ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ В CLOUD, FOG ТА EDGE COMPUTING СИСТЕМАХ

Єременко О.С., Круглова А.О., Журавльова А.С., Персіков М.А.

Харківський національний університет
радіоелектроніки, Україна

E-mail: oleksandra.yeremenko.ua@ieee.org,
anastasiia.kruhlova@nure.ua,
anna.zhuravlova@nure.ua,
mihapersikov@gmail.com

Abstract

An analysis of modern architectural approaches to complex resilience of distributed systems built using so-called integrated cloud computing technologies, including Cloud, Fog, and Edge Computing, was conducted. Classes of solutions on resilience improvement, as well as threats to the resilience of infocommunication networks and means of its provision are covered. The task of developing a universal flexible system of control, monitoring, and response is formulated in order to identify possible degradation of the Quality of Service, resilience, and security in the network and take corrective action according to its architecture and types of services provided.

Відмовостійкість інфокомунікаційної мережі (ІКМ) та відповідних сервісів, що надаються кінцевим користувачам, залежить від її готовності до різних перебоїв або навіть катастроф, які можуть спричинити внутрішні та зовнішні чинники [1, 2]. Ненадійне функціонування мережі, управління, надання мережних сервісів, користування застосунками, доступ користувачів та їхня поведінка, які можуть негативно вплинути на відмовостійкість мережі, є внутрішніми чинниками. Тим часом природні явища та погодні умови можуть бути зовнішніми чинниками, що спричиняють порушення роботи мережі або надання послуг [1].

Слід відмітити, що на сьогоднішній день все більша кількість великих розподілених систем будується шляхом використання технологій Cloud, Fog та Edge Computing – хмарних, туманних і граничних обчислень відповідно [1, 3, 4]. При цьому постає важливе завдання забезпечення відмовостійкості подібних систем. В роботі було проведено аналіз сучасних архітектурних підходів щодо комплексного забезпечення відмовостійкості розподілених систем, побудованих за допомогою технологій так званих комплексних хмарних обчислень, що включають в себе Cloud, Fog та Edge Computing.

Отже, у разі порушення функціонування мережі або послуги засоби відмовостійкості мають бути здатними відновити та забезпечити прийнятний рівень обслуговування користувачів. Водночас, для того щоб задовольнити жорсткі вимоги до надійності, ІКМ повинні бути здатними ефективно реагувати на відмови та збої, які стають усе більш імовірними зі збільшенням масштабів мереж. У загальному випадку відмовостійкість тої чи іншої системи характеризується та оцінюється відповідно до основного завдання, яке ця система має виконувати. Наприклад, рішення для резервного копіювання мають бути стійкими до втрати даних, але не обов'язково ефективні проти витоку даних (це площина відповідальності кібер-стійкості).

Складні розподілені системи функціонують в умовах різноманітних факторів, які можуть вплинути на нормальну роботу системи, це означає, що реалізації системи з підтримкою відмовостійкості повинні враховувати різні фактори. Залежно від типу сервісів, що надаються системою, такі фактори можуть включати, але не обмежуються наступними: слабким (або перерваним) зв'язком, обмеженою потужністю та розвинутими стійкими загрозами (Advanced Persistent Threats, APT) тощо [4-7]. На практиці рішення щодо підвищення відмовостійкості зазвичай фокусуються на деякій множині деструктивних факторів і умовно розділяються на наступні класи [4]:

1. Ємність системи (capacity), що означає відмовостійкість щодо її дозволеного використання (запобігання перевантаження). Тут фізичний зміст «ємності» може характеризуватися, наприклад, обсягом даних, що обробляються, та кількістю користувачів, що обслуговуються.
2. Достовірність системи (trustworthiness), що означає відмовостійкість до небажаного використання. Типові засоби забезпечення відмовостійкості в цьому контексті включають в себе шифрування, сертифікати, а також підходи, орієнтовані на довіру.
3. Ефективність системи (efficiency), що означає відмовостійкість до фізичних обмежень та граничних значень. Типовими прикладами таких обмежень є нестабільність ліній зв'язку (радіо), акумулятори малої ємності та стихійні лиха.

Не дивлячись на те, що на сьогоднішній день не розроблено універсальних метрик відмовостійкості, зазвичай використовуються спеціалізовані метрики відповідно до рівнів інфокомунікаційних систем. Тобто залежно від типу ІКМ, відмовостійкість до специфічних потенційних збоїв може забезпечуватися на різних рівнях відповідними засобами, а саме на *фізичному*, *мережному*, *протокольному* та *сервісному* рівнях (Табл. 1) [4].

Таблиця 1. Загрози відмовостійкості ІКМ і засоби її забезпечення

Рівень	Засоби забезпечення відмовостійкості	Вплив на продуктивність ІКМ
Сервісний	Поступова деградація, вимушене зниження якості обслуговування	Використання технологій cyber-foraging для розвантаження мережних пристроїв з низькою обчислювальною потужністю шляхом залучення більш потужних вузлів мережі
Протокольний	Кодування даних з виправленням помилок	Поступова деградація (наприклад, компресія даних)
Мережний	Перемаршрутизація	Резервування (ресурсна надмірність при використанні основних і резервних маршрутів)
Фізичний	Резервування (ручне відновлення)	Резервування, що надається за вимогою

Таким чином, виникає завдання розробки універсальної гнучкої системи контролю, моніторингу та реагування з метою виявлення можливого погіршення якості обслуговування, відмовостійксоті та безпеки в ІКМ та вжиття коригувальних дій з урахуванням її архітектури та типів послуг, що надаються.

Література:

1. *Rak J., Hutchison D. (eds)* Guide to Disaster-Resilient Communication Networks. Computer Communications and Networks. Springer, Cham. 2020. 813 p. DOI: https://doi.org/10.1007/978-3-030-44685-7.

2. *Shirazi S.N., Gouglidis A., Farshad A., Hutchison D.* The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective. IEEE Journal on Selected Areas in Communications. 2017. Vol. 35, No.11. P. 2586-2595. DOI: https://doi.org/10.1109/JSAC.2017.2760478.

3. *Персіков М.А., Жерноклеєв В.С., Рибінський В.М.* Створення глобальної мережі розумних пристроїв на основі концепції Internet of Everything. Третя міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології». Збірник наукових праць. Харків: ХНУРЕ. 2019. С. 129.

4. *Prokhorenko V., Babar M.A.* Architectural Resilience in Cloud, Fog and Edge Systems: A Survey. IEEE Access. 2020. Vol. 8. P. 28078-28095. DOI: https://doi.org/10.1109/ACCESS.2020.2971007.

5. *Modarresi A., Gangadhar S., Sterbenz J. P. G.* A framework for improving network resilience using SDN and fog nodes. 2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM), Alghero. 2017. P. 1-7. DOI: https://doi.org/10.1109/RNDM.2017.8093036.

6. *Huang H., Guo S.* Proactive Failure Recovery for NFV in Distributed Edge Computing. IEEE Communications Magazine. 2019. Vol. 57, No. 5. P. 131-137. DOI: https://doi.org/10.1109/MCOM.2019.1701366.

7. *Sterbenz J. P. G.* Smart city and IoT resilience, survivability, and disruption tolerance: Challenges, modelling, and a survey of research opportunities. *2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM),* Alghero. 2017. P. 1-6. DOI: https://doi.org/10.1109/RNDM.2017.8093025.