Journal of Theoretical and Applied Computer Science
ISSN 2299-2634 (printed), 2300-5653 (online)
Vol. 8, No. 1, 2014, pp. 35–49
http://www.jtacs.org

Selected aspects of security mechanisms for cloud computing – current solutions and development perspectives

Aneta Poniszewska-Maranda

Institute of Information Technology, Lodz University of Technology, Poland

{anetap}@ics.p.lodz.pl

Abstract: *The security aspects of cloud computing, especially the security of data, become more and more important. It is necessary to find and develop the new mechanisms to secure the cloud. The problem presented in the paper concerns the mechanisms for security of cloud computing with special attention paid to aspects of access control in clouds – the state of the art and the perspectives for the future.*

Keywords: *cloud computing, data security, security mechanisms, security for cloud computing*

1. Introduction

The modern application, software, information systems evolve very quickly. The information is more and more distributed through the networks or federation of numerous information systems located in different places on the globe. Also, the control domain of information system is very important in the times of very fast networks, telecommunication protocols and telecommunication equipment.

Cloud computing is a general term for everything that involves delivering hosted services over the Internet. In other words it is regarded as a ”method of running application, software and storing the related data in provided computer systems and providing customers or other users the access to them through the Internet” [1, 2]. Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet).

The purpose of cloud computing is to provide easy, scalable access to computing resources and IT services. These services are divided into three the most used categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

A cloud computing has three characteristics: it is solid on demand, elastic (users can have as much or as little of a service as they want at any given time) and service is fully managed by the provider (the consumer needs nothing but a personal computer and Internet access). Cloud providers focused more and more on providing fast and easy access to almost everything that user may need from extremely powerful computing clusters to possibility of usage just the applications that we might need, not paying for the entire infrastructure.

A cloud can be private or public. A public cloud sells services to anyone on the Internet. Cloud applications, storage, and other resources are made available to the general public by a service provider. Usually services of such cloud are free or pay for use. Those clouds are

accessible only via the Internet. If the connection with it is lost the connection with cloud is lost as well.

A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. This type of cloud is created and operates solely for a single company or organization, can be hosted internally (being a part of company internal network) or externally as a separated part of provider infrastructure. If the hosting is internal, in case of lack of Internet connection cloud can still be used by organization in its own internal network. The issue with such cloud is a lack of decreasing costs (as it would be with external cloud) because company has to buy hardware, software and manage it all by themselves.

Security of cloud computing is very important for cloud customers – customers take the decision about buying cloud service on the basis of the reputation for confidentiality, integrity and resilience, and the security services offered by a provider. Therefore, these aspects are sometimes more important than in traditional environments. For this reason, cloud providers have to improve their security practices, tools and mechanisms and compete on security level.

The problem presented in the paper concerns the mechanisms for security of cloud computing with special attention paid to aspects of access control in clouds – the state of the art and the perspectives for the future.

The first part of this paper presents the outline of the cloud computing and its types, while the second part deals with the threats and risks in security of cloud computing. The next two parts describes the recommendations for security of clouds and proposed solutions that can be put into practice to secure the clouds and their data.

2. Cloud computing and its security

Although several researchers have tried in their works to define the cloud computing, no single, agreed-upon definition exists yet. The US National Institute of Standards and Technology (NIST, http://csrc.nist.gov) defines it as follows:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models.

The five key characteristics of cloud computing include:
— on-demand self-service,
— ubiquitous network access,
— location-independent resource pooling,
— rapid elasticity
— and measured service.

All of them are geared toward using clouds seamlessly and transparently. The applications running on or being developed for cloud computing platforms provoke many various security and privacy challenges that depend on the underlying delivery and deployment models [3, 4].

2.1. Cloud service models

The models of cloud service can be divided into two types: development models and deployment models [3, 4].

There are many types of development models of cloud computing in the literature: infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS),

Network as a service (NaaS), Storage as a service (StaaS), Security as a service (SECaaS), Data as a service (DaaS), Desktop as a service (DaaS), Database as a service (DbaaS), Test environment as a service (TeaaS), API as a service(APIaaS), Backend as a service (BaaS), Integrated development environment as a service (IDEaaS), Integration platform as a service (IpaaS). The most popular ones are: Paas, SaaS and IaaS (Fig. 1) [5, 6, 7].

Platform as a Service is a category of cloud computing services that provide a computing platform and a solution stack as a service. In this model, the consumer creates the software using tools and/or libraries from the provider. The consumer also controls software deployment and configuration settings. The provider provides the networks, servers, storage and other services.

