BG Pulse Journal USA
ISSN:1947-2536 http://www.bgpulseusa.com/index.php/bg

THE CONCEPT OF CLOUD TECHNOLOGIES AND THEIR FORENSICALLY SIGNIFICANT CHARACTERISTICS

Jakhongir Mamadalievich Esanov
Independent Researcher Law Enforcement Academy of the Republic of Uzbekistan
doi:https://doi.org/10.5281/zenodo.23553026

Abstract: The article analyzes the theoretical foundations of the concept of "cloud technologies" and their features that are significant for criminal procedure and forensic science. The key characteristics set out in NIST SP 800-145, the SaaS, PaaS and IaaS service models, and the private, community, public and hybrid deployment models are examined in terms of their significance for determining who controls the data, in which environment it is generated and where the relevant records can be obtained. The author's definition of "cloud technologies" is proposed.
Keywords: cloud technologies, NIST SP 800-145, cloud forensics, service model, deployment model, SaaS, PaaS, IaaS, user account, criminal procedure.

Introduction

The use of data stored in cloud environments in criminal proceedings first requires clarification of the nature of the research object. In this context, the technical environment in which data are stored, the digital form of the data, and their evidentiary significance are interrelated concepts that nevertheless differ in substance. Confusing these concepts may lead to interpreting the capabilities of a cloud service as procedural powers or treating any technically acquired information as evidence.

Whereas, in traditional storage systems, a user can directly identify the device on which a file is located, in a cloud service, the user accesses data through a specific account, software interface, or network address. The internal procedures for storing and processing data may not be fully visible to the user. This demonstrates that the ability to view information on a screen does not necessarily correspond to the ability to control its storage environment or fully verify its origin.

The Theoretical Foundations and Definition of Cloud Technologies

The development of cloud technologies is directly associated with advances in the shared use of computing resources, the provision of services over networks, and virtualization techniques. The principal outcome of this process has been the separation of the ability to use a resource from the need to purchase and manage it on-site. Although users are provided with computing power, storage capacity, or software services, the technical infrastructure supporting these resources is managed by another entity. In this sense, the term “cloud” does not imply the loss of the physical basis of information; rather, it describes a specific organizational and technological model for accessing and using it.

T. A. Pyanzina characterizes cloud technologies as the provision of computer resources and computing power to users in the form of network services. The author notes that access to such services is not limited to the Internet, but can also be provided through a local network based on web technologies[1]. This means that it is incorrect to equate cloud technology solely with a server located abroad or a public Internet service.

[1] Pyanzina, T. A. “Cloud Technologies: Formation and Development.” Ogarev-online, 2017, No. 2, p. 2. Available at: https://journal.mrsu.ru/wp-content/uploads/2017/02/statya_pyanzina-t.pdf

A. S. Khazhieva identifies the key characteristic of cloud computing as the ability to access hardware resources and software remotely, thereby elucidating the relationship between the service user and the entity providing the service[2]. However, the user's ability to manage the infrastructure varies across service models: in some models, the user only accesses a ready-made application, while in others, the user manages the operating system, their own applications, and certain aspects of the storage environment. Therefore, the existence of provider control does not justify the general conclusion that the user has no technical control whatsoever.

This aspect is further clarified in the NIST SP 800-145 document prepared by P. Mell and T. Grance, which defines cloud computing as a model for enabling network access to a shared pool of configurable computing resources available on demand. The document distinguishes five essential characteristics, three service models, and four deployment models[3]. Likewise, the ISO/IEC 22123-1:2023 standard plays an important role in harmonizing the fundamental terminology used in cloud computing[4].

The Forensic Significance of the Essential Characteristics in the NIST Classification

The essential characteristics in the NIST classification clearly describe how cloud services are organized, what the service models provide to users, and who uses the infrastructure under the deployment models[5]. These classifications and models are not interchangeable, since each serves a distinct and important purpose from a forensic perspective. They help determine where data are generated, who controls them, and which entities have access to the relevant information. Therefore, applying a single, universal technical method of data acquisition to services with different architectures and characteristics cannot always be considered justified.

