УДК 004.056.5 **DOI:10.30837/rt.2023.1.212.03**

М.В. ЄСІНА, канд. техн. наук, А.А. КРАВЧЕНКО, С.О. КРАВЧЕНКО

ОГЛЯД ЗАГРОЗ БЕЗПЕЦІ ТА ЦІЛІСНОСТІ ДАНИХ У ХМАРНИХ ОБЧИСЛЕННЯХ

Вступ

Хмарні обчислення – це технологія, яка швидко набирає популярності та розвитку, поєднує у собі декілька підходів та моделей з надання та управління IT сервісами. Згідно з визначенням Національного інституту стандартів і технології (NIST) США, хмарні обчислення – це модель забезпечення повсюдного та зручного доступу на вимогу, через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів) і які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера [1]. Хмарні обчислення розглядаються як одна з найуспішніших обчислювальних технологій, здатних вирішити цілу низку проблем, що стоять перед людством.

Хмарні обчислення мають декілька ключових особливостей, як-то надійність, широкий мережевий доступ, масштабованість інфраструктури, гнучкість, незалежність від місця розташування, економія на масштабах і економічна ефективність та стійкість [2, 3].

Через зростаючу популярність і широку експлуатацію послуг хмарних обчислень виникає необхідність високого рівня безпеки. У сьогоднішніх реаліях люди використовують технології хмарних обчислень у великих обсягах, наприклад на роботі, в особистих цілях та інше, так як вони мають велику довіру до цих технологій. Щоб запобігти втраті довіреної інформації провайдери послуг мають забезпечити її цілісність.

Стаття присвячена огляду загроз безпеці та цілісності технологій хмарних обчислень, тому що це є важливим аспектом даної технології. Зазначимо, що безпека хмарних обчислень означає захист даних, тоді як цілісність – їх надійність. Безпека та цілісність даних є основною проблемою користувачів, пов'язаною із хмарними обчисленнями.

Основна частина

В роботі [4] визначено безпеку хмарних обчислень як «піддомен комп’ютерної безпеки, мережевої безпеки та, ширше, інформаційної безпеки. Це стосується широкого набору політик, технологій і елементів керування, які застосовуються для захисту даних, додатків і відповідної інфраструктури хмарних обчислень».

Коли організація вирішує зберігати дані або розміщувати додатки в публічній хмарі, вона втрачає можливість мати фізичний доступ до серверів, на яких зберігається її інформація [8]. Як наслідок, потенційно конфіденційні дані піддаються ризику інсайдерських атак. Згідно зі звітом Альянсу хмарної безпеки за 2010 р. [5], внутрішні атаки є однією з семи найбільших загроз у хмарних обчисленнях. Тому постачальники хмарних послуг повинні забезпечити проведення ретельних перевірок співробітників, які мають фізичний доступ до серверів у дата-центрі. Крім того, центри обробки даних рекомендується часто моніторити на предмет підозрілої активності. Існує чотири основні аспекти безпеки в хмарі, за які відповідають як постачальники, так і клієнти [6]:

- обмеження доступу. Оскільки в хмарі всі ресурси доступні через Інтернет, дуже важливо переконатися, що лише належні користувачі матимуть доступ до потрібних їм інструментів протягом визначеного часу;
- захист даних. Організації повинні розуміти, де розташовано їхні ресурси, і застосувати відповідні елементи керування для захисту даних та інфраструктури, де вони розміщені;

- відновлення даних. У разі порушення безпеки надзвичайно важливо мати надійне рішення для резервного копіювання даних і план їхнього відновлення;
- план реагування. У разі атак організаціям потрібен спеціальний план, який дасть їм змогу зменшити наслідки та запобігти ураженню інших систем.

Загрози цілісності

Як і у будь-якій іншій системі, загрози безпеки для технологій хмарних обчислень можна поділити на загрози конфіденційності, цілісності та доступності. Загалом цілісність даних означає захист даних від несанкціонованого видалення, модифікації чи фальсифікації [10].

Предметом дослідження цієї статті є саме загрози цілісності, які розглянуто нижче:

1. *Несанкціонований доступ*.

