Cloud Computing and its Challenges and Benefits in the Bank System

Bogdan NEDELCU, Madalina-Elena STEFANET, Ioan-Florentin TAMASESCU,
Smaranda-Elena TINTOIU, Alin VEZEANU
University of Economic Studies, Bucharest, Romania
bogdannedelcu@hotmail.com, mada.stefanet@gmail.com ,
ioan.tamasescu@gmail.com , alin_v12@yahoo.com , smarandat138@gmail.com

The purpose of this article is to highlight the current situation of Cloud Computing systems. There is a tendency for enterprises and banks to seek such databases, so the article tries to answer the question: "Is Cloud Computing safe". Answering this question requires an analysis of the security system (strengths and weaknesses), accompanied by arguments for and against this trend and suggestions for improvement that can increase the customers confidence in the future.
***Keywords**: Cloud Computing, Bank System, Security*

1 Introduction

Cloud computing has experienced a fast growth during the last years, and it is expected to keep developing more and more. Cloud services will be profitable in business application, which will transform services in cloud-based services. This change is needed especially for application like ERP (enterprise resource planning) or CRM (customer relationship management).

Banks are an important segment of business area that cloud computing is targeting in the next few years. Due to this type of business needs, cloud services must be similar with a "silver bullet". There are many advantages that cloud provides for banks as customers. First of all, cost savings, using cloud-servers instead of personal servers, will save a lot of money. Moreover, cloud provides: usage-based billing, business continuity, business agility, green IT.

Thus, nowadays cloud computing services has some disadvantages that stops banks to adopt the cloud, such as security, confidentiality of the data, and also quality of services.

2. Security strengths in cloud computing

Security is one of the biggest arguments used against the actual cloud computing system. However, cloud computing systems are often safer than mainframe systems managed at the local level, at least for small and medium companies (banks). This may list the strengths of cloud computing systems: private cloud, data centralization, multi-factor authentication, sharing security, economy of scale and others.

Private cloud is probably the most important argument in favor of using cloud computing systems by organizations (banks). An interesting comparison is between the current situation of internet banking and cloud computing. Security issues were also an inhibitor to adoption of internet banking[1] (about mid 90's), which can be considered a precursor of cloud computing. Similarly, as cloud computing providers who continue to address market concerns relating to safety, economy and convenience of cloud computing will become a commonplace like online banking and other online financial transactions today.

Fig.1.Cloud Security [1]

Despite the conventional and economical benefits, cloud computing may not be for everyone. For example, a security and risky perspective, public cloud computing may not appeal to organizations with missions like extreme advertisement and / or highly sensitive data. However, for most, cloud computing security advantages described above along with the ability to create private cloud (which allows customers to control who is in the cloud, where data is stored, who has access etc.) should provide the necessary security guarantees to satisfy most organizations.[2]

- *Centralization of data* falls into two categories: preventing leak of data and monitoring. Using back-up systems is inefficient in terms of time and at high risk of data loss through the physical degradation of the backup devices that visibly reduce clouds computing efficency while saving data and its potential.[2]
- *Multi-factor Authentification*: A sizable part of the cloud computing providers mainframe systems combines elements like passwords, hard token elements, biometric elements, increasing the security level. For many companies it is more profitable to resort to such a system than to implement its own cloud security system with these benefits.[1]
- *Security patching*: Cloud computing offers this concept and also offers the possibility of testing. There are organizations that do not have the resources to implement such a concept or that implementation would result in huge consumption of time, so the existence of the cloud system is a plus.[1]
- *Economy of scale*: IT services centrally managed and maintained to improve services and reduce operating costs. Cloud computing providers have the ability to invest in staff, resources and facilities that allow customers to pay only for what they use rather than invest in the resources to be managed and maintained over time. Thus, without repeating the Cloud features mentioned above, providing IT Cloud offers economies of scale, as the IT system must be scalable, fair and secure.[2]
- *Security certifications***:** Many industries require IT systems and facilities to maintain a certain type of information security and/or privacy certification. For example, compliance with the Federal Information Security Management Act, or FISMA, is required for the federal government while Health Insurance Portability and Accountability Action (HIPAA) compliance is required for the

healthcare industry. These certifications can be prohibitively expensive for smaller organizations to achieve; however, many cloud vendors provide access to systems and facilities that are already certified. Even if your business does not require a certification, it may be comforting to engage with vendors who offer them as it demonstrates mature business practices as it relates to information security.[2]

