Towards Reliable Low Cost Distributed Storage in Multi-clouds

N. Chervyakov[#1], M. Babenko[#2], A. Tchernykh[*3], I. Dvoryaninova[#4], N. Kucherov[#5]
[#]Mathematics and Mathematical Modelling, North-Caucasus Federal University
Stavropol, 355009, Russian Federation
[*]CICESE Research Center
Ensenada, Baja California, Mexico
[1]k-fmf-primath@stavsu.ru, [2]mgbabenko@ncfu.ru, [3]chernykh@cicese.mx, [4]innadv99@mail.ru ,[5]nkucherov@ncfu.ru

***Abstract*—We address the construction of a distributed cloud-based storage based on residual number system with modules of a special kind $\{2^n-3, 2^n-1, 2^n+1, 2^n+3\}$ to provide reliability and safety of stored data. We show that the proposed scheme allows obtaining an improvement of the coding and decoding rates, and the speed of data loading and data access comparing with the fastest cloud service. The costs associated with data encoding and decoding are minimal.**

Keywords—multi-clouds, resude number system, cloud storage, cloud-of-clouds.

I Introduction

Nowadays, cloud technologies become widely included into human lives. Using cloud resources for the IT infrastructure design gives an opportunity to save money, get easy access to data from every part of the world, effectively scale data storage and processing, etc. However, as it is proven in the report of the Cloud Security Alliance, the use of cloud computing requires ensuring the safety, reliability and availability of stored and processed data. [1].

According to the report of Kaspersky Security [2] DDoS attacks are the major security threat for Internet. The entity, regardless of its purpose or business, must consider itself and its resources to be a target for cybercriminals that may lead to a denial of access to the data stored and processed in the cloud. For example, it was happened with Amazon in 2009 [3], Twitter and Saudi Aramco in 2012 and 2013 [4], with Dyn in 2016 [5], etc.

When DDoS-attack happens, legitimate users cannot gain access to computing resources or obtain it with difficulties. In order to counter DDoS attacks, providers use filters that analyze Internet traffic. As proposed in [6], hardware replication and load transfer between different data centers are used for dealing with DDoS attacks. However, upon detection of DDoS-attacks, it takes time to create a replica of the virtual machine during which a technical failure may also occur. To eliminate this disadvantage, it is possible to distribute the processing load among multiple cloud providers using different data centers.

Users of cloud providers such as Amazon, Dropbox, Microsoft, Google and Yandex Disk were denied to access to the data because of problems with the data centers electricity. These new not well-established technologies can lead to the loss or distortion of data [7]. For example, in NSA data centers during 2012-2013, there were 10 technical failures in new equipment. The reasons of the failures in the electrical control systems investigated by the Army Corps of Engineers became mysteries in most cases.

Nirvanix cloud provider is notified in 2013 that the access point will be closed within two weeks due to bankruptcy. Users who stored terabytes of data on servers Nirvanix lost their data because they did not have time to move them to other media [8]. In 2014, the company Code Spaces lost most confidential data about their customers because of the the hacker attack, so it was forced to close the business [1]. In January 2016, users of the service GitLab lost their data of six hours of their work because of the system administrator error [9].

Cloud users may lose the data due to many reasons: hacker attacks, virus infection, technical glitch of the storage, bankruptcy, loss of the encryption key, technogenic disaster, etc.

To ensure reliable, secure and accessible storage it is necessary to make data backup at least once per week [1]. An alternative solution is proposed by [10]. The authors show that to improve the reliability, security and availability of data storage and processing, a distributed storage system can be based on residue number system. However, as shown in [11], data recovery according to Chinese remainder theorem has quadratic complexity regarding to the residue number system range.

In this paper, to improve the reliability, availability and security of data, we use the error correction code. It allows the use of two reference bases to detect and correct two errors in contrast to the classical error correction code in the residue number system with two controls that can detect two errors but correct only one.

In this work, we propose a high-performance, reliable, secure data storage scheme in the multi-clouds built on a four-module residue number system of a special kind $\{2^n-3, 2^n-1, 2^n+1, 2^n+3\}$.

II Related work

While building distributed systems storage in the clouds, issues of privacy, security and data availability are important. Data must be protected from the harmful effects of external factors and technical failures.

Ji Hu and Klein A, 2009 [12] examined the issue of data security during data migration. To ensure safe data, they suggest using cryptographic primitives, which lead to a large overhead for encrypting and decrypting data.

