Вычислительные технологии, 2023, том 28, № 1, с. 72–80. © ФИЦ ИВТ, 2023
Computational Technologies, 2023, vol. 28, no. 1, pp. 72–80. © FRC ICT, 2023

ISSN 1560-7534
eISSN 2313-691X

DOI:10.25743/ICT.2023.28.1.008

A survey on multi-cloud storage security: threats and countermeasures

E. S. Bezuglova[1], E. M. Shiryaev[2], M. G. Babenko[1,2,3,*], A. Tchernykh[3,4,5], B. Pulido-Gaytan[4], J. M. Cortés-Mendoza[5]

[1]North-Caucasus Center for Mathematical Research North-Caucasus Federal University, 355017, Stavropol, Russia

[2]North-Caucasus Federal University, 355017, Stavropol, Russia

[3]Ivannikov Institute for System Programming, 109004, Moscow, Russia

[4]CICESE Research Center, 22860, Mexico

[5]South Ural State University, 454080, Chelyabinsk, Russia

[*]Corresponding author: Babenko Mikhail G., e-mail: mgbabenko@ncfu.ru

Received April 30, 2022, accepted May 16, 2022.

In this paper, we study multi-cloud storage technologies that share information as a single system using services from different cloud providers. These technologies provide advantages related to the availability and cost but need protections from security threats such as collusion and data leakage, limiting its massive adoption. We analyze security methods for multi-cloud storage and present the last advances in the field. We show that security systems based on homomorphic encryption are more promising than conventional security methods due to the possibility of performing operations over encrypted data.

Keywords: multi-cloud storage, homomorphic encryption, secret sharing schemes, cryptography, distributed computing.

Citation: Bezuglova E.S., Shiryaev E.M., Babenko M.G., Tchernykh A., Pulido-Gaytan B., Cortés-Mendoza J.M. A survey on multi-cloud storage security: threats and countermeasures. Computational Technologies. 2023; 28(1):72–80. DOI:10.25743/ICT.2023.28.1.008.

Introduction

Multi-cloud systems allow using two or more public cloud resources as a single system to distribute workloads. Their popularity among consumers is driven by the desire to replicate data or split the information across multiple cloud storages.

Cloud service providers (CSPs) have multiple data centers worldwide, becoming essential the geographic coverage factor, i. e., cover the required region where users are located. The multi-cloud systems expand the distribution problem and provide users from the nearest data center by using several CSPs. Moreover, many companies do not want to depend on a single CSP for privacy and security reasons, e. g., full access to sensitive data, data center failures, etc.

An important aspect is the ability to check remotely the data transferred to the cloud storage. This feature allows ensuring data integrity without performing a download process.

Several tools enable customers to store their data on multi-cloud servers. In this case, the integrity check protocol should be efficient enough to save the verifier costs.

In order to address this challenge, Huaqun Wang [1] proposed the identity-based distributed provable data possession (ID-DPDP) model for remote data integrity checking in multi-cloud storage. ID-DPDP is safe under the assumption of the hardness of the computational Diffie – Hellman (CDH) problem. The advantages of ID-DPDP include exclusion of certificate management, efficiency, flexibility, and private, delegated, and public verification.

The main implicit problem in the cloud computing paradigm is the secure outsourcing of confidential and business-critical data. For instance, malicious servers can potentially corrupt customer data, attack CSPs for misuse of cloud services and other systems, among others [2]. Considering using a CSP, the user should be aware that all data are beyond his control and protection.

Moreover, the CSP has complete control of data processing over these processes during applications deploying in the cloud, e. g., infrastructure as a service (IaaS), platform as a service (PaaS), etc. Hence, a strong trust relationship between the CSP and the cloud user is required in cloud computing environments.

A malicious attacker with access to the cloud storage component could modify data. Analogously, an attacker with access to the cloud processing logic could modify the functions and the inputs/outputs. Moreover, the possible collusion within the CSP itself poses a threat to data security in clouds.

