Token	The service verifies and manages the tokens used to authenticate requests after user credentials have been verified
Catalog	The service provides a registry of services that can be used to discover the corresponding endpoints
Policy	The service represents a rule-based authorization mechanism

3.1. Keystone core components

Keystone consists of the following components [37]:

1) Server. A centralized server provides authentication and authorization services using the RESTful interface.

2) Drivers. Drivers or the back ends are installed on a centralized server. They provide access to information for authentication in directories external to OpenStack. These directories can already exist in the infrastructure where OpenStack is deployed (for example, SQL databases or LDAP directory).

3) Modules. Intermediate layer modules are executed in the address space of the OpenStack component that is using Keystone. These modules intercept service requests, retrieve user credentials, and send them to a centralized server for authorization. Interfaces between the middleware modules and OpenStack components use the Python interface WSGI (Web Server Gateway Interface).

3.2. Keystone Backend Services

The Keystone package provides services identification for all OpenStack projects. Integration into heterogeneous environments is performed with the help of backend plug-ins that are supported by each Keystone service. All plug-ins are able to provide a variety of functionality. The most widely used back end plug-ins are described below.

1) Key Value Store. Plug-in that store, retrieve, and manage data structure such as a dictionary or hash, make search of the value-key.

2) Memcached is chaching system that stores data and objects in RAM according to a key, reduces the number of external data source such as a database or API that should be read.

3) Structured Query Language (SQL) stores data persistently. Keystone uses SQLAlchemy migrate of the SQL database between revisions.

4) Pluggable Authentication Module (PAM). Plug-in integrates multiple low-level authentication scheme to API calls through local system's PAM.

5) Lightweight Directory Access Protocol (LDAP). Keystone connects to LDAP directory, for example, to Active Directory, for authentication and authorization services.

3.3. Keystone Authorization Model

Authentication in OpenStack is a two-stage mechanism. The first stage is the initial authentication when the user is created in Keystone and one-time-password is generated. This password is used for establishing a key-pair, public key signed with X.509 certificate is stored in Keystone, private key is only stored on the end user's side. Keystone uses its signing key and certificate to sign the user token. The second stage is the usage of the token to provide single-sign-on [37] and delegated authorization scheme in the OpenStack cluster. The format of the signed document is the Cryptographic Message Syntax [38]. PKI can improve the security at the first stage. It can both help security and scalability at the second one. For more information refer to OpenStack wiki [39].

Classical authorization model in Keystone service with generation and validation of tokens is shown in Figure 1, where

RN_c is a random number generated by the client,

RN_s is the random number generated by the server,

K_c is key value from client side,

K_s is key value from server side,

T_0 is the encryption time, used to validated token expiration date,

CMS token is Cryptographic Message Syntax [39]. Keystone produces CMS token out for such data as user roles, service catalog and metadata.

PKI does not guarantee privacy of the tokens. It is only used for checking Keystone's signature but not encryption. In order to prevent tokens from being hijacked all API endpoints using the HTTPS protocol should be secured. Interception, Spoofing and Replay attacks are the main manipulations that an attacker can make with elements that participate in the authorization process.