- *Physical security*: Reputable cloud computing vendors often host their systems in facilities that have much stronger physical security controls with meaningful certifications that many small-to-midsize companies cannot provide on their own.[1]
- *Reduce cost of testing security*: a SaaS provider only passes on a portion of its security testing costs. By sharing the same application as a service, you don't foot the expensive security code review and/or penetration test. Even with Platform as a Service (PaaS) where developers get to write code, there are potential cost economies of scale (particularly around use of code scanning tools that sweep source code for security weaknesses).[2]
- *Pre-hardened, change control builds*: this is primarily a benefit of virtualization based on Cloud Computing. Now it is the chance to start 'secure' (by your own definition) – create your Gold Image - VM and clone away. There are ways to do this today with bare-metal OS installs but frequently these require additional 3rd party tools, which are time consuming to clone or add another agent to each endpoint.
- *Reduce exposure through patching offline*: Gold images can be kept up to date securely. Offline VMs can be conveniently patched "off" the network.[2]
- *Easier to test impact of security changes:* Spin up a copy of your production environment, implement a security change and test the impact at low cost, with minimal startup time. This is a big deal and removes a major barrier to implement security in production environments.[2]
- Convenience and continuous availability: Public clouds offer services that are available wherever the end user might be located. This approach enables easy access to information and accommodates the needs of users in different time zones and geographic locations. As a side benefit, collaboration booms since it is now easier than ever to access, view and modify shared documents and files. Moreover, service uptime is in most cases guaranteed, providing in that way continuous availability of resources. The various cloud vendors typically use multiple servers for maximum redundancy. In case of system failure, alternative instances are automatically spawned on other machines. [3]
- Resiliency and Redundancy: A cloud deployment is usually built on a robust architecture thus providing resiliency and redundancy to its users. The cloud offers automatic failover between hardware platforms out of the box, while disaster recovery services are also often included. [3]

Other advantages of Cloud computing security, mention are: reliable access, automatic data backup and encryption features that are unique to each client.[1]

Cloud computing, as we have seen, can be a wonderful business enabler. However it is for a small business owner to calculate if it's the right fit for your current environment. If the limited risks can be properly managed, though, it promises cheaper, faster and more efficient ways of working which could help your business achieve stellar performance. [4]

3. Security issues in cloud computing

The intention to adopt cloud computing has increased rapidly in many organizations. Cloud computing offers many potential benefits to small and medium enterprises such as fast deployment, pay-for-use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, greater resiliency, and on-demand security controls. Despite these extraordinary benefits of cloud computing, studies indicate that organizations are slow in adopting it due to security issues and challenges associated with it. In other words, security is one of the major issues which reduce the cloud computing adoption. [5]

Organizations use the Cloud in a variety of different service models (SaaS, PaaS, IaaS) and deployment models (Private, public, hybrid, and community). There are a number of security issues or concerns associated with cloud computing, but these issues fall into two broad categories: security issues faced by cloud providers and security issues faced by their customers (companies or organizations who host applications or store data on the on the cloud.

For resolving these problems, the responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures. [6]

According to Takabi et al. (2010), cloud service providers and customers are responsible for security and privacy in cloud computing environments but their level of responsibility will differ for different delivery models. Infrastructure as a Service (IaaS) serves as the foundation layer for the other delivery models, and a lack of security in this layer affects the other delivery models. In IaaS, although customers are responsible for protecting operating systems, applications, and content, the security of customer data is a significant responsibility for cloud providers. In Platform as a service (PaaS), users are responsible for protecting the applications that developers build and run on the platforms, while providers are responsible for taking care of the users' applications and workspaces from one another.

In System as a Service, cloud providers, particularly public cloud providers, have more responsibility than clients for enhancing the security of applications and achieving a successful data migration. In the SaaS model, data breaches, application vulnerabilities and availability are important issues that can lead to financial and legal liabilities.