Chang, F., et al., 2008 [13] offered reliable storage of large Bigtable data based on three times the data replication system, where the main disadvantages are the lack of data protection and big data redundancy. Approaches for building distributed systems storage in the clouds can be divided into two groups: reliable data storage scheme based on the use of: replication, detection codes, localization and correction of errors, secret sharing schemes, threshold access structures; secure data storage scheme based on the use of: symmetric ciphers: asymmetric ciphers, homomorphic encryption, secret sharing schemes.

According to the opinion poll among IT Directors conducted by IDC (Clavister's 2009 [14]), security risks are constraining factor for widespread use of cloud technologies to 74% of interviewed.

To assess the safety of storage, we will consider three criteria: confidentiality, integrity and availability. As shown in Hashizume, K., et al., 2013 [15], security threat may occur due to the following vulnerabilities: unsafe interface and software, unlimited resource allocation, places of data location, incomplete performance of user instructions (incomplete data deletion), unlimited distribution of resources, virtual machines, unsafe migration and others.

DepSky proposed in Bessani, A., et al., 2013 [16] on the basis of the Byzantine protocol and (2, 4) code erasure, allow to provide privacy and data availability. Using DepSky allows to store about twice smaller volume of the original data in each individual cloud, but the sum of two times more than the original amount of data. The effective implementation of codes erasure proposed in Dimakis, A. G., et al., 2010, [17] with the complexity of the decoding algorithm.$O(L \cdot logL)$.

Cachin et al., 2009 [18] showed that while the organization of access to the data of group users the probability of data corruption by one of the members is sufficiently high. To resolve this problem,next ways are used: data replication J. Hendricks 2007 [19], the Byzantine protocol Cachin et al., 2009 [18], secret sharing scheme Ye Y., et al., 2010 and AlZain, M. A., 2012 [20] etc. Classical data replication ensures data availability, but does not allow to ensure the confidentiality and integrity. An alternative way of solutions to ensure the availability, confidentiality and integrity of data is the simultaneous use of cryptographic primitives: secret sharing schemes (Gu, Y., & Grossman, R. L. 2010 [21]), access structures, symmetric encryption algorithm with a digital signature.

NCCloud distributed storage system built on the basis of regenerative codes Hu, Y., et al., 2012 [12]. Regeneration codes are modifications of erasure codes. A distinctive feature of the regeneration of codes is that they require a smaller amount of network traffic as opposed to the classical error correction codes or erasure codes Dimakis, A. G., et al., 2010 [17].

Kamara, S., & Lauter, K. 2010 [22] proposed cryptographic scheme of cloud storage based on the use of a symmetric cipher AES, figure captions and one-time key generator. The advantage of this scheme is to provide cryptographic privacy and data integrity. However, in case of loss or distortion of key due to technical failures or virus exposure data will be lost without refund.

Ateniese et al., 2007 [23] proposed a scheme based on remote data auditing to ensure the integrity of data stored in the cloud. The authors used homomorphic encryption algorithm on the basis RSA. As shown in Sookhak, M., et. al. 2017 [24] major disadvantage of schemes Ateniese et al., 2007 [23], Juels, A., & Kaliski Jr, B. S. 2007 [25], Wang, Q., 2011 [26] and others based on remote data auditing is a large computational complexity, which leads to large overheads user or auditor which depends on the scheme.

Cui, H., et al., 2017 [27] offered storage scheme, which at the same time uses the public cloud for data storage and private cloud to ensure data security based on two cryptographic primitives with zero-knowledge proof of knowledge and a commitment scheme. The main benefit of this scheme is that the transfer of the decryption key is not required for the confidential exchange of data. The disadvantage of this scheme is a big calculation load on the private cloud.

As the probability of leakage of confidential data while data transmission inside the cloud is big enough be data encryption algorithms should be used. As shown Ristenpart, T., et al., 2009 [28] the sequence of actions to obtain confidential data from other virtual machines collocated on the same server as the attacker. To ensure data security cryptographic primitives data encryption should be used: symmetric ciphers, secret sharing schemes.