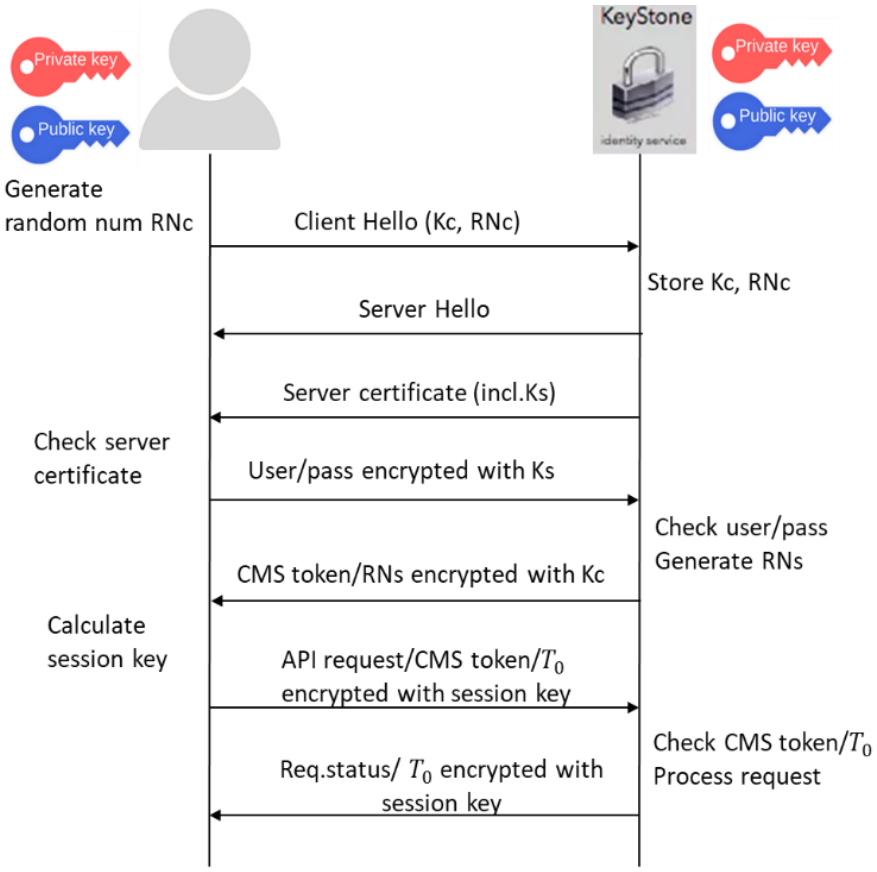

Fig. 1. Keystone authorization model

3.4. Authentication and Administration Functions of Keystone

The identity management system supports authentication and authorization of all services in OpenStack. Therefore, it should provide a mechanism that simplifies the discovery of services and at the same time provide tools for applying and control of security policies.

The simplest way to visualize the scenario of using Keystone is to split it into two functions: authentication and administration. Hence, Keystone core is split into two components: credential management and role assignment management respectively.

Credential management (i.e., authenticated entities) allows user and group accounts to store in a local SQL database, or provide support from a remote LDAP service or Active Directory.

Keystone authentication function supports also authentication of services during execution process. For example, an application uses OpenStack Swift component to store objects. Regardless of whether it is executing as part of OpenStack Compute instance or not, application must be able to authenticate. In other words, this application needs access to valid credentials.

Administrative functions in Keystone define projects, domains, roles, and assignments for these roles. Projects and applications can interact with Keystone, performing queries and verifying access permissions. All these are stored in the role assignment management service that determines what the user can do after authentication. Again, they can be stored in a local SQL database or, more rarely, in a remote LDAP or Active Directory in a case of read-write access to it. Nevertheless, Keystone domain structure that use LDAP to manage credentials is limited by a single, default domain. This does not allow the use of LDAP or Active Directory in more complex environments.

3.5. Keystone Attack Surface

An analysis of Keystone identity and access management service is conducted from the view of presence of security problems. A brief description of the identified potential and existing attacks which either run against IAM service or use the identity as the main tool for attack is presented in the Table 2.

The resulting list can be used to determine the key security functions that cloud IAM service must provide to ensure the security and privacy of identity credentials in the Cloud.

4. Mechanisms of Ensuring Security

After analysis of all the security issues associated with the cloud identity and access management service in Section 2 and 3, the following main categories for applying security were identified:

- authentication management;
- authorization management;
- privacy protection;
- trust;
- logging&auditing.

Further consideration is given to existing security mechanisms in each category.

Authentication in IAMS usually relies on at least one of the mechanisms described below that depends on requirements of security level for the service, since high-security services require a stronger authentication mechanism.

