

## Data security model in cloud computing

Ivan Kashukeev, Stoyan Denchev, Ivan Garvanov  
University of Library Studies and Information Technologies, Bulgaria  
ikashukeev@gmail.com, s.denchev@unibit.bg, i.garvanov@unibit.bg

**Abstract:** *In the last decade, cloud computing has become an extremely important business assistant that offers significantly lower costs than traditional computer-aided resource provision and greater adaptability to business changes. Thus, it helps them to achieve their business goals. The development of cloud computing poses significant risks, which serve as a partial barrier to their use by the businesses. Security and protection of information are considered to be one of the most critical points in the use of cloud computing. Compared to traditional solutions, cloud computing moves application software and databases to large data centers where information and service management are not always secure and reliable. As a result of this, the community and businesses have many concerns and questions about the security of data and applications in cloud infrastructures. In addition, concerns about data security and applications also arise due to the fact that both user data and applications are managed by the cloud provider. Clouds typically use a standardized data and application security architecture, while the demand for consumer and business services is steadily growing and becoming more diverse and with more sophisticated software design that leads to continuous upgrades to data security models in cloud computing. Due to the different methods of implementation in cloud computing service delivery models, the demand for a reasonable level of data protection is of utmost importance. The purpose of this publication is to propose a new information security model, which offers a solution for improving the use of sensitive data by introducing a three-factor authentication – an improvement of preventive control.*

**Keywords:** CLOUD SERVICES, INFORMATION SECURITY, CLOUD SERVICES ARCHITECTURE, CLOUD SECURITY, DATA SECURITY MODEL

### 1. Introduction

In the traditional calculation model, the data and software are saved entirely on the user's computer, while in the cloud model the user's computer may contain almost no software or data [1]. Cloud technologies are based on the idea that applications and software can be completely moved to an "invisible" place with shared resources on the Internet [2]. Cloud services offer a virtual platform of flexible shared resources (such as hardware, software and datasets), which are provided dynamically on demand with minimal effort made by users [3]. The main features of cloud services are the following [4]:

- Resource flexibility: Users and businesses can add or remove given resources on the basis of their immediate need. For example, at peak times, they can use more resources, which can be easily and quickly released during the rest of the time;
- Pay-as-you-go: Users pay only for the resources they use, as well as for the time they use them and for the other parameters;
- Multi-tenancy (Shared resources): Cloud services are based on a business model, whereby resources are shared at different levels - e.g. a network layer and an application layer. This means that numerous users use the same resources;
- Self-hiring of resources: Users can hire additional resources independently without much efforts (memory, software, network resources, etc.);
- Extremely scalable: Cloud technologies enable scaling up to tens of thousands of systems, as well as server space and memory.

To find a sufficiently suitable data security model in cloud technologies and especially models related to it is a particularly difficult task in today's ongoing changes in businesses and the IT sector.

Sh. Ajoudanian, for example, proposes a new data security model based on the CIA triad (Confidentiality, Integrity, Availability) and shows the role of the respective user and provider for each model [5]. However, the proposed model does not guarantee the security of sensitive data, as it allows simple user authentication. If you aim at a higher level of data security and protection, such as very sensitive data of an organization or entity, particular attention should be paid to authentication, which is not considered in the proposed model.

Another new data security and protection model is proposed by M. Mohamed, who considers three layers [6]: In the first layer, he proposes the authentication to be placed; in the second layer, he puts encryption of information, data integrity and protection for private users; and in the third layer, he proposes fast data recovery to be provided.

With the proposed model, the problem of sensitive data is partially resolved but the question remains as to whether it can be widely used. There is also a problem in terms of hybrid clouds, for example, if an organization has a private, public and community cloud, how will the three clouds be authenticated and how will the community and private clouds be protected, if the user logs in through the easily accessible public cloud and tries to gain unauthorized access to the other two hybrid clouds.

The Internet is not a place that cloud service providers can fully control and manage, which requires additional methods and techniques to ensure the security and protection of all participants in the cloud infrastructure.

The security of information and cloud infrastructure participants is of paramount importance to any cloud service provider and organization. As cloud technologies use a virtual environment, particular attention should be paid to the inherent risks, vulnerabilities and threats that threaten the security and protection of information and programs and differ significantly from the inherent risks, vulnerabilities and threats of a physical system.