In particular, the on-demand self-service characteristic enables users to provision resources independently, without having to negotiate directly with a provider’s employee each time. Its forensic significance lies in the need to examine the relationship between the resource provisioning process and a specific action performed by an individual. For example, if a virtual environment was created through a particular user account, records relating to its creation time, the network address from which the request was submitted, and the software tool that processed the request must be examined in detail. However, the fact that an account is officially registered to a particular individual does not conclusively prove that the action was performed by that individual, and this circumstance requires separate verification.

In turn, broad network access enables a service to be accessed from different devices and geographical locations. When examining this circumstance in connection with a criminal offence, examining a single device may not be sufficient to identify all participants in the exchange of information. Therefore, the possibility that an account was accessed from a computer, mobile device, or other software tool must be examined separately in each case. At the same time, recording an Internet Protocol (IP) address does not automatically identify an individual; the method by which the address was assigned, the conditions of shared use, and other related information may also be decisive.

---

[2] Khazhieva, A. S. “Cloud Technologies: Advantages and Disadvantages.” International Scientific Review, 2017, No. 6 (37).

[3] Mell P., Grance T. The NIST Definition of Cloud Computing. NIST Special Publication 800-145. Gaithersburg: NIST, 2011. DOI: 10.6028/NIST.SP.800-145. 2–3-б.

[4] ISO/IEC 22123-1:2023. Information technology - Cloud computing - Part 1: Vocabulary. Geneva: ISO, 2023. Electronic resource: https://www.iso.org/standard/82758.html

[5] Mell P., Grance T. The NIST Definition of Cloud Computing. NIST SP 800-145. 2011. 2–3-б.

The resource pooling principle is directly associated with serving multiple users within a single infrastructure. In forensic investigations, this characteristic raises the issue of clearly separating the relevant information from data belonging to other individuals, since the overall contents of a physical server do not necessarily correspond to the volume of information associated with a particular user account. Therefore, the logical boundaries of the object under examination—an account, virtual resource, dataset, or individual file—must be clearly specified; otherwise, it may remain unclear to whom the acquired data belong and which environment they originate from.

In turn, rapid elasticity enables resource capacity to be increased or decreased in response to demand. Its significance for evidentiary proceedings becomes clear when considered in the context of specific technical circumstances. For example, a virtual environment that was operating at the time of a crime may subsequently be deleted, recreated, or launched with a different configuration. Therefore, it is logically incorrect to assume that the state observed during a subsequent examination is identical to its earlier state. In addition to the resource name, its unique identifier, the period during which it existed, and records relating to the time interval under investigation are of decisive importance.

The measured service characteristic is associated with the ability to maintain aggregate records of resource consumption. Records concerning storage capacity, computing time, or network usage may, in certain cases, help reconstruct the circumstances of an incident. However, the fact that resource consumption is recorded does not necessarily mean that every file access, modification, or deletion is also logged. Therefore, it is essential to clearly distinguish service usage records from security and audit logs. Without establishing the relevant logging procedures, their scope, and the retention period, it cannot be concluded that the system preserves a complete history of all activities.

Classification of Cloud Services by the SaaS, PaaS, and IaaS Models

Classifying cloud services according to the SaaS, PaaS, and IaaS models helps develop a deeper understanding of how technical management responsibilities are distributed between the user and the provider[6]. Although this classification does not independently determine property rights, the legal status of personal data, or the powers of investigative authorities, its scientific and practical purpose is to establish which portions of the information are visible to users, which are generated automatically in the course of providing the service, and from whom the relevant records can be obtained. Accordingly, the service model is regarded as one of the initial forensic criteria for identifying the original source of information.

In particular, under the SaaS (Software as a Service) model, users can access only the functionality of a ready-made application. Although they may have direct access to their messages or files, they may not be able to view the service's internal logs or server environment. For example, the message text visible to users and the service record of the message's actual delivery constitute different information objects, and neither can fully substitute for the other. Therefore, when analyzing a SaaS environment, the information displayed in the interface should not be conflated with all the technical data of the service.

In turn, under the PaaS (Platform as a Service) model, users develop and launch their own applications in an environment provided by the service provider. In such cases, it is important to examine application-level records separately from the platform's own system logs, since the application may record that a particular action was performed, while platform data may indicate its launch or a technical error that occurred. Comparing these records helps reconstruct the sequence of events accurately. However, the platform model does not, in itself, guarantee the confidentiality

[6] Mell P., Grance T. The NIST Definition of Cloud Computing. NIST SP 800-145. 2011. 2–3-6.

or immutability of information; these characteristics depend on specific configurations and the conditions of practical use.