III A METHOD FOR STORING DATA IN THE CLOUD-BASED RNS

A. Scheme of data storage in the clouds

Consider the data storage circuit Cloud-of-Clouds based on the use of error correction codes in the residue number system. Let us mention, that file systems files are stored as sequences of bytes, so they are written like words by 8 bits All calculations are thus reduced to operations on numbers with a digit, divisible by the number 8.

Coding data is composed of two parts. The first part of this partitioning of data into small blocks which size has prevented the working range of the residual number system, which can perform calculations. These parts must be aligned by 8 bits, but they must be large enough to minimize the risk of dissection system enumeration. On the other hand, large numbers lead to a long and complex calculations, which is unacceptable for the system being developed. It is necessary to strike a balance between the speed of the system and its resistance. Another indicator of the system on the basis of the error correction codes in the residue number system is a total redundancy of all data in the data projections residue number system to the original data size.

Various solutions to these issues lead to varying degrees of data protection, a different run-time encoding, and decoding algorithms. We study the modules of a special form for the effective implementation of modular arithmetic operations underlying the data encryption and decryption algorithms.

Using RNS module of form 2^n for sharing the secret is not feasible since in this case some information is presented in an unencrypted form. Such a choice of RNS moduli results from the existence of efficient algorithms for finding the remainder of division by each of them; that allows building a fast algorithm for data encryption.

We propose a reliable system of data storage, based on secret sharing scheme (2, 4) on the basis of RNS with modules of a special form $\{2^n - 3, 2^n - 1, 2^n + 1, 2^n + 3\}$.

The input is a long L-byte file and let $X \xrightarrow{RNS} \{x_1, x_2, x_3, x_4\}$, where $x_1 = |X|_{2^n-3}$, $x_2 = |X|_{2^n-1}$, $x_3 = |X|_{2^n+1}$, $x_4 = |X|_{2^n+3}$, $X \in [0, 2^{2n-6})$ и $n = 8\left\lceil \frac{L}{2} \right\rceil + 111$. Therefore, the encryption algorithm is applied to the input line $L + 28$ bytes. At the beginning the document is added with 28 bytes, which are the file hash function obtained using the SHA-3, which has the remarkable property: with a small change of text hash value changes drastically, see Example 1.

SHA3-224("My name is Mikhail") = fef131a1fe3425bdd616ca6267835e74e2a1785c3c26b02bdb86d222

SHA3-224("My name is Mikhail.") = b9d5edd1f1b1e07c37179c4e31bb9ef299c6fa74d81d560ff1cdc68c

SHA3-224("my name is Mikhail") = 687bcbdb97b1fa1b223062565b29032c1363667f563b770d344e0d0f

Then X can be represented as : $X = X_1 2^n + X_2$, where $0 \le X_1 < 2^{n-6}$ и $0 \le X_2 < 2^n$, which means that x_1, x_2, x_3, x_4 can be calculated by the following formulas: $x_1 = |X|_{2^n-3} = |3X_1 + X_2|_{2^n-3}$, $x_2 = |X|_{2^n-1} = |X_1 + X_2|_{2^n-1}$, $x_3 = |X|_{2^n+1} = |X_2 - X_1|_{2^n+1}$, $x_4 = |X|_{2^n+3} = |X_2 - 3X_1|_{2^n+3}$, therefore algorithmic complexity of the algorithm data encryption using the RNS is $O(n)$. Thus the use of a special type RNS allows more efficient encoding the data in comparison with the algorithms operate on the basis of the erasure codes $O(n \cdot \log n)$. We obtain four equal-sized projections for secret $\left\lceil \frac{L}{2} \right\rceil + 7$ byte. So, information rate of proposed storage system is asymptotically equal to $\frac{1}{2}$ and is comparable to the same parameter in the DepSky system

B. Algorithms for decoding data

Since we use a secret division scheme (2,4), then probably $C_4^2 = 6$ data access options. As for each of the options finding the remainder of the division of numbers on the number of special form is required, the use of a method of Pascal and neural finite ring network provides the result in a single clock cycle of the neural network. We calculate coefficients to restore the stored data with the use of the Chinese remainder theorem:

1 option. Known projection secret: x_1, x_2. Now we calculate the required value of X:

$$\left|\frac{1}{2^n - 1}\right|_{2^n-3} (2^n - 1) = (2^{n-1} - 1) \cdot (2^n - 1) = 2^{2n-1} - 2^n - 2^{n-1} + 1$$

$$\left|\frac{1}{2^n-3}\right|_{2^n-1} (2^n - 3) = (2^{n-1} - 1) \cdot (2^n - 3) = 2^{2n-1} - 2^{n+1} - 2^{n-1} + 3,$$