Ця атака направлена на безконтрольні зміни даних, на які не зможе впливати авторизований користувач. Зловмисник, який проводить несанкціонований доступ з послідовною зміною даних, може провести атаку ззовні або зсередини організації-власника хмари. Це найсерйозніша атака, якщо це станеться, то витік даних відбуватиметься шляхом використання старого обладнання та повторного використання драйверів [11].

2. *Блокування даних*.

Ця загроза утворюється при переході від одного постачальника послуг до іншого. Так як різні постачальники надають різні послуги, тому при переході може трапитись втрата даних користувачів або їх блокування. У хмарі немає правил або умов щодо того, як зберігати дані, це залежить від постачальника хмарних послуг (CSP) [12]. Зазвичай, дані будуть розкидані по всьому серверу та системам. В ідеальній моделі міграція додатків від одного хмарного провайдера до іншого повинна бути простою, що є ще одним викликом для додатків хмарних обчислень, але оскільки кожен хмарний провайдер використовує окрему стандартну мову для своїх систем, це наразі неможливо.

3. *SQL-ін'єкції*.

SQL-ін’єкції націлені на SQL-сервери, які запускають уразливі програми баз даних. Хакери використовують вразливі місця веб-серверів і вводять шкідливий код, щоб обійти вхід і отримати несанкціонований доступ до серверних баз даних. У разі успіху хакери можуть маніпулювати вмістом баз даних, отримати конфіденційні дані, віддалено виконувати системні команди або навіть взяти під контроль веб-сервер для подальшої злочинної діяльності [13].

4. *Атака "людина посередині" (MiMA)*

MIMA зазвичай виникає, коли різні користувачі хмари спілкуються один з одним або спільно використовують ресурси з хмарного середовища [14]. Недостатнє шифрування може зробити користувачів вразливими до атаки "людина посередині", яка є непрямою атакою [15]. TLS – криптографічний протокол, який дозволяє клієнт-серверному додатку [16] запобігти підслуховуванню будь-якої конфіденційної інформації, що відбувається на HTTPS, який використовує TLS. Якщо людина отримує доступ до невідомої мережі і виконує свою роботу в HTTP, зловмисник, який виступає в ролі посередника, потім скористається цим, перехопивши всі конфіденційні дані через HTTPS-пакети.

5. *DDoS-атака*.

Мабуть, у сучасних технологіях це є найбільш серйозною проблемою, оскільки не може бути усуненою повністю. На сьогодні є лише деякі методи пом’якшення наслідків, які допомагають зменшити ризики та послідовності таких атак. DDoS-атаки націлені на веб-сайти та сервери, порушуючи роботу мережевих сервісів з метою виснаження ресурсів програми. Зловмисники, які стоять за цими атаками, наводнюють сайт несанкціонованим трафіком, що призводить до погіршення функціональності сайту або взагалі виводить його з ладу [17].

6. *Атаки на автентифікацію*.

Атаки на автентифікацію складно класифікувати як саме атаки на цілісність, але вони можуть спровокувати такі загрози, тому слід їх зазначити. Нижче наведено декілька відомих атак на автентифікацію:

- атака на відтворення.

Ця атака відбувається, коли невідома особа переглядає трафік даних, а потім надсилає комунікаційні дані на своє місце, як оригінального відправника. Щоб запобігти цій атаці, зазвичай впроваджують мітки часу та порядкові номери [18];

- атака грубої сили або атака за словником.

Це базова атака, при якій зловмисник перебирає всі можливі комбінації для пароля, щоб отримати доступ до даних користувачів. Чим більше довжина пароля, тим більше часу знадобиться зловмиснику, щоб вгадати правильний пароль [19];

- фішингова атака.

Йдеться про те, як зловмисник перебирає всі можливі способи атаки на жертву, підбираючи всі комбінації коду та паролів. Знов-таки, чим складніший код, тим більше часу знадобиться зловмиснику для його підбору [20], при цьому витрачений час буде зростати не лінійно.

7. *Атака відкату.*

Такі атаки можуть виникати під час оновлення системи у випадку, якщо постачальник у цей момент надає старе програмне забезпечення для користування. Це може спровокувати втрату даних, що зберігаються у цій системі. Відкат також відбувається без належного видалення старих даних користувача та оновлення системи до нової версії [21].