Paas offerings may also include facilities for application design, application development, testing and deployment as well as services such as team collaboration, web service integration and marshaling, database integration, security, scalability, storage, persistence, state management, application versioning, application instrumentation and developer community facilitation. Examples of PaaS include: *AWS Elastic Beanstalk*, *Cloud Foundry*, *Heroku*, *Force.com*, *EngineYard*, *Mendix*, *Google App Engine*, *Windows Azure Compute* and *OrangeScape*.

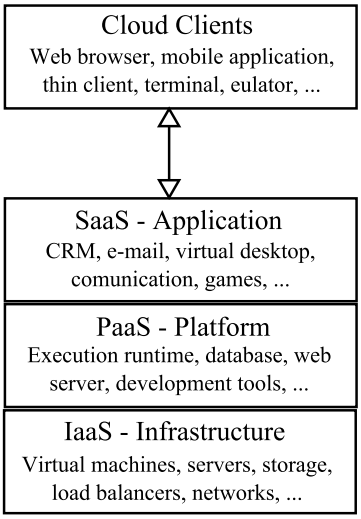

Figure 1. Types of cloud delivery models and services

Software as a Service, sometimes also referred as "on-demand software", is a software delivery model in which software and associated data are centrally hosted on the cloud. SaaS is typically accessed by users using a thin client via a web browser. Software as a Service has become a common delivery model for many business applications, including accounting, collaboration, customer relationship management (CRM), management information systems (MIS), enterprise resource planning (ERP), invoicing, human resource management (HRM), content management (CM) and service desk management.

Examples of SaaS include: *Google Apps*, *Microsoft Office 365*, *Onlive*, *GT Nexus*, *Marketo* and *TradeCard*.

In *Infrastructure as a Service* the most basic cloud-service model, providers offer computers – physical or (more often) virtual machines and other resources.

IaaS clouds often offer additional resources such as images in a virtual machine image library, raw (block) and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks and software bundles. IaaS cloud providers supply these resources on-demand

from their large pools installed in data centers. For wide-area connectivity, customers can use either the Internet or carrier clouds (dedicated virtual private networks). To deploy their applications, cloud users install operating system images and their application software on the cloud infrastructure.

Examples of IaaS providers include *Amazon CloudFormation*, *Amazon EC2*, *Windows Azure Virtual Machines*, *DynDNS*, *Google Compute Engine*, *HP Cloud*, *Joyent*, *Rackspace Cloud*, *ReadySpace Cloud Services*, *Terremark* and *NaviSite*.

Deployment methods of cloud computing can also vary according to client's needs. The most common methods are: public, private and hybrid. The fourth type of cloud deployment models is community cloud [3, 4].

Public clouds are owned and operated by companies that use them to offer rapid access to affordable computing resources to other organizations or individuals. With public cloud services, users do not need to purchase hardware, software or supporting infrastructure, which is owned and managed by providers. Many businesses are using software as a service delivered from the public cloud for applications ranging from customer resource management (CRM) like *Salesforce.com* to transaction management and data analytics.

A *private cloud* is owned and operated by a single company that controls the way virtualized resources and automated services are customized and used by various lines of business and constituent groups. Private clouds exist to take advantage of many of cloud's efficiencies, while providing more control of resources and steering clear of multi-tenancy. Key characteristics of private clouds include:

— a self-service interface that controls common services, allowing IT staff to quickly provision, allocate and deliver on-demand IT resources,
— highly automated management of resource pools for everything from compute capability to storage, analytics, and middleware,
— sophisticated security and governance designed for a companys specific requirements.

A *hybrid cloud* uses a private cloud foundation combined with the strategic use of public cloud services. The reality is a private cloud cannot exist in isolation from the rest of a company's IT resources and the public cloud. Most companies with private clouds will evolve to manage workloads across data centers, private clouds and public clouds, thereby creating hybrid clouds. Evolving to a hybrid cloud strategy allows companies to keep critical line of business applications and sensitive data in a traditional data center environment or private cloud, while also taking advantage of public cloud resources like SaaS for the latest applications and IaaS for elastic, economical virtual resources to scale [5, 6, 7, 8].

Community cloud is owned and operated by organizations of a specific community – its means that the organizations with the similar requirements share a cloud infrastructure. It is a way to generalize a private cloud because it being an infrastructure which is only accessible by certain organizations.

Storing information in the cloud gives its users almost unlimited storage capacity. Hence, there is no need to worry about running out of storage space or increasing the current storage space availability. Since all the data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device.

After registration in the cloud, it is possible to access the information from anywhere, where there is an Internet connection. This convenient feature enables users to move beyond time zone and geographic location issues. Lastly and most importantly, cloud computing gives its users the advantage of quick deployment.