This paper reviews the state-of-the-art methods for providing security in multi-cloud storage systems. We analyze such techniques across their pros and cons. Moreover, we study the taxonomy of security measures against threats associated with collusion.

The paper is structured as follows. Section 1 presents a literature review of the state-of-the-art methods to ensure security and prevent attacks in multi-cloud storage. Section 2 describes the methods that aroused the greatest interest and their classification. Finally, we conclude and discuss future work in Conclusion.

1. Related Work

Many researchers have been dealing with security problems in multi-cloud storage environments.

Ateniese et al. [3, 4] proposed a provable data possession (PDP) paradigm based on Rivest – Shamir – Adleman (RSA) cryptosystem with a proven level of security. In PDP, the verifier checks the integrity of the remote data with high probability. PDP allows the verification process without a download process, which reduces the financial cost of performing data I/O. However, the process only supports small metadata.

Erway et al. [5] proposed a full-dynamic PDP scheme based on authenticated encryption that supports the insertion operation. Wang et al. [6] developed a security model and a specific PDP proxy scheme in public clouds. Zhu et al. [7] presented a cooperative PDP model in multi-cloud servers. Subsequently, several models and protocols have also been proposed for performing remote data integrity checks [8–10].

Shaham and Waters [11] introduced the first proof of recovery (POR) with provable security, where the verifier can check the integrity of deleted data and receive it without reference to time. For more detailed information and additional consideration, refer to [12–14].

There are also scenarios where the client delegates the validation task to a remote third party [15–17]. As mentioned above, one of the benefits of cloud storage is that it provides universal access to data from any geographic location, so effective integrity verification protocols are suitable for cloud clients with mobile endpoints.

In [18–20], the solution to the security issue and data confidentiality in multi-cloud services was considered. It uses an architecture based on a secure cloud gateway that allows customers to store data in a semi-trusted multi-cloud environment, ensuring the confidentiality, integrity, and availability of data. The proposed proxy system implements a computational Secret Sharing Scheme (SSS) with a threshold value for storing shared secret parts in various cloud storages, which is efficient in terms of storage space. The system also includes security measures and cryptographic protocols to mitigate threats posed by cloud computing.

Ristenpart et al. [21] presented a study of cloud storage security vulnerabilities and problems. They studied attack methods against the Amazon Elastic Compute Cloud (EC2) IaaS virtual server. The approach cyclically generates Virtual Machines (VMs) to create a VM on the same physical machine as the victim's VM. The attack basis is to use secondary weakly protected channels between VMs in order to steal data.

Similarly, Zhang et al. [22] showed interest in Amazon EC2 and discovered a data management error. The Simple Object Access Protocol (SOAP)-based interface uses an XML signature defined in Web Services Security (WS-Security) for integrity protection and authentication. Gruschka and Iacono [23] found that EC2 signature verification implementation is vulnerable to signature transfer attacks [24].

According to the literature analysis, cloud computing in multi-cloud storage carries a threat due to the possible compromise of the cloud environment itself. When intruders penetrate the system, the stored data and user processes become objects of hostile actions. Therefore, the cloud computing model requires a great deal of attention to operational safety requirements. In the case of a single CSP, when it hosts and processes all of its users' data, an intrusion into the system affects all security requirements: accessibility, integrity, and confidentiality. This situation is compounded by the fact that actions can be performed on behalf of the cloud user. A large number of researchers are constantly working on solving this problem. As a result, many proposals have been put forward to improve the situation and develop multi-cloud services. In a nutshell, multi-cloud introduces unique features that enable new security approaches, techniques, and architectures.

2. Security methods in multi-cloud storages

The fundamentals of computing security in distributed environments were defined in [24] based on the millionaires' problem. The problem describes a scenario where two millionaires x and y want to establish which has the most capital, remaining unknown the size of their wealth. The following sections introduce the main approaches to ensure security over multi-cloud storage systems.