8. *Атака підробки тегів.*

Ця атака відбувається, якщо нечемний продавець обманює своїх клієнтів, показує неправильний штрих-код чи дає неправильне посилання. Якщо користувач сканує його на своєму пристрої, то зловмисник отримує доступ до всіх конфіденційних даних, що призводить до можливих ризиків шахрайства та витоку приватної інформації [21].

9. *Візантійська атака*.

Ця атака відбувається на різні частини хмарних обчислень шляхом зупинки або виходу з ладу систем. Це станеться, коли запит буде некоректно проходить через систему [21].

10. *Атака на систему доменних імен (DNS)*.

Ця атака відбувається, якщо систему атакує якесь шкідливе програмне забезпечення. DNS перетворює доменні імена на IP-адреси, і користувач не може бачити, наскільки правильно відбувається перетворення. Кожного разу, коли відкривається невідома веб-сторінка, зловмисник може легко отримати доступ до персональної інформації, що використовується на серверах [22].

11. *Сніфферні атаки*.

Атака відбувається, коли користувач натискає на деякі SOAP (Simple Object Access Protocol) – повідомлення або шкідливе посилання. Після того, як натиснуте посилання буде активоване, програма перехоплює потік пакетів в мережі і отримує доступ до персональних даних користувачів, таких як паролі, реквізити банківських рахунків тощо, які не є зашифрованими [23]. Залежно від обсягу даних та їх характеру, внаслідок цієї атаки втрати даних можуть бути непомітними або стати причиною великих проблем для цілої організації.

Методи забезпечення цілісності даних у хмарному середовищі

Проаналізувавши наведені вище загрози, перейдемо до методів забезпечення цілісності та запобігання атак на цілісність у хмарних сховищах. Як було зазначено, не завжди можна повністю усунути загрози, але майже завжди можна вжити заходи для їх запобігання та зменшення ймовірних втрат. Існує декілька механізмів та схем, які запропоновано для захисту володіння даними та їх цілісності в середовищі хмарних обчислень. Нижче наведено декілька механізмів та схем [21].

1. *Пом'якшення наслідків підробки тегів та атак витоку даних.*

Щоб запобігти цій атаці, існує схема, запропонована Yun Zhu та ін. [24], відома як Cooperative Provable Data Possession (CPCP), яка використовується в поєднанні з двома

іншими (Homomorphic Verifiable Response та Hash Index Hierarchy), що забезпечує прозору перевірку даних та надійний захист.

Сутність даного методу виглядає так: перед тим, як клієнт надсилає інформацію до CSP, він створює тег виклику, а надсилає його постачальнику хмарних послуг пізніше. Клієнт кидає виклик провайдеру хмарних послуг, перевіряючи цілісність даних за допомогою довіреної третьої сторони (TTP) [21].

2. *Послаблення атаки відкату*.

У запропонованій схемі захист від атаки відкату в хмарному середовищі здійснюється шляхом застосування методу геш-дерева Меркла [25, 26]. У цьому методі тег блоку даних та значення його лічильника оновлюються щоразу, коли оновлюються нові дані. Якщо зловмисник хоче змінити дані, значення лічильника також зміниться.

3. *Пом'якшення наслідків візантійського збою та зловмисних атак на дані*.

Рішенням для даної проблеми є запропонована Browers та ін. [27] криптосистема HAIL (High Availability and Integrity Layer) Protocol. Цей протокол гарантує, що дані користувача зберігаються неушкодженими і можуть бути безпечно отримані з серверів. Для забезпечення гарантії доступності даних використовується коригувальний код Erasure [21].

4. *Захист цілісності даних за допомогою шифрування*.

Даний метод є найкращим для загального захисту даних у хмарному середовищі та використовується у будь-якій системі. Оскільки технології продовжують розвиватися, а старі технології стають вразливіше, з'являтимуться нові методи злому шифрів, а також фатальні недоліки в старих методах шифрування. Хмарні провайдери повинні постійно оновлювати своє шифрування, оскільки дані, які вони зазвичай містять, є особливо цінними [7]. Перед тим як зберігати дані на сервері, слід зашифрувати їх та обчислити геш-значення даних. Це гарантуватиме, що дані не були змінені [28].