2.2. Security aspects of cloud computing

In spite of its many benefits, cloud computing also has its disadvantages. Generally, the major problem with the cloud computing is security. Before adopting this technology, companies should be aware that they will be surrendering all their company's sensitive information to a third-party cloud service provider. This could potentially put them to great risk. Hence, companies need to make absolutely sure that they choose the most reliable service provider, who will keep their information totally secure.

Figure 2 presents the differences in scope of security control between the cloud provider and cloud customer for each the service cloud models presented in the previous subsection.

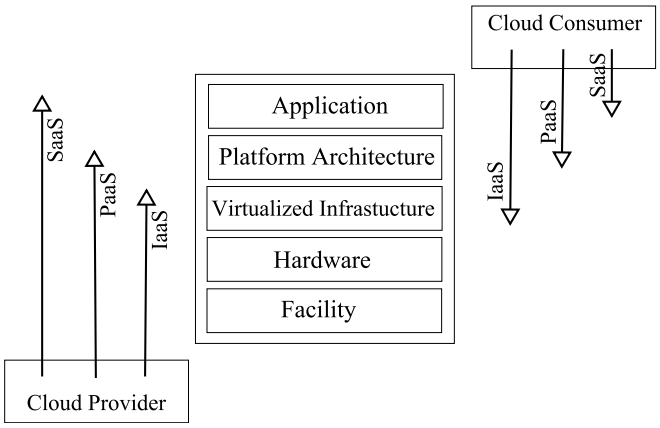

Figure 2. Differences in scope of security control among cloud models [9]

Security of cloud computing can be defined as a subdomain of computer security, network security, and, more broadly, information security. It concerns a wide set of policies, technologies and control methods developed and used to protect data, applications and associated cloud computing infrastructure. There are security issues in all aspects of the infrastructure including application level (SaaS model), host level (PaaS model) and network level (IaaS model).

Storing information in the cloud could make the company vulnerable to external hack attacks and threads. As companies are well aware, nothing on the Internet is completely secure and hence, there is always the lurking possibility of stealth of sensitive data [10, 11, 12].

The specification of data security and privacy protection in cloud computing is similar in many aspects to the traditional data security and privacy protection. Similarly it can be involved in every stage of data life-cycle. But because of the openness and multi-tenant characteristic of the cloud, the specification of data security and privacy in a cloud have also their differences [13, 14].

Understanding and clearly documenting specific user requirements is very important in development process of information systems. Determining the specific needs for data protection and information security can be very complex aspect of software design. Cloud computing as a multiuser distributed environment brings the unique security challenges, dependent on the level at which the user operates (Fig. 3):

1. *Application level* – Software as a Service (SaS) – end client applies to a person or organization who subscribes to a service offered by a cloud provider and is accountable for its use – security requirements are:
   — *access control*,

— privacy in multi-tenant environment,
— data protection from exposure (remnants),
— communication protection,
— software security,
— service availability.

2. *Virtual level* – Platform as a Service (PaS) and Infrastructure as a Service (IaS) – developer – moderator applies to a person or organization that deploys a software on a cloud infrastructure – security requirements are:
   — *access control*,
   — application security,
   — data security,
   — cloud management control security,
   — secure images,
   — virtual cloud protection,
   — communication security.
3. *Physical level* – Physical data-center – owner applies to a person or organization that owns the infrastructure upon which clouds are deployed – security requirements are:
   — *hardware security*,
   — legal not abusive use of cloud computing,
   — hardware reliability,
   — network protection,
   — network resources protection.