$M_{12} = (2^n - 3)(2^n - 1) = 2^{2n} - 2^{n+2} + 3$. According to the Chinese remainder theorem:

$$X = |2^{2n-1}(x_1 + x_2) - 2^n(x_1 + 2x_2) - 2^{n-1}(x_1 + x_2) + x_1 + 3x_2|_{M_{12}} \quad (1)$$

2 option. Known projection secret: x_1, x_3. Now we calculate the required value of X:

$$\left|\frac{1}{2^n+1}\right|_{2^n-3} (2^n + 1) = (2^{n-1} - 1) \cdot (2^n + 1) = 2^{2n-1} - 2^{n-1} - 1,$$

$$\left|\frac{1}{2^n-3}\right|_{2^n+1} (2^n - 3) = 2^{n-2} \cdot (2^n - 3) = 2^{2n-2} - 2^{n-1} - 2^{n-2},$$

$M_{13} = (2^n - 3)(2^n + 1) = 2^{2n} - 2^{n+1} - 3$. According to the Chinese remainder theorem:

$$X = |2^{2n-2}(2x_1 + x_3) - 2^{n-1}(x_1 + x_3) - 2^{n-2}x_3 - x_1|_{M_{13}} \quad (2)$$

3 option. Known projection secret: x_1, x_4. Now we calculate the required value of X:

$$\left|\frac{1}{2^n+3}\right|_{2^n-3} (2^n + 3) = \left|\frac{2^{n-1}-1}{3}\right|_{2^n-3} \cdot (2^n + 3),$$

$$\left|\frac{1}{2^n-3}\right|_{2^n+3} (2^n - 3) = \left|\frac{2^{n-1}-1}{3}\right|_{2^n+3} \cdot (2^n - 3),$$

$M_{14} = (2^n - 3)(2^n + 3) = 2^{2n} - 9$ According to the Chinese remainder theorem:

$$X = |2^{2n-2}(2x_1 + x_3) - 2^{n-1}(x_1 + x_3) - 2^{n-2}x_3 - x_1|_{M_{13}} \quad (3)$$

4 option. Known projection secret: x_2, x_3. Now we calculate the required value of X:

$$\left|\frac{1}{2^n+1}\right|_{2^n-1} (2^n + 1) = 2^{n-1} \cdot (2^n + 1) = 2^{2n-1} + 2^{n-1},$$

$$\left|\frac{1}{2^n-1}\right|_{2^n+1} (2^n - 1) = 2^{n-1} \cdot (2^n - 1) = 2^{2n-1} - 2^{n-1},$$

$M_{23} = (2^n - 1)(2^n + 1) = 2^{2n} - 1$. According to the Chinese remainder theorem:

$$X = |2^{2n-1}(x_2 + x_3) + 2^{n-1}(x_1 - x_3)|_{M_{14}} \quad (4)$$

5 option. Known projection secret: x_2, x_4. Now we calculate the required value of X:

$\left|\frac{1}{2^n+3}\right|_{2^n-1}(2^n+3) = 2^{n-2}\cdot(2^n+3) = 2^{2n-2} + 2^{n-1} + 2^{n-2}$,

$\left|\frac{1}{2^n-1}\right|_{2^n+3}(2^n-1) = (2^{n-1}+2^{n-2}+2)\cdot(2^n-1) = 3\cdot 2^{2n-2} + 2^n + 2^{n-2} - 2$,

$M_{24} = (2^n-1)(2^n+3) = 2^{2n} + 2^{n+1} - 3$. According to the Chinese remainder theorem:

$$X = |2^{2n-2}(x_2 + 3x_4) + 2^{n-2}(3x_2 + 5x_4) - 2x_4|_{M_{14}} \quad (5)$$

6 option. Known projection secret:x_3, x_4. Now we calculate the required value of X:

$\left|\frac{1}{2^n+3}\right|_{2^n+1}(2^n+3) = (2^{n-1}+1)\cdot(2^n+3) = 2^{2n-1} + 2^{n-1} + 2^{n-2}$,

$\left|\frac{1}{2^n-1}\right|_{2^n+3}(2^n-1) = (2^{n-1}+2^{n-2}+2)\cdot(2^n-1) = 3\cdot 2^{2n-2} + 2^n + 2^{n-2} - 2$,