Table 2. Attacks Description

№	Attack	Description
1	Replay attack	Attacker can avoid access restriction by recoding valid token or SID. This manipulation ensure Keystone to believe that a previously authenticated session or token is still ongoing and authentic. For example, the vendor of Fernet token in Keystone had such a vulnerability.
2	Sensitive Data Disclosure	Attacker can avoid certificates verification during authorization process (see Figure 1) and be able to implement any Man-in-the-Middle attack. OpenStack Keystone middleware allowed to disable certificate verification in configuration file.
3	Elevation of Privilege	Attackers illegitimately escalate access rights with higher privileges by impersonating other clients in order to achieve personal data or make severe damage to the stored information. Keystone earlier versions allowed remote authenticated users to access an unauthorized project for which the trustee has certain roles through the project identifier in the V2 API request token of trust.
4	Denial of Service Attack	Attacker overwhelms the Cloud identity management server with false authentication or authorization requests (malformed input data) and tries to either stop the service or consume all of its available resources so that it may not be able to process the legitimate user requests. API V3 in Keystone allowed attackers to cause denial of service by creating large number of authentication methods in request.
5	Brute-force attack	An attacker using the brute force attack method could gain unauthorized access to confidential user data stored on the identity management service. To do this, he used a combination of username and password. OpenStack Keystone when using LDAP with anonymous binding had such a vulnerability.
6	Identity Theft	Attacker tries to steal personal data like a name or a credit card number to obtain cloud resources or some other benefit on behalf of the victim name. The user-password-update command in Python Keystone client prior to version 0.2.4 allowed this vulnerability to be exploited.
7	Spoofing Attack	Attacker forges identity by copying and manipulating the identifying tokens or credentials. The Nova directory has been exposed to this vulnerability.
8	Side-Channel Attack	Attacker steals the information (like session identifiers, timing information, OAuth tokens and electromagnetic leaks) from the physical implementation of a security system. Improper delegation of Keystone access rights to earlier versions resulted in a vulnerability.

The most well-known mechanisms include:

1) Password or Personal Identification Number (PIN),

2) One-Time-Password (OTP) scheme [41, 42],
3) Challenge-Response mechanism [43],
4) Single-Sign-On (SSO) [38, 43-46],
5) Public Key Infrastructure (PKI) [47],
6) Smart Card or SecureID tokens generators,
7) Mobile Phone,
8) Biometrics.

The Keystone service itself is not able to provide techniques that implement password security policies, to control validity period and unsuccessful authentication attempts that corresponds to NIST recommendations [48]. However, Keystone can use some general methods that support all relevant recommendations:

- Multi-factor authentication must be enabled through an external authentication system, such as the Apache HTTP Server.
- By default, the expiration time of the token is 1 hour. The recommended value of this indicator should be set to the minimum allowable value, which allows OpenStack-services to complete their requests within the established timeframe, otherwise the operation (in case of termination of the token before the end of the request from the service) will be interrupted. Note that some operations are particularly time-consuming, for example, when Nova transfers the disk image to the host.
- Use Fernet tokens, which are designed specifically for the REST API because they are more secure than conventional tokens, and also require fewer resources.

Authorization defines the parts of services to which the user has access. A cloud structure is an environment with multiple service providers where one user can have access to several services, each of which can be from another provider having different levels of security. Therefore, the identity service must provide effective authorization through mechanisms such as:

1) Access Control Policies.
2) Access Right Delegation using RBAC [49, 50],
3) Standard OAUTH [51],
4) It is recommended for the Keystone domains to more accurately delineate the access rights for the tenants. The domain owner can create additional users, groups, and roles within it.

The protection of privacy includes mechanisms by which the identity and access management service can guarantee the confidentiality of users and protect their data from unauthorized or unwanted disclosure [48]. The most well-known mechanisms include:

1) Proxying.
2) Shearing of user roles (identity attributes) between multiple services.
3) Generating of pseudonym.
4) Encryption.
5) Secure manipulation of data like storage, saving, transfer and deletion.

Trust is reputation of a service provider and the most valuable asset for a company. Brand image is associated with a trust and suffers from lacking security and privacy. Both

security and privacy are ways in which trust can be established. Trust to service provider is ensured by:

1) Feedback to customers.
2) Fast reaction on discovered flaws.
3) Timely software updates.