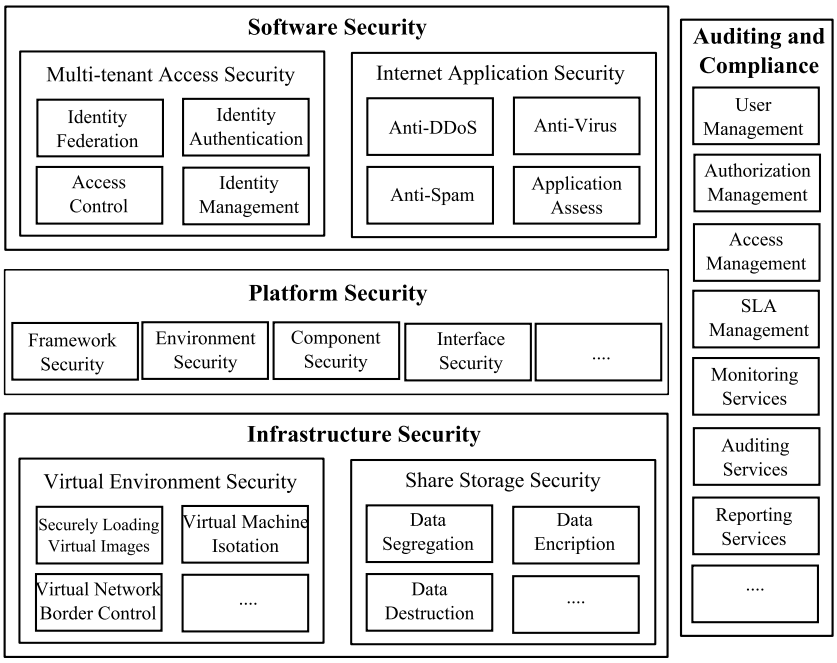

Figure 3. Security architecture of cloud computing

3. Threats and risks in security of cloud computing

Using cloud computing can carries a lot of threats. The concentration of resources in cloud services has some disadvantages for their security because it increases the occurrence

of security risks but on the other side it has the obvious advantage of cheaper physical access control (per unit resource) and the easier and cheaper application of security policy and control over data management.

Cloud computing is first of all convenient storage of data, information, applications, tools, accessible by multiple devices. It gives also other important advantages such as more instant multi-point collaboration for participants and convenient communication. Therefore the analysis of security risks in cloud computing has to take into consideration the risks of storing data in different places and risks of spread the data between collaborating persons. The level of risk significance can depends on the type of cloud architecture being considered.

Based on report of ENISA (*The European Network and Information Security Agency*), we can divide the security risks of cloud computing into three main categories [15]:

— Policy and organizational risks: loss of governance, loss of business reputation due to co-tent activities, compliance challenges, cloud service termination or failure, cloud provider acquisition.
— Technical risks: data protection risks, resources exhaustion (under or over provisioning), isolation failure, cloud provider malicious insider (abuse of high privileges), intercepting data in transit, data leakage, insecure or ineffective deletion of data, distributed denial of service, undertaking malicious probes and scans, conflict between customer procedures and cloud environments.
— Legal risks: changes of jurisdiction, licensing risks.

These types of risks represent the security risks specific for cloud computing, both from the customer point of view and from the provider point of view. We can also distinguish risks not specific for the cloud, such as network management, network traffic, privilege escalation, social attacks, and theft of computer equipment or natural disasters.

Sometimes the cloud customer can transfer the risk to the cloud provider and the risks should be considered against the cost benefit received from the services. However not all risks can be transferred.

4. Recommendations for security of clouds

The cloud computing services have an added level of security risk in comparison to traditional IT systems because important or sometimes essential services are often out sourced to a third party. Such external aspect of cloud service outsourcing makes the problems with correct maintenance of data integrity and privacy, with availability of data and services. In such situation cloud computing has to provide much of the control over data and operation at the cloud provider then at the customer organization [13, 14].

4.1. Security issues in the cloud delivery models

Different delivery models of cloud computing have different ways of providing the services to the customer. This influences the degree of security control over the management of cloud services and the privileges and responsibilities in security domain.

In *Software as a Service* model, most of the responsibility for security management is given the cloud provider. This model offers a number of solutions of access control, such as management of user identities, application level configuration and limitation of access basing on geographical customer location.

Platform as a Service provides the mechanisms to manage the security and configuration of applications, components of information systems, such as middleware, database software and application runtime environments.

The third type of cloud computing, *Infrastructure as a Service* offers the assurance solution on the level of operating systems. It transfers more control and security responsibility from the provider to the customer. Elements of operating systems are responsible for the access assurance, supporting the virtual images, networking and storage.

4.2. Security issues in the cloud deployment models

Each of the four deployment models in which cloud services can be used has its advantages and limitations. All of them have certain security areas needed to be addressed with a specific security policy.

4.2.1. Security issues in public cloud

The public cloud can have many customers on a shared platform and infrastructure security is provided by the service provider. It is possible to distinguish the following key security issues for a public cloud:

— The three basic security requirements, i.e. confidentiality, integrity and availability are required to protect the data throughout its life-cycle – its means during its creation, sharing, archiving, processing. The problems can be occurred when we do not have any control over the service provider's security practices.
— The same infrastructure is shared between multiple tenants and the chances of data leakage between these tenants are very high, especially because many service providers run a multi-tenant infrastructure. In such a case it is necessary to pay particular attention to the proper choice of service provide.
— When a service provider uses a third party vendor to provide its services, the customer has to be ensured what service level agreements (SLAs) they have and what are the contingency plans in case of the breakdown of the third party system.
— The proper SLAs define the security requirements of a cloud (i.e. level of encryption data) and what are the penalties in case the service provider fails to do so.
— Because the customer cannot deny the possibility of an insider attack originating from the service provider's end, an access control policy has to be proposed, based on the inputs from the client and provider to prevent such attacks.
— Policy enforcement implemented at the nodes and the data centers can prevent a system administrator from carrying out any malicious action – there are three main steps to achieve this: defining a policy, propagating the policy by means of a secure policy propagation module and enforcing it through a policy enforcement module.