5. *Техніка доказового володіння даними (PDP)*.

Техніка PDP використовує протокол відповіді на запит для перевірки цілісності даних, що зберігаються на хмарному сервері. Цей метод використовує симетричне шифрування, наприклад MAC або будь-яке інше. Файл заповнюється метаданими перед зберіганням або надсиланням його на хмарний сервер. Після надсилання файлу до постачальника хмарних послуг користувач все одно зберігає метадані файлу, щоб перевірити його цілісність. Після цього користувач видаляє локальну копію файлу та перевіряє докази володіння файлом сервером за допомогою протоколу відповіді на виклик [29].

6. *Техніка доведення можливості вилучення (POR)*.

Метод Proof of Retrievability (POR) використовується для віддаленої перевірки даних, які зберігаються у постачальника хмарних послуг, за допомогою ключа автентифікації. У цьому методі дані не потрібно отримувати з CSP, і користувач також не зберігає оригінальну копію файлу локально. Користувач зберігає свій файл у CSP разом із ключем автентифікації. Потім користувач може перевірити цілісність даних за допомогою ключа автентифікації, не отримуючи файл з CSP [29, 9].

Висновки

Розглянуто поняття безпеки даних у хмарних обчисленнях та декілька з тих поширених загроз, що заважають забезпечити цілісність інформації, що там зберігається. Зараз технології хмарних обчислень – це те, чим люди користуються, майже не акцентуючи на це увагу, бо у сьогоденні це – явище, що зустрічається майже усюди та у кожній компанії. Не дивлячись на те, що хмарні технології зазвичай впроваджують найсучасніші технології безпеки, на жаль, абсолютно позбутись усіх ризиків неможливо. Також розглянуто можливі методи вирішення проблем, мінімізування можливих вразливостей від атак та забезпечення цілісності у хмарних обчисленнях.

Список літератури:

1. P. Mell and T. Grance. The NIST Definition of Cloud Computing // National Institute of Standards and Technology. 2009. Vol.53,no.6. P. 50.

2. Reese G. (2009) Cloud Application Architectures: Building Applications and Infrastructure in the Cloud. Sebastopol. California : O'Reilly Media.

3. Buyya R., Yeo C.S., Venugopal S., Broberg J., and Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility // Future Generation Computer Systems. 2009. 25 (6). P. 599 – 616.

4. Cloud computing security. Режим доступу: http://en.wikipedia.org/wiki/Cloud_ computing_security.

5. Top Threats to Cloud Computing v1.0 Cloud Security Alliance.

6. Що таке безпека в хмарі?, Microsoft. Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cloud-security.

7. Rukavitsyn Andrey, Borisenko Konstantin, Holod Ivan, Shorov Andrey. The method of ensuring confidentiality and integrity data in cloud computing // 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM). 2009. P. 272 – 274.

8. Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu – Data Security and Privacy in Cloud Computing.

9. M. S. Giri, B. Gaur, D. Tomar. A Survey on Data Integrity Techniques in Cloud Computing.

10. Yunchuan Sun, Junsheng Zhang zhangjs, Yongping Xiong, and Guangyu Zhu (2014. Data Security and Privacy in Cloud Computing.

11. Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. Vulnerability prioritization, root cause analysis, and mitigation of secure data analytic framework implemented with mongodb on singularity linux containers // Proceedings of the 2020 the 4th International Conference on Compute and Data Analysis. 2020. P. 58 – 66.

12. A. Jyoti, M. Shrimali, S. Tiwari, and H. P. Singh. Cloud computing using load balancing and service broker policy for IT service: a taxonomy and survey // Ambient Intell. Humaniz. Comput., vol. 11, no. 11, pp. 4785 – 4814, Nov. 2020, doi: 10.1007/s12652-020-01747-z.

13. Te-Shun Chou. Security threats on cloud computing vulnerabilities // International Journal of Computer Science & Information Technology (IJCSIT) Vol. 5, No 3, June 2013, pp. 84 – 85.