This publication proposes a new data security model that improves the preventive control and the use of sensitive data by introducing three-factor authentication.

### 2. Security of service delivery models in cloud computing

Due to the specifics of each service delivery model in cloud technologies, the security is considered according to SLAs between the user and the provider for each of the following three main models:

#### 1. Software as a Service

With this model, users pay a subscription for a software product, whereby part of the information or the full information is saved on a remote location and users can access this service via the Internet [7].

With SaaS, users do not have any control or authority to modify or manage cloud infrastructures or even specific applications that

are already developed [8]. Users have limited options to configure settings related to the use of these applications. The provider fully controls the cloud infrastructure and is responsible for the confidentiality, integrity and accessibility of the data and information.

**2. Platform as a Service**

This model enables users to develop their own cloud infrastructure applications using programming languages and additional software tools, which are provided by the cloud service provider (such as .NET, Ruby, Java, etc.). PaaS provides users with all the resources they need, so as to be able to develop applications and services entirely on the Internet without the need to download or install additional software. The user is not yet able to manage the underlying cloud infrastructure but only the applications developed by him/her [7].

One disadvantage of PaaS is the lack of interoperability and transfer of applications, which are already developed by the user, to other providers. I.e. if the user wants to transfer the applications developed with the current provider to another cloud provider, this cannot be done or if it can be done, the costs will be extremely high. Another disadvantage is that if the provider decides to leave the business, the applications and information in them will be deleted. With this model, the providers' liability is associated only with the integrity and accessibility of data. The user is responsible for the confidentiality and protection of the information.

**3. IaaS**

The infrastructure as a service allows the respective organization to create its own software environment. In the SaaS and PaaS models, the provider provides the user with applications but in the IaaS model, this is not done [7]. This model only provides the hardware on which the organization can install whatever it wants.

The control, exercised by providers, is at an extremely low level. They are only responsible for the accessibility of the services provided by them. Compared to providers, the users' responsibility is at a quite high level. They are responsible for the confidentiality, integrity of the data and its protection. The following table shows the responsibilities of cloud service providers and users for each model.

Before an updated version of a data security model in cloud technologies is proposed, the evolution of cloud technologies should be known very well, as well as their advantages and disadvantages. The following figure shows the overall development of these technologies by years.

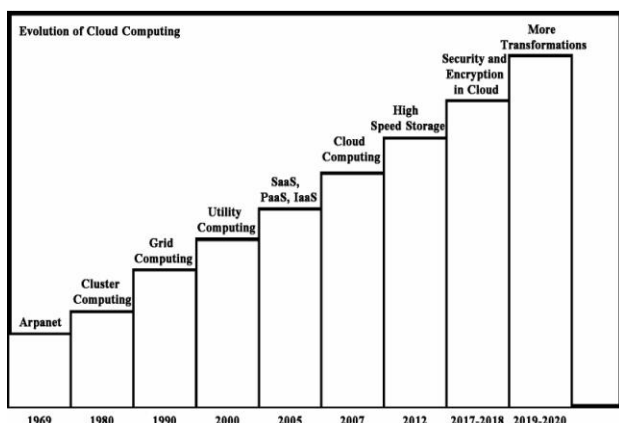


Figure 1. Evolution of Cloud Computing

The beginning of cloud technologies dates back to 2005, when the main models for the provision of cloud services were presented for the first time, namely the Software as a Service, Platform as a Service and Infrastructure as a Service. Subsequently, Cloud technologies began to focus more on data storage, accessibility and

other indicators. In 2012 the main goal was to increase the data and information storage speed (High Speed Storage).

In early 2016, cloud technologies encountered one of the biggest problems in this field, which have not yet been resolved - security and protection of information and data. Figure 1 also shows that the main work done in 2017 and 2018 focused on ensuring security and protection of these technologies.

In recent years, emphasis has been placed on creating more possibilities and transformations in cloud technologies, such as productivity, speed, security, etc. Unfortunately, the problem with the security and protection of these technologies remains unresolved.

In cloud service delivery models, it is important to properly allocate the responsibilities of the user and the provider for each model. Table 1 presents these responsibilities with respect to the so-called CIA triad.