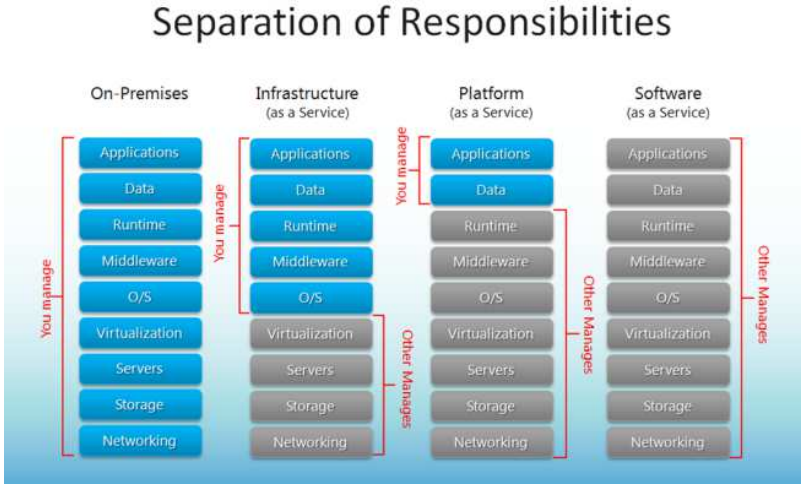

Fig 2. Separation of Responsibilities [5]

When an organization chose to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially business sensitive and confidential data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the third biggest threat in cloud computing. Therefore, cloud service providers must ensure that use background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity.

In order to conserve resources, cut costs, and maintain efficiency, cloud service providers often store more than one customer's data on the same server. As a result there is a chance that one user's private data can be viewed by other users. To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.

Over time, cloud providers are increasingly concerned about the security services, therefore, have implemented various ways of protection within the cloud community. [7]

Data Security - Data security is a common concern for any technology, but becomes a major problem when users SaaS providers must rely on the security itself. In SaaS, organizational data are often processed and stored in clear text in the cloud. SaaS provider is directly responsible for their safety as long as they are stored and processed. The best way is to encrypt their data security, the client, or that the client alone can be clearly read in the data. But the most commonly used method of data security backup is increasingly used lately. Also, the backup can raise large problems when providers of cloud backup services contracted to third persons or companies. But encryption itself is not a complete solution, because at some point, the data will be decrypted to be processed or to carry out the specific tasks.

A truly viable solution for data security is also more detailed filtering sites especially web content - this of course requires high costs for implementation of cloud providers.

There are complex data security challenges in the cloud:

- The need to protect confidential business, government, or regulatory data
- Cloud service models with multiple tenants sharing the same infrastructure
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- Lack of standards about how cloud service providers securely recycle disk space and erase existing data
- Auditing, reporting, and compliance concerns
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management

A new type of insider who does not even work for your company, but may have control and visibility into your data

But encryption itself is not a complete solution, because at some point, the data will be decrypted to be processed or to carry out the specific tasks.

A truly viable solution for data security is also more detailed filtering sites especially web content - this of course requires high costs for implementation of cloud providers.

There are complex data security challenges in the cloud:

- The need to protect confidential business, government, or regulatory data
- Cloud service models with multiple tenants sharing the same infrastructure

- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- Lack of standards about how cloud service providers securely recycle disk space and erase existing data
- Auditing, reporting, and compliance concerns
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
- A new type of insider who does not even work for your company, but may have control and visibility into your data

Specific security challenges pertain to each of the three cloud service models—Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

- SaaS deploys the provider's applications running on a cloud infrastructure; it offers anywhere access, but also increases security risk. With this service model it's essential to implement policies for identity management and access control to applications. For example, with Salesforce.com, only certain salespeople may be authorized to access and download confidential customer sales information.
- PaaS is a shared development environment, such as Microsoft™ Windows Azure, where the consumer controls deployed applications but does not manage the underlying cloud infrastructure. This cloud service model requires strong authentication to identify users, an audit trail, and the ability to support compliance regulations and privacy mandates.
- IaaS lets the consumer provision processing, storage, networks, and other fundamental computing resources and controls operating systems, storage, and deployed applications. As with Amazon Elastic Compute Cloud (EC2), the consumer does not manage or control the underlying cloud infrastructure. Data security is typically a shared responsibility between the cloud service provider and the cloud consumer. Data encryption without the need to modify applications is a key requirement in this environment to remove the custodial risk of IaaS infrastructure personnel accessing sensitive data.[8]

Techniques for Protecting Data in the Cloud

Traditional models of data protection have often focused on network-centric and perimeter security, frequently with devices such as firewalls and intrusion detection systems. But this approach does not provide sufficient protection against APTs, privileged users, or other insidious types of security attacks. Many enterprises use database audit and protection (DAP) and Security Information and Event Management (SIEM) solutions to gather together information about what is happening. But monitoring and event correlation alone do not translate into data security. At a time when regulation and compliance issues are at an all-time high, it's dangerous to assume that monitoring, collecting, and storing logs can protect the organization from security threats, as they are reactive controls. In today's environment, both data firewalls and data security intelligence are essential to adequately protect the enterprise from new and different types of attacks. Best practices should include securing sensitive data, establishing appropriate separation of duties between IT operations and IT security, ensuring that the use of cloud data conforms to existing enterprise policies, as well as strong key management and strict acces policies.