2.1. Secret sharing schemes

There are two main alternatives for secure multi-party computing (MPC): SSS [25] and corrupt schemes (CS) [26].

SSS schemes split data into several shares and distribute them among several CSPs. The CSPs compute fractions that collectively represent an objective function, the exchanging data is necessary between them. Thus, CSPs contain fractions of the result that are sent to the user when the data are recovered using the key. SSS requires at least three CSPs where two of them should not interact with each other.

Although the essence of MPC is outdated, research continues to reduce overhead. Recent improvements, e. g., concerning equality and value comparison, have led to the construction of programming frameworks that can already be considered practical [27, 28].

In the CS approach, a CSP generates and encrypts a scheme to compute the desired function, creating a corrupt scheme that remains executable. Then, it helps users to encrypt their input appropriately. The presence of another CSP is now required to evaluate the scheme using users' inputs.

TwinClouds [29] uses a private CSP to prepare CSs. The chains themselves are evaluated in a lower-trust, high-performance commodity CSP without compromising security guarantees for processes outsourced to the public cloud. In all cases, the use of MPC in a separate CSP ensures input privacy, unless the CSP colludes to open shared resources or decrypt the input. Assuming the CSP itself is not an attacker but could be compromised by attacks or has individual attackers, this collusion is difficult to establish to provide good protection. Cross-cloud MPC allows computing a function for data so that no cloud provider knows anything about the input/output.

2.2. Cryptographic data separation

Data encryption represents the simplest cryptographic method to implement secure data storage. A cryptographic key is a special set of data that encrypts and decrypts information. The success of decryption depends on the key used.

Storing a cryptographic key has its peculiarities. It can stay directly with the user, but in order to increase the flexibility of cloud data processing and ensure the operation of multi-user systems, it is useful to have the key available online [29]. In the second alternative, encrypted data are distributed across different clouds. XML data can be encrypted within the document [30].

Similar approaches are also used in several solutions for organizing secure cloud storage. The first approach to implementing cryptographic cloud storage [31] is a solution for encrypted key/value storage in the cloud while maintaining easy access to data. Encryption is used to search the encrypted data and keywords (if an authorized token is provided for the keyword). In this case, the keys are in a private cloud, and the data is in a secure public cloud.

One example of a relational database with encrypted data processing is CryptDB [31]. The database consists of a database server that stores encrypted data, a proxy server containing the keys, and a standard SQL interface. Data encryption is performed at different levels using the following schemes: order-preserving encryption (OPE) [32], homomorphic encryption (HE) [33], searchable encryption (SE) [34], and advanced encryption standard (AES) system. The proxy server authenticates and provides the server with the necessary keys to respond to an SQL request. Consequently, with each new request, the server learns a new key, which reduces the level of protection against intruders. The advantage of cryptDB is that part of the database is a standard MySQL database, which is marginally less efficient than unencrypted data storage.

The second approach is to implement secret data sharing, i. e., the secret sharing protocol does not contain a single cryptographic key. Multi-user secret sharing divides data between multiple shares in such a way that data are collected and recovered only if a specified data threshold is exceeded. This method has a high level of integration with MPC. MPC is often used with shared resources, including cloud storage, which form multi-party protocol peers and can permanently store their shared resources without compromising security.

The issue of using multiple CSPs securely is not trivial. There is no single optimal approach to simultaneously ensuring a high level of security and compliance with legal norms. Moreover, technically successful approaches are otherwise inconvenient for regulation and vice versa. The few approaches that find a compromise lack versatility and ease of use, so they are not popular. It can be concluded that the entire area of multi-block approaches still needs to be studied because it contains many shortcomings, but using various combinations of approaches, it will be possible to achieve an optimal system.

For example, an n-cloud approach (and its integrity guarantees) with strong data encryption (and its confidentiality guarantees) can satisfy technical and regulatory requirements. We have also identified the areas of HE and secure MPC protocols as promising areas in terms of security and compliance.