$M_{24} = (2^n-1)(2^n+3) = 2^{2n} + 2^{n+1} - 3$. According to the Chinese remainder theorem:

$$X = |2^{2n-2}(x_2 + 3x_4) + 2^{n-2}(3x_2 + 5x_4) - 2x_4|_{M_{14}} \quad (6)$$

IV MODELING

A. *Optimization* of neural network finite ring

Using neural network finite ring (NNFR) during the implementation of modular arithmetic of addition and multiplication operations can improve program performance and reduce computing costs by a large degree of concurrent computing. Besides sharing the NNFR and feature Pascal divisibility for the system of residual classes module of a special kind $\{2^n-3, 2^n-1, 2^n+1, 2^n+3\}$, allows to improve the processing speed.

Consider the general guidelines for the implementation of modular operations of addition and multiplication using NNFR. The NNFR neurons are arithmetic device, rather than the usual non-linear activation function used in training the neural network. Analysis of the final arithmetic ring showed that the computational model based on iterative mechanism for reducing module is a basic operation for a modular data processing.

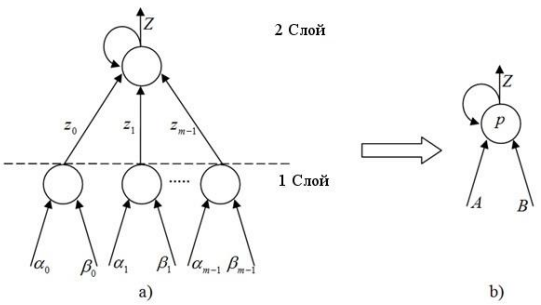

Fig.1 – The structure of the subnet (a) and its symbolic notation (b)

On the basis of computer models of the final ring,, главным оператором the main operator in which is the operator of extracting individual bits of the binary representation of the number being converted, multi-subnet can be built.. subnet structure is shown in Figure 1, where the synaptic weights are equal to $w_i = \left|2^i\right|_p$, $i = 0,1,\dots,n-1$. For each module of residue number system ans $M_{12}, M_{13}, M_{14}, M_{23}, M_{24}, M_{34}$ NNFR is designed separately. Given that the modules residue number system and $M_{12}, M_{13}, M_{14}, M_{23}, M_{24}, M_{34}$ are the numbers of special type that allows to optimize the structure of the NNFR.

1. Result of operations converting a binary number to the residue, multiplication, addition, computed using the NNFR is a function of the weighted sum of the input bits.

2. The result of calculation is determined by the positive logic. The end result of the NNFR will have a stable form..

B. *Experimental results*

Here are the results of testing the data storage system based on the erasure and our proposed calculation scheme codes held with a general purpose processor Intel Core i5 2,7 GHz, 8 GB 1867 MHz DDR3. To simulate the coding rate and the data decoding processing will process the video image 100 MB.