4.2.2. Security issues in private cloud

The private cloud model gives the possibility to have a total control over the data and network and provides the flexibility to the customer to implement traditional security practices. However, it is possible to find some risk issues that should be considered in private cloud:

— Because the virtualization techniques are popular in private clouds, the risks to hypervisor should be carefully analyzed. For example a guest operating system can run the processes on other guest virtual machines (VMs) or hos. The VMs can communicate in virtual envi-

ronment with all the VMs including the ones who they are not supposed to. In such case the proper authentication and encryption techniques, e.g. IPsec, should be implemented to ensure that the VM only communicates with the ones which it is supposed to.
— The host operating system should be free from any threads and monitored to avoid any risks. Moreover, the guest VMs can communicate with the host operating systems by dedicated physical interfaces but not directly.
— The users can manage the part of a cloud and access the infrastructure by a web interfaces or HTTP end points. In this case the interfaces have to be properly developed and standard security techniques of web applications have to be deployment to protect the diverse HTTP requests.
— It is also necessary to implement the security policy in the organization cloud to safeguard the system from any attacks originating within the organization. The proper security rules and principles should exist across the organization's departments to implement the security control.

The hybrid cloud model is a combination of public and private cloud so the security issues discussed with respect to both are applicable in case of hybrid cloud. However, a trust model of cloud security in terms of social security has to be defined. Two additional layers of trust, internal trust layer and contracted trust layer, have been proposed in the literature to enhance the security in a cloud environment.

However, there is still the lack of mechanisms and tools for security and control, concerning the protection of sensitive information, the storage of regulated information in shared, externally managed environments.

4.3. Best practices for cloud computing

No matter what type of cloud we consider, both the provider and the customer are always responsible (in different proportions) for the security of particular services. As it was mentioned above, provider has the least control over security in IssS cloud as the customer sets up him own system, middle-ware and deploys his software and takes care of its security. In contrast, in SaaS cloud nearly whole responsibility for the proper security lies on the cloud provider as the end user deals with a ready-to-use application. This subsection discuss some of the best practices for both provider and customer to properly secure the data and systems in the cloud environment [13, 14].

4.3.1. Cloud providers

The main respectability failing on the shoulders of cloud providers is ensuring a secure and isolated environment for their customers [16]. This means making sure that each user can access only their environment and data and that other customer's systems, data and applications are invisible to him. Some of best practices for the cloud providers include:
— *Physical data center security* including building security (keycard protocols, biometric scanning protocols and round-the-clock interior and exterior monitoring, access to data center only by the authorized personnel.
— *Isolating and securing networks* – each isolated network has to have proper perimeter controls and policies to limit access to it.
— *Host machine operating system security* manages many guest virtual machines at once and any security hole might give the attacker an access to multiple customer environment. Host machine protection should include [17]:

  - intrusion detection system monitoring network and system for any malicious activities.
  - as small number of user accounts as possible with limited administrator's access to them,
  - policy on strong and complex access passwords,
  - no publicly accessible network services and only necessary programs running on the machine.
- Performing regular *vulnerability scanning* of cloud infrastructure in order to find and identify any new or recurring vulnerabilities to prepare proper mitigation strategies [18].
- *Strong authorization and authentication* must be implemented to provide the customer with secure access to their data and resources. The principle of least privilege should be taken into consideration ensuring that the user can access only the resources he needs. And only the authorized administrators can access the cloud's resources [16].
- Ensuring *auditing mechanisms* are in place logging every time the customers or administrators access and use the resources.
- *Frequent backups of data* should be performed by the provider. It has to be transparent to the customer what backups the provider will perform and what should be done by the user [16].
- *Encrypting APIs* through which the customers access the cloud resources with SSL, recommended to provide the secure communication over Internet [17].