Table 1. Responsibility of providers and users in cloud computing models

	Provider	User
Software as a Service	Confidentiality, Integrity and Availability	X
Platform as a Service	Integrity and Availability	Confidentiality
Infrastructure as a Service	Integrity	Confidentiality and Availability

As it can be seen in the table, for each model, the responsibilities of the user and the provider are different. For example, in case of the most widely used model globally - the Software as a Service - the provider is required to ensure the confidentiality, integrity and accessibility of data and information, while the user has no responsibilities. These are the so-called services or products for which a subscription fee is payable for the right to use the product or service. All new versions, patches, new modules, security and data protection, information, etc. are the sole responsibility of the provider of cloud services or products. In the other two models, the responsibility is divided between the provider and the user. For example, in case of the Infrastructure as a Service, the responsibility of the provider is only to ensure the integrity of the data and information (i.e. the provision of basic resources). Any other things are the responsibility of the user.

**3. Information security in cloud computing**

With the development of modern information technologies and systems, the problem of data security and protection remains one of the biggest problems of the 21st century. It is a particularly sensitive issue of cloud technologies and related service delivery models.

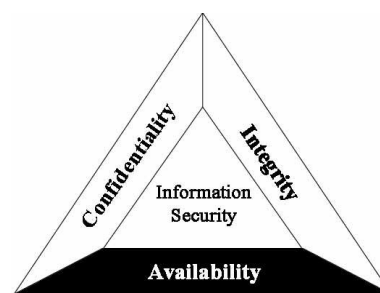


Figure 2. CIA triad of Information Security

To secure information in cloud technology, we should consider the main information security triad, the so-called CIA triad.

On the basis of this triad, all modern models of information security are considered.

### 1. Confidentiality of information in clouds

Information confidentiality aims to prevent disclosure of information by unauthorized users or systems. There are two categories of privacy in cloud infrastructure: privacy in a private cloud and privacy in a public cloud. Private cloud privacy is not a major concern, as it relates to private networks in an organization. There are several privacy issues with public clouds. The first one concerns controls of authentication and authorization. As numerous users use public clouds, they must be properly authenticated in the system by additional rigorous policies and procedures in addition to username and password controls. Some of the most up-to-date security models aim at either two-factor or three-factor authentication or web proxy logon [8] using Security Assertion Markup Language (SAML). With SAML, each organization manages its users by using trusted links to share authentication between sites. SAML is a very good solution for scaling up authentication. It uses the so-called Single sign-on, which is a process by which the user enters a username and a password to access numerous sites/applications with the same data securely and reliably [9].

### 2. Data Integrity in Clouds

Data integrity is the overall accuracy, completeness, and consistency of data. Data integrity also refers to the safety of data. Data integrity is not only whether the information is correct but whether it is reliable. In addition to this, users often use different cloud service providers and in some cases there is no guarantee of data security at the input and transaction management levels. Cloud providers must implement data integrity standards in their cloud services [9]. Some of the data integrity standards for today's cloud services are Data Integrity Field (DIF), SNIA Cloud Management Interface (CDMI), XML Based Solutions, etc.

### 3. Availability of Data in the Cloud

Data availability is the process of ensuring that data is available to end users and applications, when and where they need it. It defines the degree or extent to which data is readily usable along with the necessary IT and management procedures, tools and technologies required to enable, manage and continue to ensure data availability. One of the most significant security challenges for cloud technologies is the availability of data. Many providers aim at improving the availability of cloud infrastructures. There are several ways to improve the accessibility of cloud services. One of them is to provide users with back up information. A better option is to provide them with a caching proxy server that can respond to queries without contacting the specific server using content retained from a previous request by the respective user or even by another user. Another option is the transfer data from an online server to a so-called "hot" server that always has the contents of a cloned server and in case of a server failure, the user's information is not lost [10-13].

### 4. A new data security model in cloud computing

The development of the new data security model in cloud technologies and related service delivery models is based on the CIA triad for cloud services, which is described above. The CIA shows the responsibilities of providers and users for each of the three most widely used cloud service delivery models. For example, in the case of the most widely used model globally – the Software as a Service, privacy, data integrity and availability are the sole responsibility of the provider of cloud services or products. For the other two models – the Platform as a Service and Infrastructure as a Service, the responsibilities are allocated differently between the user and the provider, as shown in Table 1. In this allocation, the

most significant problem with cloud technology remains - the problem of data security and protection.