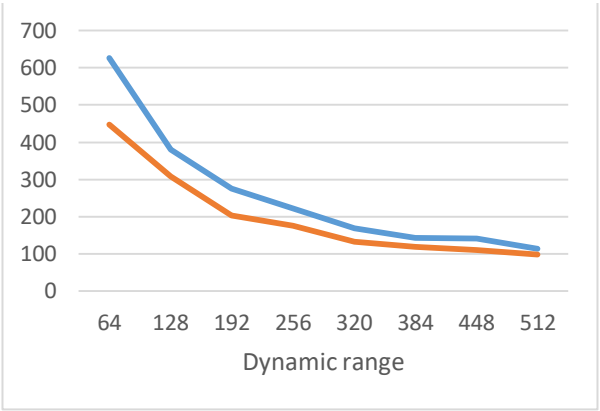

Fig 2. Speed Coding

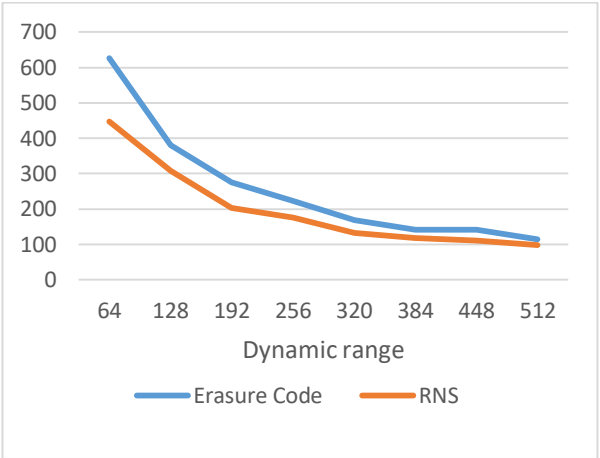

Fig 3. Speed Decoding

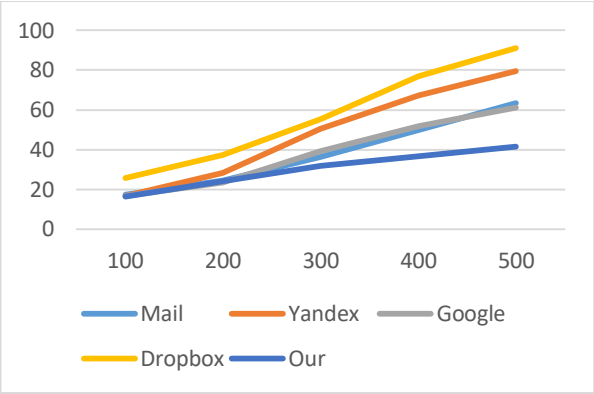

Fig 4. The download speed of data in the cloud

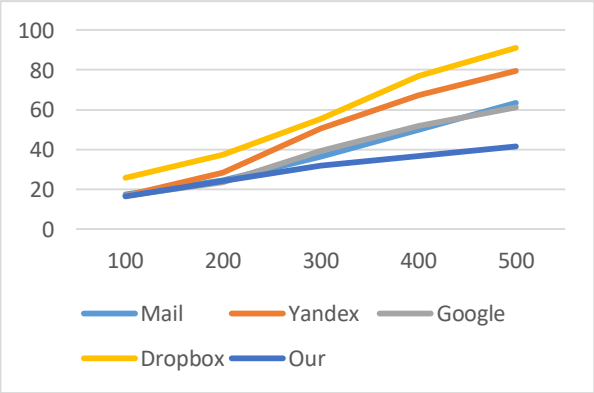

Fig 5. The speed of access to data from the cloud

From Figures 2 and 3 that the proposed storage scheme allows to receive the average gain in the coding rate to 1.48 times and 1.87 times in decoding as compared to erasure codes. Analysis of the simulation results shown in Figures 4 and 5 shows that the data loading speed increases cloud on average 1.5 times, and data access by 1.7 times compared with the fastest cloud service. Thus the costs arising from the encoding and decoding of data is minimal, and the use of residual number system ensures reliability and data security.

V Conslusion

A residual number system with modules of special type $\{2^n - 3, 2^n - 1, 2^n + 1, 2^n + 3\}$ allows to reduce costs of data storage and obtain average gain of 1.48 times in the coding rate and 1.87 times in decoding as compared to erasure codes. Speed of data loading into the cloud increases on average 1.5 times, and data access by 1.7 times compared with the fastest cloud service. Thus the costs arising from the encoding and decoding of data is minimal, and the residue number system allows the use of reliability and safety data.

Aknowlegment

The work is partially supported by CONACYT (Consejo Nacional de Ciencia y Tecnología, México), grant No. 178415, and Tsinghua Global Scholars Fellowship Program No. 201609020001. Part of the work was supported State task No. 2.6035.2017 and Russian Federation President Grant SP-1215.2016.5.

Referenses

[1] CSA 2016, https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf, 27.02.2017

[2] Kaspersky 2016 https://securelist.com/analysis/quarterly-malware-reports/76464/kaspersky-ddos-intelligence-report-for-q3-2016/, 27.02.2017

[3] Metz, C. (2009). DDoS attack rains down on Amazon Cloud. The Register.

[4] F.J. Cilluffo, S. L. Cardash, and, G.C. Salmoiraghi, “A blueprint for cyber deterrence: Building stability through strength,” Military and Strategic Affairs, 2012, vol. 4(3), pp. 3-23.

[5] Sebastian Moss http://www.datacenterdynamics.com/content-tracks/security-risk/major-ddos-attack-on-dyn-disrupts-aws-twitter-spotify-and-more/97176.fullarticle, 27.02.2017

[6] A. Bakshi, and, Y.B. Dujodwala, “Securing cloud from ddos attacks using intrusion detection system in virtual machine,” In Communication Software and Networks, ICCSN'10, Second International Conference, 2010, pp. 260-264.