Finally, under the IaaS (Infrastructure as a Service) model, users are provided with dedicated virtual computing and storage resources. A forensic analysis of this model requires a clear distinction between the data stored in a virtual machine, the user's own administrative actions, and the provider's infrastructure logs. Just as the ability to manage a virtual environment does not imply control over every component of the physical server, the mere fact that a particular virtual resource was used cannot, by itself, fully prove that a specific individual committed a criminal act.

In the field of cloud forensics, researchers such as K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie examine technical, organizational, and legal aspects collectively. They rightly emphasize the need to clearly distinguish between objects on the user's side and those within the provider's infrastructure during data acquisition, as well as the fact that access to information depends directly on the service model[7]. This approach demonstrates that the service model is crucial for clearly identifying the technical location of the data and the entity that controls them.

Cloud Deployment Models

In turn, cloud deployment models include private, community, public, and hybrid clouds[8], in this context, the concept of "deployment" refers not only to the geographical location of a server but also to the scope of infrastructure use and management. Therefore, the limited views that a public cloud must necessarily be located abroad, whereas a private cloud must be located exclusively within an organization's premises, do not correspond to the scientific substance of this classification. The entity served by the infrastructure, the party managing it, and its geographical location are interrelated but constitute distinct circumstances that must be determined separately in practice.

In particular, a private cloud refers to an environment dedicated to the exclusive use of a specific organization. When examining such an environment, the organization's internal rules and the relationships between the unit managing the service and the external technical service provider play an important role. The characteristic of being private does not necessarily mean that the information is managed exclusively by the organization itself or that the resources are stored on its premises. Therefore, when locating data, the investigation should not be limited to the name of the organization; it is also necessary to examine in detail who has been granted authority over the relevant account records, storage environment, and log management.

In turn, a community cloud serves a group of organizations united by a common purpose or set of requirements. The forensic significance of this model becomes apparent when information may have been generated with the involvement of multiple organizations. For example, the individuals who create, edit, and view a document stored in a shared resource may belong to different organizations. In such circumstances, the right to access the shared infrastructure must be clearly distinguished from the authority to create or modify specific information. It is insufficient to determine each organization's relationship to the information solely on the basis of its membership in the service.

At the same time, although access to a public cloud is provided to a broad range of customers, this characteristic does not predetermine either the owner of the infrastructure or the country in which all copies of the data are stored. From a research perspective, the most important aspect is

[7] Ruan K., Carthy J., Kechadi T., Crosbie M. Cloud Forensics // Advances in Digital Forensics VII. IFIP Advances in Information and Communication Technology. 2011. Vol. 361. P. 35–46. 36–40-б.
[8] Mell P., Grance T. The NIST Definition of Cloud Computing. NIST SP 800-145. 2011. 3-б.

that a particular user's data are provided in a manner that ensures their clear logical separation from the data of other customers. The existence of a single account of investigative interest does not, in itself, necessitate an examination of the entire service infrastructure. Rather, identifying the specific information object helps justify the scope of the investigation and maintain clear boundaries between the relevant data and information belonging to other individuals.

Finally, a hybrid cloud involves the interconnected operation of separate cloud environments. When analyzing this model, it is necessary to distinguish the transfer of data from one environment to another from their original provenance. A file created within an organization's internal environment may subsequently be stored in an external service; however, its presence in the external service does not mean that the file was originally created there. Accordingly, the relationships between copies, their versions, and transfer logs must be identified. Such an analysis fully clarifies the distinction between the current storage location of the data and the history of their creation.

Authorship of the Concept of Cloud Technologies

At the same time, the various definitions presented in the scholarly literature illuminate different aspects of cloud technologies. In particular, T. A. Pyanzina emphasizes the provision of computing resources through network services, whereas A. S. Khazhieva focuses on the possibility of remotely accessing hardware resources and software. These scholarly approaches contribute to a deeper understanding of the relationship between the user and the service provider. From the perspective of forensic research, this relationship is crucial for identifying the connection between the ability to access data and the authority to manage the environment in which they are stored.