4.3.2. Cloud customers

Even thought a significant amount of security responsibility falls on the provider, the cloud's customers have to be aware of certain practices as follows:

- *Proper firewall protection* is required to analyze the incoming and outcoming traffic and making sure any unauthorized access is blocked. User has to make sure that the hardware firewalls are properly configured to correctly protect all the machines on a local networks [17]. Software firewalls have to be installed on individuals machines to prevent a third party from taking control of the machine and to protect the customer's virtual machines.
- *Up-to-date software* including anti-virus, operating system and browsers through which the users usually access the cloud services. It is vital to keep everything updated to be protected from the newest threats and any bugs found in particular software [19].
- *Enforcing strong passwords policies* since most attacks occur due to using the insecure passwords. They can be considered the weakest link in the whole security domain. Users have to know how to make sure their passwords are strong [17, 11]: not use common dictionary words or words associated with the user's personal data, use the passwords with mix of lowercase, uppercase characters, numbers and special characters, use long passwords, change passwords periodically (usually every 90 days) and the best use different passwords for different services.
- *backup policies* which the customer has to discuss with the service provider to be certain what is whose responsibility. It is useful to have some third-party backup services to have the copies of the data in a case of sudden data loss in the cloud services [17].
- *Securing virtual machines* especially in a case of IaaS cloud where the user sets up everything on his own including operating system, any middle-ware and software. Is is his main responsibility to ensure the security including [17]:
  - ensuring a firewall for virtual machines service ports,
  - using encryption for communication,
  - performing frequent backups and file integrity checks,

  - control over what devices are connected,
  - making use of Intrusion Detection Systems to monitor system and network for any malicious activities.
- In case of organizations thorough *background checks* should be performed regarding any potential employees to ensure they do not pose a threat to the company and ts data.
- Keep up to data with the *latest cloud security developments* and any changes made to the security policies or infrastructure by the provider.
- *Limiting access to data* by setting proper access privileges to limiting number of other users or employees.
- *Controlling all devices* connected to cloud especially any mobile devices like laptops, mobile phones, tablets. Since they are mobile they can be easily stolen and therefore ensuring that an administrator has the ability to wipe the data from them might prevent serious security breach [17].
- *Encrypting data*, especially of sensitive kind. Securing the cloud service and client machine will be meaningless if the data that is sent over to the cloud is not encrypted as it is transported thorough shared networks [16].

4.4. Implementation of security for cloud services

The authors in [20] propose the following security measures to implement the security of cloud services:

- *implementing and maintaining of security program* to provide the structure for managing information security, the risks and threads for the target environment,
- *building and maintaining of secure cloud infrastructure* to provide the cloud resiliency and confidence that the data stored in a cloud is sufficiently protected,
- *providing the protection of confidential data* – the sensitive information has to be adequately protected in order to preserve its confidentiality,
- *implementing of identity and strong access management* – identity and access are very critical for cloud security in order to limit the access to data and applications to authorized and appropriate users,
- *establishing of provisioning for applications and environment* – it is important to have automated provisioning for cloud services, such as applications, especially in centrally managed cloud environment,
- *implementing of program for governance and audit management* – such program can help to defines when, how, and where to collect the logs and audit information in case of internal audits,
- *implementing of program for vulnerability and intrusion management* – it is important to implement such mechanisms as intrusion detection systems and intrusion prevention systems to provide the constant monitoring of IT resources (servers, network, infrastructure components) for any security vulnerabilities and breaches,
- *maintaining of testing and validation of environment* – it is important to assure the intact cloud environment.

The presented security measures concern different types of security – logical security, physical, organizational and communication security. From the point of view of logical aspects of security, the most important measures are: implementing of identity and strong access management, providing the protection of confidential data and in second order implementing and maintaining of security program, building and maintaining of secure cloud infrastructure.

Security threats on cloud users are both external and internal. Many of the external threats are similar to the threats that large data centers have already faced. This security concern responsibility is divided among the cloud users, the cloud vendors and the third party vendor involved in ensuring secure sensitive software or configurations [21, 22].

We propose some points which are very important for cloud providers to provide the protection of cloud computing. There are some tips how to implement a secure cloud [20].

First of all company should check the legal requirement of country in which they are operating. What are the conditions of storing personal information? Than prioritize security attributes from most important to least.

Next firewall should be placed at external network interface and between security zones in cloud. All unauthorized accesses should be blocked and logged. Also access to confidential data should be blocked. Firewall software must be installed at all external devices that interact with server. All administrative actions should be secured using networking protocols such as: SSH, SSL and IPSEC.

Very important is physical place of cloud. Unauthorized access to facility should be blocked, emergency power strategy planed. Employees that have access to sensitive data should have background check. Company has to ensure that communication between remote and corporate infrastructure is encrypted, protected by firewall and limited to minimum.

The encryption keys have to be managed securely. It means company should set up expiration date, old one should be destroyed, log all access to key and check access rights of key. Data communication has to use SSL/TSL and IPSEC protocols to protect sensitive information.