"It is important to utilize security controls that protect sensitive data no matter where it lives, as point solutions by their very nature provide only limited visibility," says Tumulak. He emphasizes that an effective cloud security solution should incorporate three key capabilities:

- Data lockdown
- Access policies
- Security intelligence

Security applications - Applications are typically delivered through a web browser. Any application vulnerabilities can create problems in the SaaS services. These security issues are no different than any other web technology, but traditional solutions have proven ineffective. Therefore, The Open Web Application Security Project (OWASP) has identified the top 10 problems and tried to offer viable solutions.

Studies indicate that most websites are secured at the network level while there may be security loopholes at the application level which may allow information access to unauthorized users. Software and hardware resources can be used to provide security to applications. In this way, attackers will not be able to get control over these applications and change them. XSS attacks, Cookie Poisoning, Hidden field manipulation, SQL injection attacks, DoS attacks, and Google Hacking are some examples of threats to application level security which resulting from the unauthorized usage of the applications.[9]

4. Changes needed in Cloud Computing

Cloud computing security or, more simply, cloud security is an evolving sub-domain of computer security, network security , and, more broadly, information security.It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management. The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:

Deterrent controls

These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed.

Preventive controls

Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

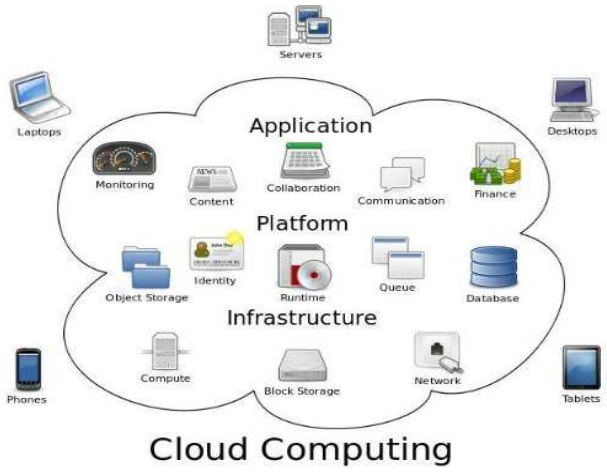

Fig. 3. Cloud Computing [9]

Detective controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue. System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.

Corrective controls

Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.[10]

The For Steps to a Secure Cloud Deployment

Most IT executives think cloud computing is a way to reduce capital expenditures by using virtualization technology. Many vendors tack the word "cloud" onto any Internet service. For our purposes here, we're using the GARTNER Inc. description of how the cloud came to be so important to business: "the commoditization and standardization of technologies, in part to virtualization and the rise of service-oriented software architectures, and most importantly, to the dramatic growth in popularity of the Internet." This is important in four specific areas:

1. *Centralized data management, using SharePoint as an example*
2. *Centralized application management, using Exchange as an example*
3. *Federated identity management, using Active Directory Federation Services (ADFS) as an example*
4. *Additional assistance for migrating to the cloud*

Centralized Data Management

In 2007, Gartner began telling security conferences it was time to abandon the hardened perimeter boundary between the enterprise and the Internet. Even at that time, experts were arguing that enterprise boundaries were already porous. Perimeters had become irrelevant to the task of keeping out intruders, so access control was required with every IT service. Security de-perimeterization is the current reality. To be truly secure, only the server that contains data can ultimately control access.

Still, it isn't rational to manage access at every server, because many deployments contain hundreds or even thousands of servers. IT can't really determine data

rights and access rules. IT can, however, establish a role-management system with which business owners can permit or deny access relevant to business objectives.