Summarizing these theoretical perspectives, it should be emphasized that the conceptual approaches presented by P. Mell and T. Grance in the NIST SP 800-145 document constitute a fundamental methodological basis for explaining the nature of cloud technologies in scholarly research and practice. The document describes cloud computing as a model for enabling network access, on demand, to a shared pool of configurable resources, identifying on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service as its essential characteristics. These characteristics make it possible to assess remote access to data alongside the organization and allocation of resources, as well as to distinguish cloud services from other information resources.

In this context, resource pooling, network access, and the adjustment of allocated capacity to meet demand are interconnected. This approach reveals the technical foundations for organizing the storage, processing, and use of data in a cloud environment, providing a basis for examining their handling within the service more broadly rather than limiting the analysis to a local file stored on a specific device.

Within forensic research, these characteristics of cloud technologies are important for determining the possibilities for accessing and managing data. In particular, the SaaS, PaaS, and IaaS models in the NIST classification differ in terms of the software functionality and resources that users can manage. Therefore, a user's ability to view and modify data and to control the storage environment requires separate examination, since the existence of one capability does not imply the existence of the others. These capabilities and their limitations must be taken into account when determining from which entity and technical environment the data can be obtained.

At the same time, characteristics such as distributed or cross-border data storage, the degree of dependence on a service provider, and the automatic logging of activities are not mandatory elements of the universal definition of cloud computing. Rather, their presence depends on the structure and operating procedures of a particular service. For example, a private cloud may operate

entirely within the territory of a single country, while the recording of resource consumption does not necessarily mean that a complete history of actions performed on each file is retained. Distinguishing the general characteristics of the technology from the specific features of a particular service that are relevant to data examination helps clearly define the scope of the research.

This approach establishes initial guidelines for examining the origin of data and the conditions under which they are stored, while their relevance to a criminal case and the possibility of using them as evidence require separate procedural assessment at a subsequent stage.

By integrating the approaches of the foreign and national scholars mentioned above, as well as the criteria of international standards, with criminal procedural law and forensic science, we propose the following original definition of the concept of "cloud technologies":

«Cloud technologies are methods and tools for providing and organizing the use of computing, storage, and software resources over a network, on demand and in variable quantities, based on a shared pool of resources».

Conclusion

The analysis conducted demonstrates the need to examine the forensic nature of data stored in cloud environments in relation to their content, form of representation, and storage environment. Cloud technologies organize access to computing and storage resources over a network. In such environments, the capabilities to access and modify data and to manage the storage infrastructure may be distributed among different entities.

The forensic characteristics of cloud data are determined by the structure and operating procedures of a particular service. Service and deployment models help establish who manages the data, in which environment they are generated, and where the relevant records can be obtained. The distributed storage of data, changes in resources, and log retention periods require the object of examination and the period under investigation to be clearly defined. In this context, the fact that an account or network address belongs to a particular individual is not sufficient to establish that the action was performed by that individual.

References:

1. Pyanzina, T. A. "Cloud Technologies: Formation and Development." Ogarev-online, 2017, No. 2, p. 2. Available at: https://journal.mrsu.ru/wp-content/uploads/2017/02/statya_pyanzina-t.pdf
2. Khazhieva, A. S. "Cloud Technologies: Advantages and Disadvantages." International Scientific Review, 2017, No. 6 (37).
3. Mell, P., and Grance, T. The NIST Definition of Cloud Computing. NIST Special Publication 800-145. Gaithersburg: National Institute of Standards and Technology, 2011, pp. 2–3. DOI: https://doi.org/10.6028/NIST.SP.800-145.
4. ISO/IEC 22123-1:2023. Information Technology — Cloud Computing — Part 1: Vocabulary. Geneva: International Organization for Standardization, 2023. Available at: https://www.iso.org/standard/82758.html..
5. Ruan, K., Carthy, J., Kechadi, T., and Crosbie, M. "Cloud Forensics." Advances in Digital Forensics VII. IFIP Advances in Information and Communication Technology, 2011, Vol. 361, pp. 35–46.
6. National Institute of Justice (NIJ). "Digital Forensics." U.S. Department of Justice, Office of Justice Programs. Available at: https://nij.ojp.gov/topics/articles/digital-forensics.