Proper Logging&Auditing ensures uninterrupted operation of the service, and it is also responsible for increasing the trust. For secure interoperation with Keystone service there is a need to constantly monitor emerging vulnerabilities and update the working environment. This will help to stabilize the work with the service, logging on the system, managing policies. In addition, work with directories that are under threat can be restored. In a multi-service cloud environment it is difficult to identify the person responsible for any misconfiguration, mismanagement or security flaw. The most well-known mechanisms in IAMS include:

1) Operating System (OS) Events. Start up and shut down of the system, services can be monitored as well as network connection changes or failures, or attempts to change system security settings.
2) Monitoring of user activity such as log on attempts, successful/failed use of privileged accounts.
3) Saving and automation of log data collection.
   Enable logging for supporting services and modules in OpenStack.

5. Results

Summarized categories for applying security and protection mechanism in identity and access management service is shown in Fig. 2.

In addition, for secure interoperation with the Keystone service we need to constantly monitor emerging vulnerabilities and update the working environment. This will help to stabilize the work with the service, logging on the system, managing policies. Moreover, work with directories that are under threat can be restored. Strengthening of OpenStack security should be provided at several levels, from the physical (data center, equipment and infrastructure) to the application level (user load modules) and the business process level (formal agreements with cloud customers about privacy, reliability and security). There are many additional OpenStack projects related to security that also are recommended to use:

• OpenStack Barbican [52] is a PKI and cryptographic service for the clouds of OpenStack available from the release of Havana. Barbican supports confirmed CA for TLS certificates, transparent encryption and key distribution for Cinder LVM volumes, KDS services for signing messages and encrypting Swift objects.

• Anchor [53] is a lightweight PKI service for creating reliable encryption tools in OpenStack services. Anchor uses short-term certificates, which usually operate for 12-24 hours.

• Firewall as a Service (FWaaS) [54] is a plug-in that applies firewall policy to OpenStack objects such as projects, routers, and router ports and supports one firewall policy and logical firewall instance per project. Its goal is to provide a unified API for traditional L2 / L3 firewalls, as well as next-generation firewalls for the use in the OpenStack clouds.

• Load Balancer as a service (LBaaS) [55] is currently an advanced service of Neutron project. Its goal is to provide a tool for improving the efficiency of balancing technologies for the proprietary and open-source components when performing load balancing in query processing.

To protect and prevent the previously listed attacks in Sec. Attacks against Keystone identity management service, the following protection mechanisms were proposed, divided by categories and presented in Table 3 (influence on attack can be viewed in Table 2).