The regulatory environment has become increasingly stringent both for data modification and data access. This requires a new paradigm: one that will allow data to migrate to whichever server is best able to service access requests, while ensuring compliance at reasonable cost. Here are some requirements to consider for data management in a cloud environment:

- Fast access to data for which the user is authorized, and when and where it is required
- Access not compromised by a natural or business catastrophe
- Data discovery by legal governmental requests, assuming the enterprise can provide the data needed
- Data Loss Prevention (DLP) is an integral part of the service offering
- A service-oriented architecture (SOA) should enable easy data migration back and forth to the cloud
- Identity of data must not include its physical location, so that the data can easily be moved
- Location tags for data should be the logical country of origin, not the data's physical location
- Data backup and recovery operations need to be based on the data identity, not its location
- Data-access rules can be created and maintained by the business owner of the data
- Access permissions can be viewed by compliance auditors
- Sensitive data can have audit controls for both modification and access
- Separation of duties prevents the same administrator from modifying data and audit logs
- Service Level Agreements (SLAs) need to spell out everyone's expectations and responsibilities

Starbucks Corp. found that the cost and delay of physical (paper-based) distribution of current pricing, business analysis and news was not cost-effective. As a result, it now supports SharePoint for its network of 16,000 locations. That SharePoint site has become a business-critical communications channel through which employees can get current information, with the ability to search quickly for the information that they need when they need it.

Availability and reliability is tracked with Microsoft System Center of Operation Manager (SCOM) and other analytic tools. Because SharePoint supports both internal and external network connections, the server locations can adapt to suit the current network topology without concern for local, cloud or mixed environments. This deployment has enabled Starbucks to realize the following benefits:

- Supporting store growth and capacity needs by improving system stability with effective monitoring and reporting tools
- Allowing store partners to work more efficiently and effectively with an intuitive portal interface and easy access to information across the enterprise
- Maintaining data security with enhanced document management and privacy functionality
- Aligning store priorities with company objectives by integrating trends and growth reports with partner communications

Integrity Protection

Any data store must be prevented from becoming an infection vector for viruses or spyware. Data types, like executables and compressed or encrypted files, can be blocked for a variety of integrity and compliance concerns. Microsoft employee David Tesar blogged about some of the

business reasons to protect SharePoint using ForeFront Protection 2010 for SharePoint, which was released in May 2010.

Data Loss Protection and Detection

To ensure full protection, data from one customer must be properly segregated from that of another. It must be stored securely when "at rest" and able to move securely from one location to another (security "in motion"). IT managers must ensure that cloud providers have systems in place to prevent data leaks or access by third parties. This should be part of an SLA. Proper separation of duties should ensure that unauthorized users can't defeat auditing and/or monitoring—even "privileged" users at the cloud provider. [11]

5. Banks and Cloud Computing

To maintain and achieve better performance in the future, banks around the world will have to adopt and master two fundamental changes:

1. The first transformation consists in changing product offerings, customer service should reflect the fact that the consumer is in control. Nowadays, the consumer is impatient and wants to be fully in control after interaction with the internet where he can do what he wants.
2. A second transformation consists in reshaping and reinventing core banking operations to enable a model Economic Competitiveness, efficient and sustainable business.

The reasons for banks to move to the cloud are many but the most important reason is the multitude of applications. Using Cloud, banking institutions pay only for the services they use .This is easier and more efficient to test new applications on the Cloud to traditional infrastructure. [12]

Models in Cloud

Cloud offers three different service models:

Platform-as-a-Service (PaaS)

In the PaaS model, cloud providers deliver a computing platform which can be accessed via web browsers, typically including an operating system, programming language execution environment, databases, and web servers. [13][14]

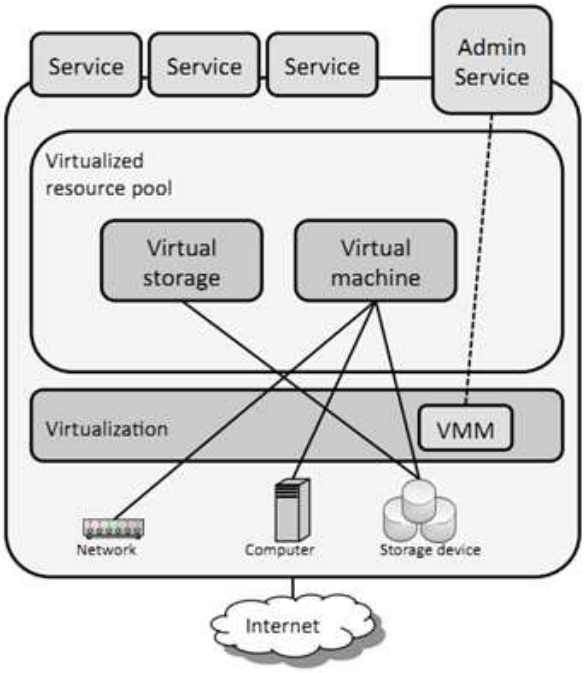

Fig. 4. PaaS model [15]