[7] NSA http://spectrum.ieee.org/tech-talk/computing/it/nsa-data-center-electrical-problems-arent-that-shocking, 27.02.2017

[8] S. Wu, K.C. Li, B. Mao, and M. Liao, “DAC: Improving Storage Availability with Deduplication-Assisted Cloud-of-Clouds”. Future Generation Computer Systems, 2016.

[9] GitLab https://www.theregister.co.uk/2017/02/01/gitlab_data_loss/, 27.02.2017

[10] A. Tchernykh, U. Schwiegelsohn, E.G. Talbi, and M. Babenko, “Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability,” Journal of Computational Science, 2016.

[11] Bach, E., & Shallit, J. O. (1996). Algorithmic Number Theory: Efficient Algorithms (Vol. 1). MIT press.

[12] J. Hu, and A. Klein, “A benchmark of transparent data encryption for migration of web applications in the cloud,” In Dependable, Autonomic and Secure Computing, DASC'09, Eighth IEEE International Conference on 2009, pp. 735-740.

[13] F. Chang, J. Dean, S. Ghemawat, W.C. Hsieh, D.A. Wallach, M. Burrows, and R.E. Gruber, “Bigtable: A distributed storage system for structured data,” ACM Transactions on Computer Systems (TOCS), 2008, vol. 26(2), p. 4.

[14] Clavister’s new dimension in network security reaches the Cloud https://www.clavister.com/globalassets/documents/resources/white-papers/clavister-whp-cloud-security-en.pdf, 27.02.2017

[15] K. Hashizume, D.G. Rosado, E. Fernández-Medina, and E.B. Fernandez, “An analysis of security issues for cloud computing,” Journal of Internet Services and Applications, 2013, vol. 4(1), p. 5.

[16] A. Bessani, M. Correia, B. Quaresma, A. André, and P. Sousa, “DepSky: dependable and secure storage in a cloud-of-clouds,” ACM Transactions on Storage (TOS), 2013, vol. 9(4), p. 12.

[17] A.G. Dimakis, P.B. Godfrey, Y. Wu, M.J. Wainwright, and K. Ramchandran, “Network coding for distributed storage systems,” IEEE Transactions on Information Theory, 2010, vol. 56(9), pp. 4539-4551.

[18] C. Cachin, I. Keidar, and A. Shraer, A., “Trusting the cloud,” Acm Sigact News, 2009, vol. 40(2), pp. 81-86.

[19] J. Hendricks, G.R. Ganger, and M.K. Reiter, “Low-overhead byzantine fault-tolerant storage,” In ACM SIGOPS Operating Systems Review, 2007, vol. 41, No. 6, pp. 73-86.

[20] M.A. AlZain, E. Pardede, B. Soh, and J.A. Thom, “Cloud computing security: from single to multi-clouds,” In System Science (HICSS), 45th Hawaii International Conference on 2012, pp. 5490-5499.

[21] Y. Gu, and R.L. Grossman, “Sector: A high performance wide area community data storage and sharing system,” Future Generation Computer Systems, 2010, vol. 26(5), pp. 720-728.

[22] S. Kamara, and K. Lauter, “Cryptographic cloud storage,” In International Conference on Financial Cryptography and Data Security 2010, pp. 136-149.

[23] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted

stores," In Proceedings of the 14th ACM conference on Computer and communications security, 2007, pp. 598-609.
[24] M. Sookhak, A. Gani, M.K. Khan, and R. Buyya, "Dynamic remote data auditing for securing big data storage in cloud computing," Information Sciences, 2017, vol. 380, pp. 101-116.
[25] A. Juels and Jr, B.S. Kaliski, "PORs: Proofs of retrievability for large files," In Proceedings of the 14th ACM conference on Computer and communications security, 2007, pp. 584-597.
[26] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE transactions on parallel and distributed systems, 2011, vol. 22(5), pp. 847-859.
[27] H. Cui, R.H. Deng, Y. Li, and G. Wu, "Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud," 2017, IEEE Transactions on Big Data.
[28] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," In Proceedings of the 16th ACM conference on Computer and communications security, 2009, pp. 199-212.