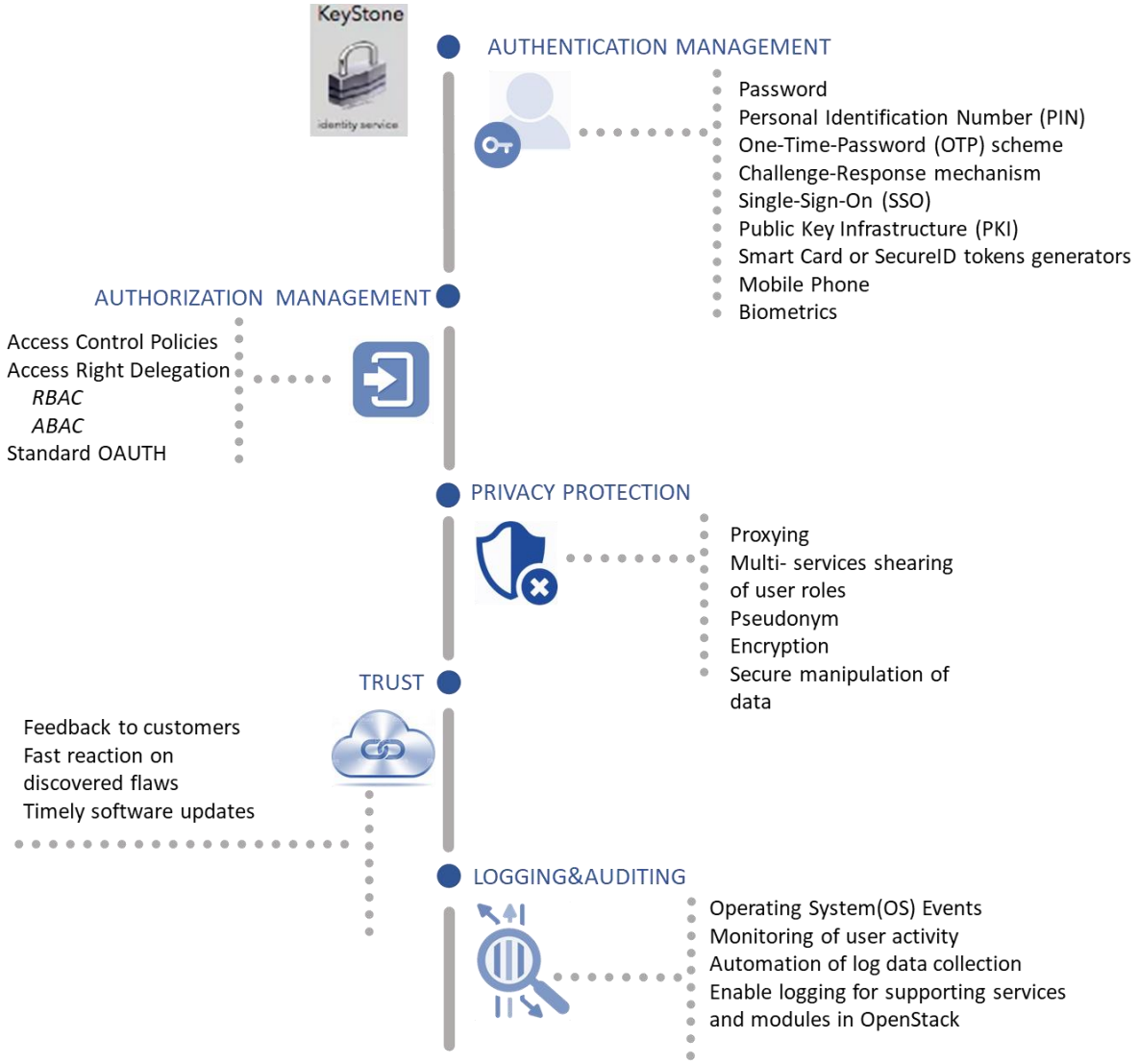

Fig. 2. Mechanisms of ensuring security in the Keystone service

Table 3. Mechanisms of protection

Category	Mechanism	Influence on attack
Authentication management	- mutual authentication (PIN&OTP, for example) - creation of the security token of the session and their distribution - deletion and cancellation of tokens policy - multi-factor authentication (password and smart card, for example) - limit the number of requests for identity	Attacks 1,2,4, 5,7,8
Authorization management	- role-based architecture - separation of identities to personal, corporate and social	Attacks 3, 8
Privacy	- processing only encrypted data, abstraction from a person - active bundles mechanism for unreachable hosts, sources - encrypted storage of identity data - limited disclosure of personal data to service providers	Attacks 2, 6, 8
Trust	- authentication and authorization as an as-a-Service	Attacks all
Logging &audit	- setting up logging of events that can be identified as unauthorized access - storage of the backend copy in a secure place - controlling access to folders with logs	Attack 1,4,5,7

6. Discussion

As it is seen from Table 3, for some attacks there are several methods of solution and protection. In order to ensure that the attacker is not able to steal confidential data or access a user account using a replay attack, the infrastructure managers must enhance authentication management, privacy and logging, as the protection mechanisms used in these categories can provide the necessary authorisation security for the Keystone service:

• Mutual authentication may be used as a starting point to verify each party's identity; this allows to eliminate risks related to fraud by one of the parties.

• Security tokens created at the beginning of each session would allow to recognize a specific participant among all users; given the risks associated with sending security tokens over the network in an open form, it would be preferable to create a one-time security token, generated by each particular user and passed to the server. Even if the attacker intercepts a token, he/she will not have any useful long-term information, since the token only serves one request. Session stealing could indeed be accomplished by token spoofing, but since the attacker does not have any information from the server, such as a session key, the generation of his own hash becomes impossible.

• Multi-factor authentication should be employed to secure personal data because in order to gain access to personal information, the attacker needs to use several methods of authentication. Both a password and a smart card could be used as authentication mechanisms.

• Lockout policy should be used to restrict the number of authentication requests. It helps to prevent the brute-force or long-terms attack.

• Access control restrictions can be used to ensure security, since in case of non-compliance of the subject and his rights the IAM system will not grant certain privileges.