Software-as-a-Service (SaaS):
SaaS is a cloud service that provides some data and software that are accessed via a web connection. Types of software that can be delivered this way include accounting, customer relationship management, enterprise resource planning, invoicing, human resource management, content management, and service desk management. [13][14]

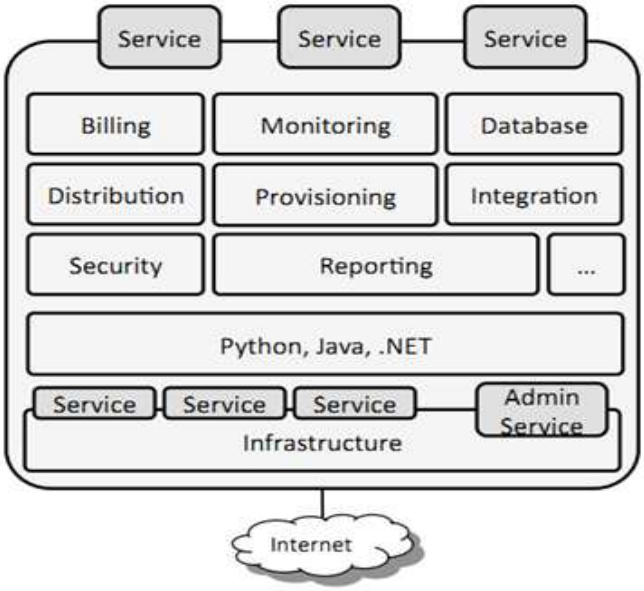

Fig. 5. SaaS model [15]

Infrastructure-as-a-Service (IaaS)
This cloud model offers a full service outsourced packages without the necessity of buying a server, software, data center space or any network equipment. [13][14]

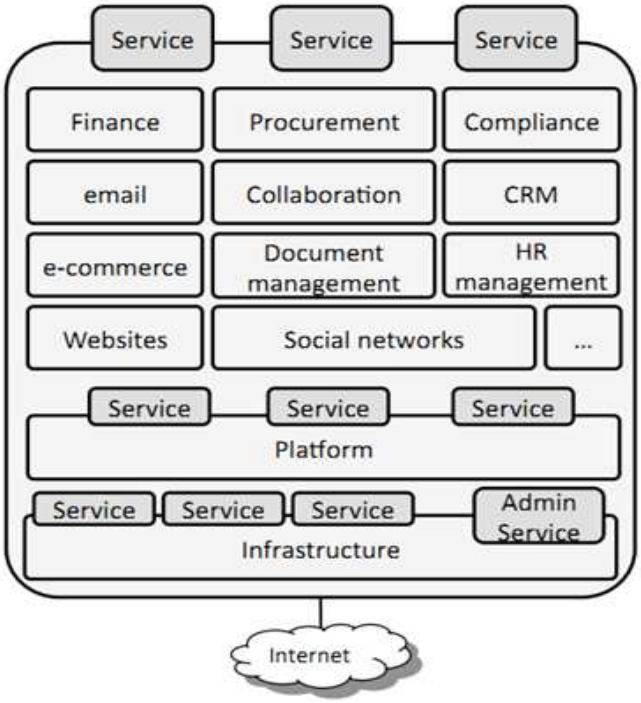

Fig. 6. IaaS model [15]

Business Process-as-a-Service (BPaaS)
BPaaS combines all the other service and it is used for billing, payroll and human resources.

Banking Industry Trends:
What the banks do not understand, and it is difficult to switch to another way to run things, is that the customer can't be controlled. This is known by the new banks using online platforms for its customers.
Banks need to look at the things from the outside, from the point of view of the consumer, to change something in the banking system.
Offering services that best fits the character and needs of each individual, banks want to replace the information offices and queues. [12]
Private cloud has come to dominate core banking. Banks are aware of the potential security breach or disruption in areas such as transactions and withdrawals by utilizing ATM. Banks must keep its core banking processes under control in their database to know when data are used. [12]