What is more cloud provider should encrypt all passwords and set up expiration date. Define how strong password should be. Company should implement intrusion detection system and system of prevention. Then test all system if they are preventing form attacks and if encryption is high enough.

All those steps must be stored in documentation and guidelines how to react in different situations. The organization has to identify its security requirements for cloud services as a criterion for its use and for the selection of a cloud type and provider. Such security requirements consider the following aspects:

— logical and physical access controls,
— data retention, data protection, resource management,
— personal security requirements such as roles, responsibilities and duties,
— risk management,
— system configuration, patch management, network access control,
— service availability, continuity of operations, backup and recovery,
— problem and incident reporting, review and resolution,
— certifications, independent audits of services,
— regulatory requirements and assurance level.

5. Access control, authorization and delegation in cloud computing

The cloud is regarded as a large scale platform of data sharing with multiple owners, different users but this process is most often highly untrusted. The tools that can help in this activity represent the mechanisms of logical security, i.e. access control, authorization and delegation of rights. It is necessary these services prevent the untrusted client-owners, client-users, cloud compute and cloud storage provider. They are also an integral part of

end-to-end security framework to secure the access to data and/or to delegate the access to the resources.

Heterogeneity and diversity of services offered by cloud and the domains diverse access requirements in cloud computing environments, demand the fine-grained access control policies. Therefore, the access control services should be flexible enough to capture dynamic, context or attribute- or credential-based access requirements and to enforce the principle of least privilege. Such access control services can have to integrate the privacy-protection requirements expressed through complex rules.

Among the many methods proposed so far, the role-based access control (RBAC) model and its extensions have been widely accepted as the most promising model because of its simplicity, flexibility in capturing dynamic requirements and the support for least privilege principle and efficient management. RBAC is a neutral policy and can capture various policy requirements. But because of the highly dynamic nature of clouds, obligations and conditions are very important factors to assure the richer and finer controls of usage of the resources provided by a cloud.

Some important issues in area of access control, authorization and delegation, those have to be consider, can be as follows:

1. End-to-end authorization that can be represented by access control at different layers:
   — strong access control policies to support fine-grained authorization, e.g. policies of RBAC (Role-Based Access Control) type, for example extended RBAC model [23],
   — extensive delegations of privileges from owner to cloud to achieve fine-grained temporal access control, e.g. dynamic access control policies, for example Usage Role-based Access Control model [24],
   — extensive delegations of privileges from user to cloud to support mobile device access, e.g. dynamic access control policies with attributes.
2. Computation over encrypted/authenticated data.
3. Management of access control with the use of access control lists (ACLs) – this type of access control is not so sure as it should to be, very often it violets the principle of least privilege, it is insecure and very hard to scale.
4. Cloud services can change, especially in case of SaaS because users want to:
   — place data where they want,
   — access data from anywhere via different protocols,
   — update data, version data, and take snapshots,
   — share versions with who they want,
   — synchronize data among locations.

It is possible to have an addressed secure interoperation and policy engineering mechanisms to integrate the access policies of different domains and define global access policies. A centralized approach can create a global policy that mediates all accesses and is appropriate for a cloud application that consists of various services with different requirements. However, the cloud environment is dynamic, the domains are transient and can interact for a specific purpose so the centralized approach is in appropriate. It is also needs the specification frameworks to ensure that the cross-domain accesses are properly specified, verified, and enforced. Security Assertion Markup Language (SAML), Extensible Access Control Markup Language (XACML) and web services standards are viable solutions toward this.

Security engineering mechanisms can support the definition of global policies. Role mining uses the existing system configuration data to define the roles. In a cloud, users acquire different roles from different domains based on the services they need. To define global poli-

cies, RBAC type systems configurations can be used from different domains to define the global roles and policies. Each global role can include roles from different domains that have been assigned to the same groups of users.

In summary, it is necessary to investigate an efficient secure mechanism to express complex policy required by fine-grained access control, to investigate an efficient delegation mechanism to achieve temporal access control and to explore the computation over encrypted / authenticated data stored in a cloud.

6. Conclusions

The benefits of use of cloud computing are clear, so it is important to develop the models, mechanisms and tools to provide the proper security of cloud implementations. The presented extended abstract provides an overview of threats and risks in security of cloud computing, both from the point of view of cloud provider and from customer point of view, the general recommendations for security of clouds and the outline of issues related to proposed solution for cloud security.

In summary, cloud computing has some advantages and disadvantages. When considering using this technology companies should be aware of both. Cloud computing is cost effective, its providers offer unlimited storage capacity, much easier backup and recovery, automatic software integration, easy access to information and quick deployment. However, apart from potential technical issues, the main concern when using cloud computing is security. Clouds like anything else connected to Internet can be a target for hackers and therefore it needs to be protected. The bigger the clouds are, the bigger the risks and responsibilities are. This results in much greater need for proper security measures, as nowadays, this is the most important issue for potential customers.