• Event Logging allows protecting sensitive data by blocking attacks that are inconsistent with normal system access.

If an attack take place, keeping a backend copy in a secure location is critical, as it prevents the attacker from gaining access to personal information through a replay attack. Moreover, it is recommended to differentiate access to folders with logs. Denying of access will not allow an attacker to use logs to perform unimpeded logons.

To protect against Replay attacks, it is recommended to use proper authentication management methods, protection of personal data and privacy will help to preserve personal data.

To avoid Privilege elevation used as a method of stealing personal data it is recommended to perform authorization control of delegating the access rights that will be assigned to each of the users based on the roles. This will allow to create different hierarchies that will inherit the set of granted rights. Similarly, differentiation of identities by category to personal, corporate and social can be used to ensure that each user is granted access only for their category. Users will be able to separate personal information from the service information, thereby securing access to each data category by separate authorization.

In order to minimize the risks that can be caused by a DoS attack the categories of authentication management, privacy and logging should be enhanced. In this context, when an attacker is performing a brute-force attack, the protection mechanisms for authentication management, confidentiality and logging should be enhanced.

The Identity theft attack is avoided by ensuring security in the privacy sector. For example:

• Encryption of data during its computation and processing will protect information from unauthorized access that will minimize the possibility of attacker's intrusion.

• Encrypted storage of identification data will not allow using information about the user without permission.

• Limited disclosure of personal data will not allow the interception of information during its provision to the provider.

Spoofing attack can be eliminated by managing authentication, confidentiality and logging. Side-channel attack is eliminated by all provided mechanisms of protection, except logging.

Conclusions

The paper reviewed the main vulnerabilities that lead to security risks in the Keystone identity and access management service. As highlighted by the discussion, most vulnerabilities relate to authentication token generating, processing and storing. In the process of patching, it is often the case when addressing one vulnerability may create additional opportunities for attack through exploiting of other services. The importance of the absence of vulnerabilities in Keystone service lies in the fact that this service manages the catalogue services during OpenStack deployment. The vulnerabilities make it difficult to work with the cloud system, often making it impossible to log into the system, manage policies, or maintain directories. This paper will help in research focused on the prevention mechanisms of unauthorized access to personal data. The list of possible attacks obtained during the analysis can be used to determine the key security functions that the IAM system in the cloud structures must provide to protect and secure identity credentials in the Cloud.

References:

1. *Habiba, U., Masood, R., Shibli, M. and Niazi, M.* Cloud identity management security issues & solutions: a taxonomy. Complex Adaptive Systems Modeling, 2(1). DOI: 10.1186/s40294-014-0005-9.

2. *Nexia International*. Global Cybersecurity Report 2017, 50p. URL: https://www.nexiabt.com/wp-content/uploads/2018/01/file-28.pdf

3. *Cisco.* 2017 Annual Cybersecurity Report. 2017, 110 p. URL: https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf

4. *Cisco.* 2018 Annual Cybersecurity Report. URL: https://www.cisco.com/c/en/us/products/security/security-reports.html

5. *Willis Towers Watson*. Willis Towers Watson Cyber Risk Survey. 2017. 38 p. URL: https://www.willistowerswatson.com/-/media/WTW/PDF/Insights/2017/06/WTW-Cyber-Risk-Survey-UK-2017.pdf?la=en&hash=EC5D9C3C2888B4D4C7BF1476AF319D4E344984C3

6. *McAfee Labs*. 2017 Threats Predictions. 2016, 56 p. URL: https://www.mcafee.com/de/resources/reports/rp-threats-predictions-2017.pdf

7. *Ponemon Institute LLC and Accenture*. Cost of Cyber Crime Study. Insights on the Security Investments that Make a Difference. 2017, 56 p. URL: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

8. *Ponemon Institute LLC and Hewlett Packard Enterprise*. Cost of Cyber Crime Study & the Risk of Business Innovation. 2016. 37 p. URL: https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

9. *Symantec*. Internet Security Threat Report. 2017, 77 p. URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