5.1. Pros for actual level
1. *Reduced costs*: using cloud banks do not have to invest so much in the software, hardware and labor. [16]
2. *Highly flexible*: Cloud Platform provides the ability to respond quickly to market changes, customer needs but also to respond quickly technological. Capacity will be an important competitive advantage. [16]
3. *Faster customer service*: Free Cloud services and products developed and released easily. Banks will be able to increase computing power to meet peak demand without having to improving technology. [16]
4. *It strengthens the relationship between customer and bank*: The combination of Big Data and unlimited computing power will allows to banks to develop systems that will make better decisions for their clients. [16]
5. *It brings customers closer to the banks*: transactions between buyers and sellers will be done easily at the moment. La more work needed to process the payments are inefficient because they use different technologies. This deficiency can be remedied in the Cloud. [16]

5.2 Cons for actual level
1. *Security and Privacy* - These two concepts are the most important when it comes to date. Keeping in mind that your client entrusts his personal data, shows a very high confidence and the bank must ensure the security and confidentiality of date. Cloud does not stay in this chapter, and this was mentioned by the founder of the cloud, Rajat Bhargav: "When you use cloud, you have a network that is open to the rest of the world. Cloud is more insecure than it was the repository data to headquarters." [17]
2. *Downtime* outages and downtime data, this is due to internet connection. [19] A disconnect from the network or from the Internet for a few minutes has a huge impact on a bank because, most likely, in time occur certain transactions or other exchanges of information that are lost in a year time.
The types of losses [18]:

- *Loss of the application service*: very much depends on the application and the bank branch.
- *Data loss*: if such an incident data may be lost and this has a financial impact but also legal

3. Vulnerability: We have to consider that any system is vulnerable to cyber-attacks, and banks in turn are not protected from hackers. Public and private clouds can be affected by both malicious attacks and infrastructure failures such as power outages. Such events can affect Internet domain name servers, prevent access to clouds or directly affect cloud operations. [19]

6. Opportunities

Since there are many doubts and suspicions about the security of cloud computing systems, opportunities for them to be integrated into banking systems (or in large organizations) appeard, once new methods of increasing the level of security were developped. Some of the possibilities of increasing security are: Kerberos authentication servers, firewall, VPN systems and virtualization.

The most powerful and widely used authentication service is Kerberos Authentication Server world. It was created in the project Athena, Get MIT (Massachusetts Institute of Technology). It allows users to communicate on the network to disclose their identity and to authenticate, preventing Iiniilor listening situations. Kerberos performs data security through encryption. The Kerberos is an authentication protocol based on a trusted authority called trusted third party (trusted third party). Kerberos works by providing the users or service vouchers, which are used for identification, and some cryptographic keys required for secure communication network. The Kerberos system is a relatively inexpensive option, but that ensures a better level of security.[21]

In general, a firewall (sometimes called bridge security) is a system that requires access control policy between two networks. A firewall is to implement this policy in terms of network configuration, one or more host systems and routers with special functions, other security measures such as customer authentication cryptographic methods. In other words, a firewall is a mechanism used to protect a trusted network from the point of view of security unsecure, we can not trust. Typically, one is the internal networks of organizations / banks (safe, reliable), while the other is network Cloud (they do not have confidence in terms of security) .[22]

VPNaaS (Virtual Private Network as a Service) is a solution of different market requirements: companies / banks want their mobile employees can access their internet network through a solution managed and controlled. For economic reasons desired VPN Cloud outsourcing providers by this system. NCP (Next Generation Network Access Technology) is a VPN solution which complies with the requirements and desires of suppliers and users, bringing benefits to both parties. Another plus for using VPNs in Cloud, considering the parallel made above with Internet banking is that banks offering Internet Banking systems used internally VPN systems to ensure greater data security. [23]

Another opportunity for cloud computing is virtualization. Virtualization is software that separates physical infrastructures to create various dedicated resources. It is the fundamental technology that powers cloud computing. "Virtualization software makes it possible to run multiple operating systems and multiple applications on the same server at the same time," said Mike Adams, director of product marketing at VMware, a pioneer in virtualization and cloud software and services. "It enables businesses to reduce IT costs while increasing the efficiency, utilization and flexibility of their existing computer hardware." In contrast, with virtualization, companies can maintain and secure their own "castle", Rick Philips said. This "castle" provides the following benefits**:**

- *maximize resources* — Virtualization can reduce the number of physical systems you need to acquire, and you can get more value out of the servers. Most traditionally built systems are underutilized. Virtualization allows maximum use of the hardware investment;
- *multiple system* — With virtualization, you can also run multiple types of applications and even run different operating systems for those applications on the same physical hardware;
- *IT budget integration* — When you use virtualization, management,

administration and all the attendant requirements of managing your own infrastructure remain a direct cost of your IT operation. [20]

7. Conclusions

In recent years, cloud computing has grown considerably and services offered increasingly better, this development will not stop.

