УДК 004.75:004.056]:001.89

БЕЗПЕЧНА ПЛАТФОРМА НА БАЗІ AWS ДЛЯ ЗБОРУ ДАНИХ ТА СПІВПРАЦІ ДОСЛІДНИКІВ.

Григор'єв Д.А., Кривенко С.А.
e-mail: danylo.hryhoriev@nure.ua, stanislav.kryvenko@nure.ua
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна

This research explores architectural best practices for deploying a secure, scalable AWS platform that hosts global development statistics for social science researchers. The proposed architecture leverages Amazon Web Services to provide secure MySQL database hosting, controlled administrative access, and anonymous public web access. By implementing EC2 instances in private subnets, load balancing, and auto-scaling capabilities, the platform ensures high availability and performance. This design balances security requirements with accessibility needs, creating a robust infrastructure for data collection and researcher collaboration without requiring HTTPS or custom domain implementation.

Дослідники в галузі соціальних наук дедалі більше покладаються на централізовані платформи для доступу до статистики глобального розвитку та співпраці над проєктами, заснованими на даних. Однак створення безпечної, масштабованої інфраструктури, яка захищає конфіденційні дані, водночас надаючи відкритий доступ дослідникам, пов'язане з унікальними архітектурними викликами. Згідно з AWS [1], хмарні рішення пропонують гнучкі моделі безпеки, які можуть забезпечити як публічний доступ, так і адміністративний контроль в межах однієї інфраструктури. У цій публікації розглядається, як Amazon Web Services можна використовувати для створення платформи, яка відповідає конкретним потребам дослідницьких спільнот у галузі соціальних наук. Запропонована архітектура відповідає критичним вимогам, включаючи безпечне розміщення баз даних, контрольований адміністративний доступ, анонімний публічний доступ, високу доступність та автоматичне масштабування. Розуміючи ці архітектурні компоненти, студенти та викладачі можуть краще зрозуміти, як сучасна хмарна інфраструктура підтримує академічні дослідницькі ініціативи, зберігаючи при цьому відповідні межі безпеки.

Метою роботи є дослідження безпечної платформи на базі AWS для збору даних та співпраці дослідників.

Основою цієї архітектури є безпечне розміщення бази даних MySQL в AWS. База даних має бути розгорнута за допомогою Amazon RDS (Relational Database Service), яка забезпечує автоматичне резервне копіювання, керування виправленнями та шифрування в стані спокою. Розміщуючи екземпляр RDS у приватних підмережах без прямого доступу до Інтернету, база даних залишається захищеною від зовнішніх загроз, залишаючись доступною для серверів додатків у віртуальній приватній хмарі (VPC).

Безпечний доступ до бази даних вимагає впровадження кількох рівнів автентифікації та мережевого контролю. Групи безпеки повинні обмежувати підключення до бази даних виключно серверами додатків, тоді як політики IAM (Identity and Access Management) контролюють, які ресурси AWS можуть взаємодіяти з базою даних. Адміністративний доступ здійснюється через SSH-підключення до екземплярів EC2, при цьому адміністратори підключаються через хост-бастіон або AWS Systems Manager Session Manager, щоб уникнути безпосереднього доступу до портів SSH до Інтернету.

Веб-додаток працює на екземплярах t2.micro EC2, розгорнутих у приватних підмережах у кількох зонах доступності. Ці екземпляри розміщують код програми, який запитує базу даних та надає контент дослідникам. Розміщуючи їх у приватних підмережах, до екземплярів неможливо отримати прямий доступ з Інтернету, що зменшує поверхню атаки. Згідно з Amazon Web Services [2], цей архітектурний шаблон значно покращує безпеку, зберігаючи при цьому функціональність для загальнодоступних програм.