10. *Kaspersky Lab*. Measuring Financial Impact of IT Security on Businesses. IT Security Risks Report. 2016, 12 p. URL: https://media.kaspersky.com/en/business-security/kaspersky-it-security-risks-report-2016.pdf

11. *Kaspersky Lab*. A global survey into attitudes and opinions on IT security. 2017, 11 p. URL: https://media.kaspersky.com/documents/business/brfwn/en/The-Kaspersky-Lab-Global-IT-Risk-Report_Kaspersky-Endpoint-Security-report.pdf

12. *PwC UK and BAE Systems.* Operation Cloud Hopper. Technical Annex. 2017, 30 p. URL: https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf

13. *PwC UK and BAE Systems*. Operation Cloud Hopper. 2017, 25 p. URL: https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf

14. *Aviram N., Schinzel S. et al.* DROWN: Breaking TLS using SSLv2. USENIX Security Symposium. 2016. 18 p.

15. Mott N. Drown attack: how weakened encryption jeopardizes 'secure' sites. The Guardian, 2017. URL: https://www.theguardian.com/technology/2016/mar/02/secure-https-connections-data-passwords-drown-attack

16. *Konoth R.K. van der Veen V., Bos H.* How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication. Financial Cryptography and Data Security FC 2016. Lecture Notes in Computer Science, vol 9603. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-662-54970-4_24

17. *RedLock CSI Team*. Lessons from the Cryptojacking Attack at Tesla. URL: https://blog.redlock.io/cryptojacking-tesla

18. *Tripware*. The WADA Hack of Olympic Athletes' Medical Data – A Timeline. URL: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-wada-hack-of-olympic-athletes-medical-data-a-timeline/

19. *WADA*. Cyber Security Update: WADA's Incident Response URL: https://www.wada-ama.org/en/media/news/2016-10/cyber-security-update-wadas-incident-response

20. Hackers steal McDonald's customer data URL: https://www.computerworld.com/article/2511778/security0/hackers-steal-mcdonald-s-customer-data.html

21. Epsilon breach: hack of the century? URL: https://www.computerworld.com/article/2471044/cloud-computing/epsilon-breach--hack-of-the-century-.html

22. A Hacker Claims to Have Leaked 80,000 Amazon Users' Passwords and Personal Information. URL: https://mic.com/articles/148207/a-hacker-claims-to-have-leaked-80-000-amazon-users-passwords-and-personal-information#.YreVcSQqr

23. Nearly 7 Million Dropbox Account Passwords Allegedly Hacked. URL: https://thehackernews.com/2014/10/nearly-7-million-dropbox-account.html

24. *Kaspersky Lab.* How to protect yourself from cloud service leaks. URL: https://www.kaspersky.com/blog/celebrity-photos-leaked/5895/

25. After Celebrity Photo Hack, How Safe Is the Cloud? URL: https://mashable.com/2014/08/31/how-safe-is-icloud/#NugtDdlkTuqt

26. How I Hacked My Own iCloud Account, for Just $200 URL: https://mashable.com/2014/09/04/i-hacked-my-own-icloud-account/#i.Uzn2JLoGqw

27. *Ahmadi V., Tutschku K.* Privacy and Trust in Cloud-Based Marketplaces for AI and Data Resources. IFIPTM, 2017: proceedings. IFIP AICT 505: Springer International Publishing AG. DOI:10.1007/978-3-319-59171-1

28. *Pearson S., Benameur A., Pearson S.* Privacy, security and trust issues arising from cloud computing. IEEE Second International Conference on Cloud Computing Technology and Science

(CloudCom): proceedings, 2010. Indianapolis, IN, USA: IEEE. P.693- 702. DOI: 10.1109/CloudCom.2010.66

29. British Airways cancels all flights from Gatwick and Heathrow due to IT failure. URL: https://www.theguardian.com/world/2017/may/27/british-airways-system-problem-delays-heathrow

30. Verizon originally asked for $925M discount following Yahoo breach disclosures URL: https://www.ciodive.com/news/verizon-originally-asked-for-925m-discount-following-yahoo-breach-disclosu/438014/

31. *Saakov V.* Khakery zlamaly novyy sayt minenerhovuhillya Ukrayiny. Deutsche Welle, 2018 URL: http://www.dw.com/uk/хакери-зламали-новий-сайт-міненерговугілля-україни/a-43507063