2.3. Homomorphic encryption and secure multilateral computation

The combination of HE methods and MPC is the use of cryptographic data protection during data processing. HE allows encrypting data with a public key and uploads the ciphertext to the cloud.

Several CSPs in the system can perform independent calculations while obtaining a general encrypted result, where the target recipient of the data can only decrypt them. An asymmetric fragmentation is used in the proposed scenario, the trusted part of the system manages keys and the encryption/decryption operation, while the public part processes the encrypted data.

The results in [35–37] make it possible; the goal is to obtain a fully HE that allows processing an unlimited number of homomorphic additions and multiplications. Previously, homomorphism could be established in only one of both operations. Thus, the main load falls on the clouds when applying HE, since they operate on the encrypted input data to generate the encrypted output data.

The most popular schemes are the integer-based Brakerski – Fan-Vercauteren (BFV) scheme [35] and Cheon – Kim – Kim – Song (CKKS) [36] for discrete real numbers with a fixed point.

Even though HE involves only two operations: multiplication and addition, there are methods for number comparison [37, 38] and matrix multiplication [39]. This set of operations is enough to process data in multi-cloud storage. The disadvantages of HE are low performance and high redundancy [40].

HE is a nascent research direction, wherein an extensive list of contributions has been proposed in the last years. HE schemes such as CKKS with support for real numbers make this domain attractive for further research.

Conclusion

In this paper, we review the multi-cloud storage technology and the classification of security measures against threats associated with prior collusion. We found that the technology under study combines clouds from several providers into a single cloud.

One of the main threats to using this technology is the collusion of one of the cloud service providers. In order to address collusion, secret sharing schemes and several encryption methods are traditionally used. However, these types of encryption have many inherent problems. In the case of secret sharing schemes, the compromised part of the multi-cloud storage may have a sufficient share to decrypt the data. In the case of traditional encryption, a decryption process is needed for data processing.

There are no such vulnerabilities for homomorphic encryption since the keys are stored only by the user, and information in the clouds is processed in an encrypted way. Homomorphic encryption denotes the most promising area of research in the field of providing security for multi-cloud storage. As future work, we plan to study the optimization of the redundancy and performance of state-of-the-art homomorphic encryption schemes.

Acknowledgements. This work was supported in part by the Russian Science Foundation, project No. 19-71-10033.

References

[1] **Wang H.** Identity-based distributed provable data possession in multicloud storage. Proceedings of the IEEE Transactions on Services Computing. 2015; (8):328–340. DOI:10.1109/TSC.2014.1.

[2] **Sebé F., Domingo-Ferrer J., Martínez-Ballesté A., Deswarte Y., Quisquater J.** Efficient remote data possession checking in critical information infrastructures. Proceedings of the IEEE Transactions on Knowledge and Data Engineering. 2008; 20(8):1034–1038.

[3] **Ateniese G., Burns R., Curtmola R., Herring J., Kissner L., Peterson Z., Song D.** Provable data possession at untrusted stores. Proceedings of the 14th ACM Conference on Computer and Communications Security. 2008: 598–609.

[4] **Ateniese G., DiPietro R., Mancini L.V., Tsudik G.** Scalable and efficient provable data possession. Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks. 2008: 1–10.

[5] **Erway C., Kupcu A., Papamanthou C., Tamassia R.** Dynamic provable data possession. Proceedings of the ACM Transactions on Information and System Security (TISSEC). 2015; 17(4):1–29.

[6] **Wang H.** Proxy provable data possession in public clouds. Proceedings of the IEEE Transactions on Services Computing. 2012; 6(4):551–559.

[7] **Zhu Y., Hu H., Ahn G., Yu M.** Cooperative provable data possession for integrity verification in multicloud storage. Proceedings of the IEEE Transactions on Parallel and Distributed Systems. 2012; 23(12):2231–2244.