The new data security model aims at increasing the level of security of data and programs by checking users with the so-called three-factor authentication from another server. Three-factor authentication uses a combination of the following methods:

- **something the user knows:** it is a symbolic sequence that is known only to a given user and is unknown to others. When it is claimed with the user ID, it is taken as proof of possession of the identity. Typical examples of something known are passwords, PINs, private keys, etc. The most common and accessible means of authentication are passwords, which are a sequence of characters chosen by the system administrators or by the users themselves.
- **something the user owns:** it is a material object (card or other medium) on which additional information is usually recorded. In the process of authentication, the user claims the owned object by placing it in a device that can read its contents and confirm or reject the declared identity. Such techniques, for example, can help authenticate users using electronic signatures to share information with different institutions.
- **biometric data:** it represents unique data that can belong to only one individual. Fingerprints, iris, retina, voice recognition, etc. can be included in this category.

The model achieves a higher degree of security, as it focuses mainly on the preliminary control – the highest degree of efficiency. SSL or IPsec, as well as DoS protection, are added here.

The model also uses the so-called Single sign-on, which also requires authentication from an external server. Once the user is admitted to the system (cloud), he/she can access all cloud infrastructures in the environment (private, public, community) through Single sign-on without the need to enter authentication data again. That is, once a user is successfully admitted to the cloud infrastructure, this means that he or she has successfully passed the three-factor authentication described above and has the right to use his or her access to enter other cloud infrastructures in the environment, without the need to authenticate to each cloud individually (as it will be the case without a Single sign-on).

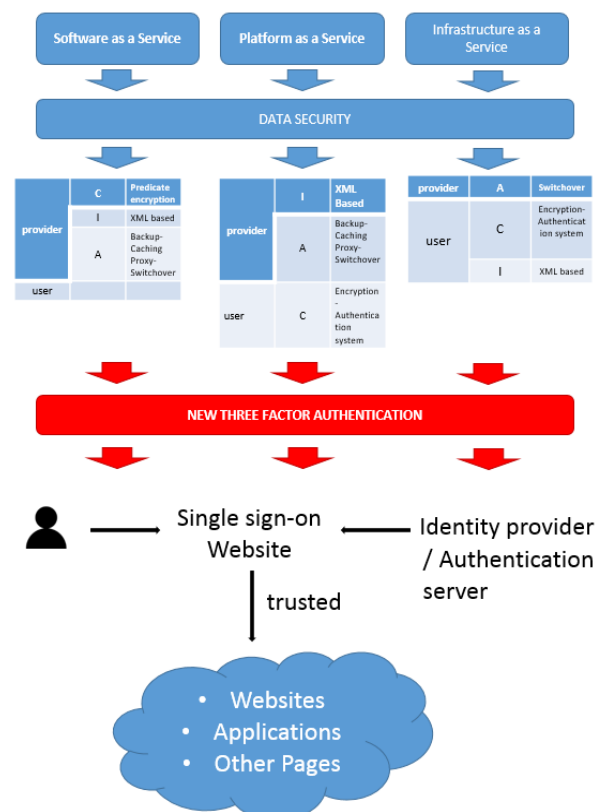


Figure 3. A New model for data security in cloud with three-factor authentication (based on CIA triad)

The model encrypts the information before it sends it to users by SSL, IPsec protocols. Another improvement of the model is that authenticated users and end users cannot be eavesdropped, which guarantees a high degree of confidentiality of the model. The model is mainly used in a cloud environment that requires maximum security and protection of data and information and enables the successful collection of biometric data.

Cloud providers are primary responsible to secure the information. Each provider uses special techniques to secure its resources in this system. Upon entry of a username and password, Single sign-on also allows some authenticated users to use this registration for other sites and applications.

## 5. Conclusion

After the massive implementation of cloud technologies in businesses and enterprises, the security of users' information and authentication has become increasingly important issue, which is discussed by many organizations around the world. Because of security issues, many users and businesses still refuse to use the cloud-based model. Risks, threats and vulnerabilities in virtual environments of cloud technologies significantly differ from the ones in physical environments. This publication introduces a new CIA triad data security model. It adds a three-factor authentication (3FA), as well as a Single sign-on using the OpenID standard. Thus, the effectiveness of preventive control is increased – this is the most important and effective control in an organization. The model focusses on data security and protection. Security management in an organization should also be in line with IT policies and standards for cloud technologies, as well as with business objectives for data security through the CIA triad – confidentiality, integrity and availability of information.