Vendors should remember about the security of the physical data and host machine operating systems. They should not forget about maintaining the integrity of the hypervisor layer, preventing DoS attacks by using a proper resource management or implementing strong authentication, authorization and auditing mechanisms. Providing secure and consistent backups and restoration of cloud-based resources is also an important issue. Vendors should also provide the proper network security mechanisms and rules. Isolation of networks is the main concern in this matter.

No matter how well providers ensure the security of the data stored in the cloud, customers should also participate in its security. Customers should have a good firewall protection of their local networks. Administrators of Operating Systems, that run in the cloud should secure at least in the same manner as any other Operating System, that stores protected data. It is also vital to remember about the encryption of that data. Customers should not forget about passwords in their systems, which must be complex and frequently changed. Lastly, access to devices in the cloud should be controlled and rationalized. Lastly, ensuring the security of staff can be essential. They should undergo security check to avoid deliberate security breaches.

References

[1] Cloud computing. Encyclopedia Britannica Inc., 2012.

[2] Foster, I., Zhao, Y., Raicu, I., Lu, S.: Cloud Computing and Grid Computing 360-Degree Compared. In: Proceedings of Grid Computing Environments Workshop (GCE'08), pp. 1–10. 2008.

[3] Hausman, K., Cook, S. L., Sampaio, T.: Cloud Essentials. John Wiley and Sons, 2013.

[4] Ahson, S., Ilyas, M.: Cloud Computing and Software Services. Theory and Techniques. CRC Press, 2011.

[5] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M.: A View of Cloud Computing. Communications of the ACM, 53, pp. 50–58, 2010.

[6] IBM: What is cloud? http://www.ibm.com/cloud-computing/us/en/what-is-cloud-computing.html, 2009.

[7] Viswanathan, P.: Cloud Computing Is it Really All That Beneficial? Advantages and Disadvantages of Cloud Computing. http://mobiledevices.about.com/od/additionalresources/a/Cloud-Computing-Is-It-Really-All-That-Beneficial.htm.

[8] Velte, T., Velte, A., Elsenpeter, R.: Cloud Computing, A Practical Approach. McGraw-Hill, Inc. New York, NY, USA, 2010.

[9] Grance, T., Jansen, W.: Guidelines on Security and Privacy in Public Cloud Computing. NIST, US Department of Commerce, 2011.

[10] Wang, Q., Wang, C., Li, J., Ren, K., Lou, W.: Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing. In: Computer Security ESORICS 2009, LNCS, volume 5789, pp. 355–370. Springer, 2009.

[11] Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34, p. 111, 2011.

[12] Zissis, D., Lekkas, D.: Addressing cloud computing security issues. Future Generation Computer Systems, 28, p. 583592, 2012.

[13] Krutz, R. L., Vines, R. D.: Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley Publishing, 2010.

[14] Yang, K., Jia, X.: Security for Cloud Storage Systems. Springer, 2014.

[15] ENISA: Cloud Computing Risk Assessment. *http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment*, 2009.

[16] VMWare: Securing the Cloud A Review of Cloud Computing, Security Implications and Best Practices. Whitepaper, 2011.

[17] CloudU: The Elephant in the Room, Cloud Security and What Vendors and Customers need To Do To Stay Secure. Diversity Limited, 2011.

[18] Winkler, J. R. V.: Securing the Cloud. Cloud computer security techniques and tactics. Syngress, 2011.

[19] Cloud Computing Security – Best Practices. *www.ryerson.ca/ccs/itsecurity/CloudComputingSecurity*.

[20] Cloud Security Guidance. International Technical Support Organization Team, IBM Recommendations for the Implementation of Cloud Security, 2009.

[21] Takabi, H., Joshi, J. B. D., Ahn, G.-J.: Security and Privacy Challenges in Cloud Computing Environments. Security & Privacy, 8, pp. 24–31, 2010.

[22] Madavi1, T. J., Gawande, Y. V., Kale, M. B.: Security in Cloud Computing. In: Proceedings of the International Conference on Advances in Computer and Management. 2012.

[23] Goncalves, G., Poniszewska-Maranda, A.: Role engineering: from design to evaluation of security schemas. Journal of Systems and Software, 81, pp. 1306–1326, 2008.

[24] Poniszewska-Maranda, A.: Modeling and design of role engineering in development of access control for dynamic information systems. Bulletin of the Polish Academy of Sciences, Technical Science, 61, pp. 569–580, 2013.