[8] **Zhu Y., Wang H., Hu Z., Ahn G., Hu H., Yau S.** Efficient provable data possession for hybrid clouds. Proceedings of the 17th ACM Conference on Computer and Communications Security. 2010: 756–758.

[9] **Curtmola R., Khan O., Burns R., Ateniese G.** MR-PDP: multiple-replica provable data possession. Proceedings of the IEEE 28th International Conference on Distributed Computing Systems. 2008: 411–420.

[10] **Barsoum A., Hasan M.** Provable possession and replication of data over cloud servers. Proceedings of the Centre For Applied Cryptographic Research (CACR). University of Waterloo; 2010: CACR 2010-32.

[11] **Shacham H., Waters B.** Compact proofs of retrievability. Proceedings of the ASIACRYPT. Berlin: Springer; 2008: 90–107.

[12] **Bowers K.D., Juels A., Oprea A.** Proofs of retrievability: theory and implementation. Proceedings of the 2009 ACM Workshop on Cloud Computing Security. 2009: 43–54.

[13] **Zheng Q., Xu S.** Fair and dynamic proofs of retrievability. Proceedings of the CODASPY. 2011: 237–248.

[14] **Zhu Y., Wang H., Hu Z., Ahn G.J., Hu H.** Zero-knowledge proofs of retrievability. Sciece China. Information Sciences. 2011; 54(8):1608–1617. DOI:10.1007/s11432-011-4293-9.

[15] **Wang C., Wang Q., Ren K., Lou W.** Privacy-preserving public auditing for data storage security in cloud computing. Proceedings of the IEEE INFOCOM. 2010: 1–9. DOI:10.1109/INFCOM.2010.5462173.

[16] **Wang Q., Wang C., Ren K., Lou W., Li J.** Enabling public auditability and data dynamics for storage security in cloud computing. Proceedings of the IEEE Transactions on Parallel and Distributed Systems. 2010; 22(5):847–859.

[17] **Zhu Y., Ahn G.J., Hu H., Yau S.S., An H.G., Chen S.** Dynamic audit services for outsourced storages in clouds. Proceedings of the IEEE Transactions on Services Computing. 2011; 6(2):227–238.

[18] **Junghanns P., Fabian B., Ermakova T.** Engineering of secure multi-cloud storage. Computers in Industry. 2016; (83):108–120.

[19] **Miranda-López V., Tchernykh A., Babenko M., Avetisyan A., Toporkov V., Drozdov A.Y.** 2Lbp-RRNS: two-levels RRNS with backpropagation for increased reliability and privacy-preserving of secure multi-clouds data storage. Proceedings of the IEEE Access. 2020; 8:199424–199439. DOI:10.1109/ACCESS.2020.3032655.

[20] **Tchernykh A., Babenko M., Chervyakov N., Miranda-López V., Avetisyan A., Drozdov A.Y., Du Z.** Scalable data storage design for nonstationary IoT environment with adaptive security and reliability. Proceedings of the IEEE Internet of Things Journal. 2020; 1(10):10171–10188.

[21] **Ristenpart T., Tromer E., Shacham H., Savage S.** Hey, you, get off of my cloud: exploring information leakage in ThirdParty compute clouds. Proceedings of the 16th ACM Conference on Computer and Communications Security. 2009; 199–212.

[22] **Zhang Y., Juels A., Reiter M.K., Ristenpart T.** Cross-VM side channels and their use to extract private keys. Proceedings of the 2012 ACM Conference on Computer and Communications Security. 2012: 305–316.

[23] **Gruschka N., Lo Iacono L.** Vulnerable cloud: SOAP message security validation revisited. Proceedings of the IEEE International Conference on Web Services. IEEE; 2009: 625–631.

[24] **Ioannidis I., Grama A.** An efficient protocol for Yaos millionaires problem. Proceedings of the 36th Annual Hawaii International Conference on System Sciences. IEEE; 2003: 6–9. DOI:10.1109/HICSS.2003.1174464.