Expanded areas where most is the bank has expanded greatly in this area because it offered many advantages as a customer.

The advantages are: cost saving, using cloud servers and applications and platforms made available instead of using personal servers and software purchased from specialty companies in banking will save a lot of money

But unfortunately like any tool it has drawbacks, the most common drawback in cloud computing is security and downtime. Considering the fact that we are in the 21st century nothing is safe as long as it is in a database, it can be broken easily by people specialized in IT, cloud computing has therefore created a model , private cloud, especially for banking institutions to avoid problems with security.

And about the downtime this is very difficult to avoid because not only refers to the banking system but in all market areas by using a network.

Cloud computing and cloud infrastructure have become a great ally for some areas, very popular after market, these areas are the banking and mobile networks as well as that of small and medium enterprises.

References

[1] “Security Advantages of Cloud Computing “, John Wood & Rick Tracy, 25.01.2011, unpublished

[2] “Assessing the Security Benefits of Cloud Computing”, Craig Balding, 21.07.2008, unpublished

[3] “Advantages and Disadvantages of Cloud Computing – Cloud computing pros and cons”, Ilias Tsagklis, 23.04.2013

[4] “Cloud computing & small businesses security -pros and cons”, Dan Conlon, Trend Micro, 2011

[5]”Cloud Computing Security – Network and Application Levels" - CloudTweaks.com

[6] From Wikipedia, the free encyclopedia - article "Cloud computing security"

[7] "Cloud Computing Security – Network And Application Levels" - Mojgan Afshari - senior lecturer in the Department of Educational Management, Planning and Policy at the University of Malaya

[8] "Cloud computing and application security: Issues and risks" - Kevin Beaver, CISSP-independent information security consultant

[9] "Data Security in the Cloud" - Vormetric si Custom Solution Grup

[10] “Cloud computing security" - wikipedia

[11] "Cloud Security: Safely Sharing IT Solutions" - Dan Griffin, Tom Jones

[12] A new era in banking - Cloud computing changes the game - Accenture

[13] Cloud Computing in Banking - Capgemini

[14] Cloud computing - Wikipedia

[15] WHAT ARE SERVICE MODELS IN CLOUD COMPUTING? - CLOUD COMPETENCE CENTER

[16] Six reasons why cloud computing will transform the way banks serve clients – and the five hurdles to overcome – bankingtech.com

[17] Cloud computing is the future but not if security problems persist- tech time

[18] Downtime, Outages and Failures - Understanding Their True Costs - Martin Perlin

[19] Advantages and Disadvantages of Cloud Computing – Cloud computing pros and cons - Illias Tsagklis

[20] “Virtualization vs. Cloud Computing: What's the Difference?” - Sara Angeles, Business News Daily, 2014

[21][22] „Securitatea arhitecturilor de tip Cloud” - Cloud Computing, Clubul Informaticii Economice - Cyber Knowledge Club, pg. 57-58 , 62-63

[23] „NCP's Cloud VPN Solution - Provider and Users on Cloud Nine”, NPC Network Communications Products engineering GmbH, 2014

Bogdan NEDELCU graduated Computer Science at Politehnica University of Bucharest in 2011. In 2013, he graduated the master program “Engineering and Business Management Systems” at Politehnica University of Bucharest. At present he is studying for the doctor's degree at the Academy of Economic Studies from Bucharest.

Madalina-Elena STEFANET studies at Academy of Economic Studies from Bucharest, Faculty of Cybernetics, Statistics and Economic Informatics since 2013.

Ioan-Florentin TAMASESCU studies at Academy of Economic Studies from Bucharest, Faculty of Cybernetics, Statistics and Economic Informatics since 2013.

Smaranda-Elena TINTOIU studies at Academy of Economic Studies from Bucharest, Faculty of Cybernetics, Statistics and Economic Informatics since 2013.

Alin VEZEANU studies at Academy of Economic Studies from Bucharest, Faculty of Cybernetics, Statistics and Economic Informatics since 2013.