Висока доступність досягається за допомогою балансувальника навантаження програм (ALB), розгорнутого в загальнодоступних підмережах. ALB розподіляє вхідний трафік між справними екземплярами EC2 у кількох зонах доступності, гарантуючи, що веб-сайт залишається доступним, навіть якщо окремі екземпляри або цілі зони доступності зазнають збоїв. Перевірки справності постійно контролюють стан екземплярів, автоматично спрямовуючи трафік від несправних цілей. Перевірки справності (Health Checks) – це критичний механізм для автоматичного відновлення: Періодичність: ALB надсилає запити (наприклад, GET /health) до кожного екземпляра EC2 кожні кілька секунд. Поріг відмови (Unhealthy Threshold): Якщо екземпляр не відповідає певну кількість разів поспіль, він маркується як "Unhealthy". Ізоляція: Трафік миттєво припиняє надходити на несправний екземпляр. Як тільки екземпляр знову проходить перевірку (Healthy Threshold), ALB автоматично повертає його в ротацію.

Автоматичне масштабування реагує на коливання трафіку за допомогою групи автоматичного масштабування, налаштованої за допомогою шаблону запуску. Шаблон запуску визначає конфігурацію екземпляра, включаючи AMI, тип екземпляра, групи безпеки та сценарії даних користувача. Політики масштабування запускають або завершують запуски екземплярів на основі таких показників, як використання процесора або кількість запитів, гарантуючи, що платформа підтримує продуктивність під час пікового навантаження, мінімізуючи витрати в періоди низького трафіку.

Анонімний доступ до веб-користувачів забезпечується за допомогою загальнодоступного балансувальника навантаження, який не вимагає автентифікації для дослідників, які отримують доступ до статистики та візуалізації даних. Ця модель відкритого доступу підтримує академічну місію демократизації даних, тоді як засоби контролю безпеки серверної частини захищають базову інфраструктуру та базу даних. Ось ключові аспекти такої реалізації. Демократизація даних: Використання Google Cloud Load Balancing або AWS Elastic Load Balancing дозволяє обробляти велику кількість запитів від дослідників без затримок, забезпечуючи стабільний доступ до візуалізацій. Безпека інфраструктури: Поки фронтенд залишається відкритим, бекенд-сервери зазвичай розміщуються в приватних підмережах (Private Subnets) і доступні лише через обмежені порти, що мінімізує ризики згідно з порадами OWASP щодо безпеки API.

Міркування щодо практичного впровадження. Ця архітектура вимагає ретельного налаштування VPC з публічними та приватними підмережами в кількох зонах доступності. Групи безпеки реалізують принципи доступу з найменшими привілеями, дозволяючи лише необхідний трафік між компонентами. Моніторинг CloudWatch забезпечує видимість продуктивності системи та подій безпеки, що дозволяє швидко реагувати на інциденти.

Висновок.

Створення безпечної платформи для досліджень у галузі соціальних наук, що розміщується на базі AWS, вимагає ретельного архітектурного планування, яке поєднує доступність та безпеку. Завдяки впровадженню безпечного розміщення баз даних, контрольованого адміністративного доступу, балансування навантаження та автоматичного масштабування, ця архітектура забезпечує надійну основу для збору даних та співпраці дослідників. Розділення публічних та приватних мережевих рівнів у поєднанні з керованими сервісами AWS створює платформу, яка відповідає академічним потребам, зберігаючи при цьому відповідні засоби контролю безпеки. Студенти та викладачі можуть застосовувати ці архітектурні принципи до подібних проектів, що потребують безпечної, масштабованої інфраструктури для досліджень та співпраці.

Список використаних джерел:

1. Amazon Web Services, “AWS security best practices,” AWS Whitepaper, 2023. [Online]. Available: https://docs.aws.amazon.com/pdfs/whitepapers/latest/aws-security-best-practices/aws-security-best-practices.pdf. [Accessed: Feb. 21, 2026].

2. Amazon Web Services, "Architecting on AWS: Best practices for security," AWS Documentation, 2024. [Online]. Available: https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html. [Accessed: Feb. 21, 2026].