[25] **Ben-Or M., Goldwasser Sh., Wigderson A.** Completeness theorems for non-cryptographic fault-tolerant distributed computation. Proceedings of the 20th Annual ACM Symposium Theory of Computing (STOC'88). 1988: 1–10. DOI:10.1145/62212.62213. Available at: `https://www.researchgate.net/publication/221590203_Completeness_Theorems_for_Non-Cryptographic_Fault-Tolerant_Distributed_Computation_Extended_Abstract`.

[26] **Goldreich O., Micali S.M.S., Wigderson A.** How to play any mental game. Proceedings of the 19th Annual ACM Symposium on Theory of Computation (STOC'87). 1987: 218–229.

[27] **Damgard I., Geisler M., Kroigaard M., Nielsen J.B.** Asynchronous multiparty computation: theory and implementation. International Workshop on Public Key Cryptography. PKC 2009: 160–179. Available at: https://link.springer.com/chapter/10.1007/978-3-642-00468-1_10.

[28] **Burkhart M., Strasser M., Many D., Dimitropoulos X.** SEPIA: privacy-preserving aggregation of multi-domain network events and statistics. Proceedings USENIX Security Symposium 2010: 223–240. Available at: https://www.researchgate.net/publication/202120696_SEPIA_Privacy-Preserving_Aggregation_of_Multi-Domain_Network_Events_and_Statistics.

[29] **Bugiel S., Nürnberger S., Sadeghi A.R., Schneider T.** Twin clouds: secure cloud computing with low latency. Proceedings of the IFIP International Conference on Communications and Multimedia Security. 2011: 32–44. Available at: https://link.springer.com/chapter/10.1007/978-3-642-24712-5_3.

[30] **McIntosh M., Austel P.** XML signature elent wrapping attacks and countermeasures. Proceedings of the 2005 Workshop on Secure Web Services. SWS 2005. Fairfax, VA, USA; 2005: 20–27. DOI:10.1145/1103022.1103026. Available at: https://www.researchgate.net/publication/221560863_XML_signature_elent_wrapping_attacks_and_countermeasures.

[31] **Bogetoft P., Christensen D.L.D., Damgard I., Geisler M., Jakobsen T.P.T., Kroigaard M., Nielsen J.D.J., Nielsen J.B.J., Nielsen K., Pagter J., Schwartzbach M.I.M., Toft T.** Secure multiparty computation goes live, financial cryptography and data security. Springer-Verlag; 2009: 325–343.

[32] **Popa R.A., Redfield C.M., Zeldovich N., Balakrishnan H.** CryptDB: protecting confidentiality with encrypted query processing. Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles. 2011: 85–100.

[33] **Rivest R., Adleman L., Dertouzos M.** On data banks and privacy homomorphisms, foundations of secure computation. Computer Science, Mathematics. 1978; 4(11):169–180. Available at: https://www.semanticscholar.org/paper/ON-DATA-BANKS-AND-PRIVACY-HOMOMORPHISMS-Rivest-Dertouzos/c365f01d330b2211e74069120e88cff37eacbcf5.

[34] **Bellare M., Boldyreva A., O'Neill A.** Deterministic and efficiently searchable encryption. Proceedings of the Annual International Cryptology Conference. Berlin: Springer; 2007: 535–552.

[35] **Halevi Sh., Polyakov Yu., Shoup V.** An improved RNS variant of the BFV homomorphic encryption scheme. Proceedings of the Cryptographers Track at the RSA Conference. 2019: 83–105. Available at: https://link.springer.com/chapter/10.1007/978-3-030-12612-4_5.

[36] **Chen H., Chillotti I., Song Y.** Improved bootstrapping for approximate homomorphic encryption. Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cham: Springer; 2019: 34–54.