The proposed model will significantly increase data security in cloud technologies and thus reduce the risk of misuse and misuse of personal data, as well as the misuse of identity. Cyber threats and cyber-crimes will be reduced. The use of smart technologies will be safer and psychological stress and distrust in consumers will be reduced.

## 6. Acknowledgment

This work is supported by the Bulgarian National Science Fund, Project: KP-06-N 32/4/07.12.2019.

## 7. References

- [1] El-Gazzar R., Hustad E., (2016), Olsen D, Understanding cloud computing adoption issues: A Delphi study approach, *Journal of Systems and Software*, Volume 118, pp. 64-84. <https://doi.org/10.1016/j.jss.2016.04.061>
- [2] Viega J., (2009), Cloud Computing and the Common Man, in *Computer*, vol. 42, no. 8, pp. 106-108, DOI: 10.1109/MC.2009.252
- [3] National Institute of Standards and Technology(NIST), U.S. Department of Commerce, The NIST definition of Cloud Computing, Special publication of Computer Security, 2011
- [4] Center Of The Protection Of National Infrastructure CPNI by Deloitte, "Information Security Briefing of Cloud Computing"; The Security of Cloud Services, A Middle East Point of View, 2019
- [5] Ajoudanian Sh., Ahmadi M., (2012), A Novel Data Security Model for Cloud Computing, *IJET* 2012, Vol. 4 (3): pp. 326-329, DOI:10.7763/IJET.2012.V4.375
- [6] Mohamed M., Abdelkader H., El-Etriby S., (2012), Enhanced data security model for cloud computing, 2012 8th International Conference on Informatics and Systems (INFOS), Cairo, 2012, pp. CC-12-CC-17.
- [7] Hoyer U., Obel H., (2017), Guide on SaaS vs PaaS and IaaS, <https://www.linkedin.com/pulse/guide-saas-vs-paas-iaas-ulrik-hoyer-hansen-obel>
- [8] Zhiying W., Nianxin W., Xiang S., et al., (2020), An empirical study on business analytics affordances enhancing the management of cloud computing data security, *IJIM*, Volume: 50, Pages: 387-394, DOI: 10.1016/j.ijinfomgt.2019.09.002
- [9] Sheikh M, Liang J., Wang W., (2020), Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey,

*Wireless Communications & Mobile Computing*, Volume: 2020, DOI: 10.1155/2020/5129620NIST, *Cloud Computing Standards Roadmap*, Special Publication 500-291

- [10] Garvanov I., H. Kabakchiev, V. Behar, M. Garvanova, R. Iyinbor, (2019), On the Modeling of Innovative Navigation Systems, *Business Modeling and Software Design. BMSD 2019. Lecture Notes in Business Information Processing*, vol 356. Springer, Cham, pp. 299-306, 2019. DOI: 10.1007/978-3-030-24854-3\_23
- [11] Garvanova M., Shishkov B., (2019), Capturing human authority and responsibility by considering composite public values. *Business Modeling and Software Design. BMSD 2019. Lecture Notes in Business Information Processing*, vol. 356, 290-298. Springer, doi: [https://doi.org/10.1007/978-3-030-24854-3\\_22](https://doi.org/10.1007/978-3-030-24854-3_22).
- [12] Garvanova M., Shishkov B., Janssen M., (2018), Composite public values and software specifications. *Business Modeling and Software Design. BMSD 2018. Lecture Notes in Business Information Processing*, vol. 319, 412-420. Springer, doi: [https://doi.org/10.1007/978-3-319-94214-8\\_32](https://doi.org/10.1007/978-3-319-94214-8_32).
- [13] Garvanova M., Shishkov B., Vladimirov S., (2018), Mobile devices – effect on human health. *Proceedings of the Seventh International Conference on Telecommunications and Remote Sensing – ICTRS'18*, October 8-9, 2018, Barcelona, Spain, 101-104. New York: ACM, doi: <https://doi.org/10.1145/3278161.3278176>.