14. Ramandeep Kaur, Pushpendra Kumar Pateriya. A Study on Security Requirements in Different Cloud Frameworks // International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Vol.3, Iss.1, March 2013, pp.134 – 135.

15. Y. Chen, L. Li, and Z. Chen. An Approach to Verifying Data Integrity for Cloud Storage // 2017 13th International Conference on Computational Intelligence and Security (CIS), Dec. 2017, pp. 582 – 585, doi: 10.1109/CIS.2017.00135.

16. H. Mohapatra. Handling of Man-In-The-Middle Attack in WSN Through Intrusion Detection System // Int. J. Emerg. Trends Eng. Res., vol. 8, no. 5, pp. 1503 – 1510, May 2020, doi: 10.30534/ijeter/2020/05852020.

17. What is a DDoS attack? Режим доступу – https://www.microsoft.com/en-us/security/business/security-101/what-is-a-ddos-attack.

18. Lai Cheng-I., Alberto Abad, Korin Richmond, Junichi Yamagishi, NajimDehak, and Simon King. Attentive filtering networks for audio replay attack detection // ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 6316 – 6320. IEEE, 2019.

19. Shetty, Roshan Ramprasad, Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, Ravi Vadapalli, and Hafiz Khan. Secure NoSQL based medical data processing and retrieval: the exposome project // Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 99 – 105. 2017.

20. Mailewa Dissanayaka, Akalanka, Roshan Ramprasad Shetty, Samip Kothari, Susan Mengel, Lisa Gittner, and Ravi Vadapalli. A review of MongoDB and singularity container security in regards to hipaa regulations // Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 91 – 97. 2017.

21. Survey on various data integrity attacks in cloud environment and the solutions // IEEE Conference Publication. Режим доступу – https://ieeexplore.ieee.org/abstract/document/6528889.

22. Thapa, Suman, and Akalanka Mailewa. The Role of Intrusion Detection/Prevention Systems in Modern Computer Networks: A Review // Conference: Midwest Instruction and Computing Symposium (MICS), vol. 53, pp. 1 – 14. 2020.

23. S. Sudalai and S. S., A Survey on Cloud Security Issues and Challenges with Possible MeasuresA Survey on Cloud Security Issues and Challenges with Possible Measures. 2016.

24. Y. Zhu, H. Hu, G. Ahn, and M. Yu. Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage // IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231 – 2244, Dec. 2012, doi: 10.1109/TPDS.2012.66.

25. J. Feng, Y. Chen, D. H. Summerville, and K. Hwang. Fair Non-repudiation Framework for Cloud Storage: Part II // Cloud Computing for Enterprise Architectures, Z. Mahmood and R. Hill, Eds. London: Springer, 2011, pp. 283 – 300.

26. J. Feng, Y. Chen, D. Summerville, W. Ku, and Z. Su. Enhancing cloud storage security against roll-back attacks with a new fair multi-party nonrepudiation protocol // 2011 IEEE Consumer Communications and Networking Conference (CCNC), Jan. 2011, pp. 521 – 522, doi: 10.1109/CCNC.2011.5766528.

27. H. Lin and W. Tzeng. A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding // IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 6, pp. 995 – 1003, Jun. 2012, doi: 10.1109/TPDS.2011.252.

28. R. V. Rao and K. Selvamani. Data Security Challenges and Its Solutions in Cloud Computing // Procedia Comput. Sci., vol. 48, pp. 204 – 209, Jan.2015, doi: 10.1016/j.procs.2015.04.171.

29. K. N. Sevis and E. Seker. Survey on Data Integrity in Cloud // 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), Jun. 2016, pp. 167 – 171, doi: 10.1109/CSCloud.2016.35.

Надійшла до редколегії 11.03.2023

Відомості про авторів:

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; науковий співробітник-консультант АТ «Інститут Інформаційних технологій»; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606

Кравченко Софія Олександрівна – Харківський національний університет імені В. Н. Каразіна, студентка кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: sofiya.krav@gmail.com

Кравченко Анастасія Андріївна – Харківський національний університет імені В. Н. Каразіна, студентка кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: aakrav02@gmail.com