[37] **Babenko M., Tchernykh A., Chervyakov N., Kuchukov V., Miranda-López V., Rivera-Rodriguez R., Talbi E.G.** Positional characteristics for efficient number comparison over the homomorphic encryption. Programming and Computer Software. 2019; 40(8):532–543.

[38] **Babenko M., Tchernykh A., Pulido-Gaytan B., Golimblevskaia E., Cortés-Mendoza J.M., Avetisyan A.** Experimental evaluation of homomorphic comparison methods. Proceedings of the Ivannikov Ispras Open Conference (ISPRAS). 2020: 69–74. DOI:10.1109/ISPRAS51486.2020.00017.

[39] **Wang S., Huang H.** Secure outsourced computation of multiple matrix multiplication based on fully homomorphic encryption. KSII Transactions on Internet and Information Systems (TIIS). 2019; 13(11):5616–5630.

[40] **Pulido-Gaytan L., Tchernykh A., Cortés-Mendoza J.M., Babenko M., Radchenko G., Avetisyan A., Drozdov A.Y.** Privacy-preserving neural networks with Homomorphic encryption: challenges and opportunities. Peer-to-Peer Networking and Applications. 2021; 14(4):1666–1691. DOI:10.1007/s12083-021-01076-8. Available at: https://www.researchgate.net/publication/349901947_Privacy-preserving_neural_networks_with_Homomorphic_encryption_Challenges_and_opportunities.

Вычислительные технологии, 2023, том 28, № 1, с. 72–80. © ФИЦ ИВТ, 2023 ISSN 1560-7534
Computational Technologies, 2023, vol. 28, no. 1, pp. 72–80. © FRC ICT, 2023 eISSN 2313-691X

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

DOI:10.25743/ICT.2023.28.1.008

Обзор безопасности мультиоблачных хранилищ: угрозы и меры противодействия

Е. С. Безуглова[1], Е. М. Ширяев[2], М. Г. Бабенко[1,2,3,*], А. Черных[3,4,5], Б. Пулидо-Гайтан[4], Х. М. Кортес-Мендоса[5]

[1]Северо-Кавказский центр математических исследований Северо-Кавказского федерального университета, 355017, Ставрополь, Россия
[2]Северо-Кавказский федеральный университет, 355017, Ставрополь, Россия
[3]Институт системного программирования им. В.П. Иванникова РАН, 109004, Москва, Россия
[4]Центр научных исследований и высшего образования, 22860, Энсенада, Мексика
[5]Южно-Уральский государственный университет, 454080, Челябинск, Россия
*Контактный автор: Бабенко Михаил Григорьевич, e-mail: mgbabenko@ncfu.ru

Поступила 30 апреля 2022 г., принята в печать 16 мая 2022 г.

Аннотация

Представлены результаты изучения технологий мультиоблачных хранилищ, обменивающихся информацией с помощью сервисов различных провайдеров и являющихся единой системой. Мультиоблачные хранилища доступны и имеют низкую стоимость, но нуждаются в дополнительном обеспечении безопасности для противостояния хакерским атакам и утечке данных, что является ограничением для массового пользовательского внедрения данной технологии. Проанализированы существующие методы обеспечения безопасности и последние достижения в этой области. Сделан вывод, что системы безопасности, основанные на гомоморфном шифровании, превосходят традиционные методы защиты, так как в них возможно выполнение операций над зашифрованными данными.

Ключевые слова: мультиоблачное хранилище, гомоморфное шифрование, схемы разделения секретов, криптография, распределенные вычисления.

Цитирование: Безуглова Е.С., Ширяев Е.М., Бабенко М.Г., Черных А., Пулидо-Гайтан Б., Кортес-Мендоса Х.М. Обзор безопасности мультиоблачных хранилищ: угрозы и меры противодействия. Вычислительные технологии. 2023; 28(1):72–80. DOI:10.25743/ICT.2023.28.1.008. (на английском)

Благодарности. Исследование выполнено при частичной финансовой поддержке РНФ (проект № 19-71-10033).