32. *Ukrainian Cyber Alliance.* Ministerstvo sotsial'noyi polityky Ukrayiny…[Facebook post]. URL:https://www.facebook.com/photo.php?fbid=435547163560314&set=pcb.435547266893637&type =3&theater

33. *Ukrainian Cyber Alliance*. Vot eshchë smeshnoe ot Kirovohrads'ka Oblasna Derzhavna Administratsiya… [Facebook post]. URL: https://www.facebook.com/photo.php?fbid=435633553551675&set=p.435633553551675&type=3&theater

34. *Ukrainian Cyber Alliance*. Upovnovazhenyy Verkhovnoyi Rady Ukrayiny z prav lyudyny… [Facebook post]. URL: https://www.facebook.com/photo.php?fbid=435557056892658&set=a.130395897408777.1073741828.100013151020465&type=3&theater

35. *RedHa*t. Identity Management. Cloud Administrator Guide. Red Hat Enterprise Linux OpenStack Platform. URL: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux_OpenStack_Platform/5/html/Cloud_Administrator_Guide/index.html

36. *Rhoton J.* The Identity component Keystone. URL: https://www.ibm.com/developerworks/cloud/library/cl-openstack-keystone/index.html

37. Keystone Installation Tutorial. OpenStack. URL: https://docs.openstack.org/keystone/pike/install/

38. *Garg P., Singh Y.* SSO (Single Sign On) Implementation. International Journal of Science and Research (IJSR), 2016. Vol.5, Is.6. P.988-990. DOI: 10.21275/v5i6.nov164426

39. *Housley R.* Cryptographic Message Syntax (CMS): IETF RFC 5652. September 2009. 56 p.

40. PKI – OpenStack. URL: https://wiki.openstack.org/wiki/PKI

41. *Luo S., Hu J., Chen Z.* An identity-based one-time password scheme with anonymous authentication. International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC), 2009: proceedings. Wuhan, Hubei, China: IEEE, 2009. P.864-867. DOI:10.1109/NSWCTC.2009.287

42. *Olden E.* Architecting a cloud-scale identity fabric. Computer. 2011. Vol. 44, Is. 3. P.52-59. DOI:10.1109/MC.2011.6011.

43. *Choudhury A.J., Kumar P., Sain M., Lim H., Jae-Lee H.* A strong user authentication framework for cloud computing. Services Computing Conference (APSCC), 2011: proceedings. Jeju Island, South Korea: IEEE, 2011. P.110-115. DOI:10.1109/APSCC.2011.14.

44. *Wang G., Yu J., Xie Qi.* Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks. IEEE Transactions on Industrial Informatics. 2013. Vol. 9 (1). P. 294- 302.

45. *Cigoj P., Blai B.J.* An Authentication and Authorization Solution for a Multiplatform Cloud Environment. Information Security Journal: A Global Perspective. 2015. Vol. 24 (4-6). P. 146-156.

46. *Chadwick D., Casenove M., Siu K.* My private cloud--granting federated access to cloud resources. Journal of Cloud Computing. 2013. Vol.2. P.1-16. DOI:10.1186/2192-113X-2-3.

47. *Wazan A.S., Laborde R., et al.* Trust Management for Public Key Infrastructures: Implementing the X.509 Trust Broker. Security and Communication Networks. 2017. Vol. 2017. P.1-23. DOI:10.1155/2017/6907146.

48. *Jansen W., Grance T.* Guidelines on Security and Privacy in Public Cloud Computing. NIST: Special Publication 800-144, 2011. 80 p.

49. Information Technology – Role Based Access Control: ANSI INCITS 359, 2012.

50. *Kuhn D.R., Coyne E.J., Weil T.R.* Adding Attributes to Role Based Access Control. Computer. 2010. Vol.43, Is. 6. P. 79-81.DOI:10.1109/mc.2010.155.

51. *Hardt D.* The OAuth 2.0 Authorization Framework: IETF RFC 6749. October 2012, 76p.

52. OpenStack: Barbican. URL: https://wiki.openstack.org/wiki/PKI.