УДК 004.056.5(043.2)

Д. Ю. Радзіховський

СИСТЕМА АВТОМАТИЗОВАНОГО КЕРУВАННЯ БЕЗПЕКОЮ ЗАСТОСУНКІВ У ХМАРНОМУ СЕРЕДОВИЩІ

Вінницький національний технічний університет

Анотація. *Робота присвячена розробці автоматизованої підсистеми для забезпечення безпеки застосунків у хмарному середовищі. Розглянуто ключові виклики та ризики, пов'язані з хмарними технологіями, а також методи і підходи для їх вирішення. Практична значимість роботи полягає у підвищенні надійності та безпеки хмарних застосунків..*

Ключові слова: *Хмарне середовище, безпека застосунків, автоматизоване керування.*

Abstract. *This work is dedicated to the development of an automated subsystem for ensuring the security of applications in a cloud environment. It addresses the key challenges and risks associated with cloud technologies, as well as the methods and approaches to resolve them. The practical significance of this study lies in enhancing the reliability and security of cloud applications.*

Keywords: *Cloud environment, application security, automated management.*

Вступ

У наш час, коли цифрова трансформація набирає обертів, хмарні технології відіграють ключову роль у глобальній IT-інфраструктурі. Завдяки своїй гнучкості, масштабованості та економічній ефективності, хмарні рішення стали невід'ємною частиною бізнес-процесів багатьох компаній і організацій. Вони пропонують нові можливості для зберігання даних, їх обробки та управління. Однак, разом із численними перевагами, хмарні технології приносять і нові виклики, особливо в аспекті кібербезпеки.

Дана робота зосереджується на розробці підсистеми автоматизованого керування безпекою застосунків у хмарному середовищі. Основна увага приділяється ідентифікації ключових ризиків, пов'язаних з хмарними технологіями, та розробці інноваційних рішень, здатних забезпечити високий рівень захисту інформації та застосунків, розгорнутих в хмарному середовищі. Робота включає аналіз популярних хмарних платформ, зокрема Amazon Web Services (AWS), та визначення специфічних вимог до системи безпеки. Ключовим аспектом є інтеграція сучасних методів автоматизації, забезпечення безпеки, та врахування особливостей хмарних технологій.

Результати дослідження

Головна задача розробників полягає у створенні додатків, які б відрізнялися високою ефективністю: були б надійними, зручними у використанні, легко адаптовувалися до нових вимог та були захищені.

У прагненні підвищити продуктивність та оптимізувати час розробки програмного забезпечення, було створено інструменти, які покращують процес планування та моделювання систем, запобігаючи критичним помилкам, які можуть стати відомими лише після написання значної кількості коду. Використання моделей є ключем для чіткої візуалізації структури та функціонування системи, керування архітектурою, зниження ризиків. Моделювання підсилює розуміння системи, що сприяє її спрощенню і забезпечує можливості для повторного використання. Систему можна описати під різними кутами, використовуючи різноманітні моделі, кожна з яких представляє важливу абстракцію системи.

Щоб створити комплексну, безпечну та ефективну веб-програму, наша розробка буде слідувати найкращим практикам сучасної веб-архітектури, використовуючи весь спектр послуг AWS. На рисунку 1 наведено архітектуру системи веб-додатку розроблену з використанням хмарного середовища AWS та керуючись усіма актуальними політиками та сервісами безпеки.

Цей інтегрований підхід до архітектури не лише забезпечує високий рівень безпеки та надійності, але й забезпечує гнучкість та масштабованість, що є необхідними для сучасних додатків. Завдяки хмарним сервісам AWS, таким як Elastic Compute Cloud (EC2), Simple Storage Service (S3), і

DynamoDB, можна гарантувати не тільки ефективне зберігання даних, але й швидку їх обробку і відмінну продуктивність системи.

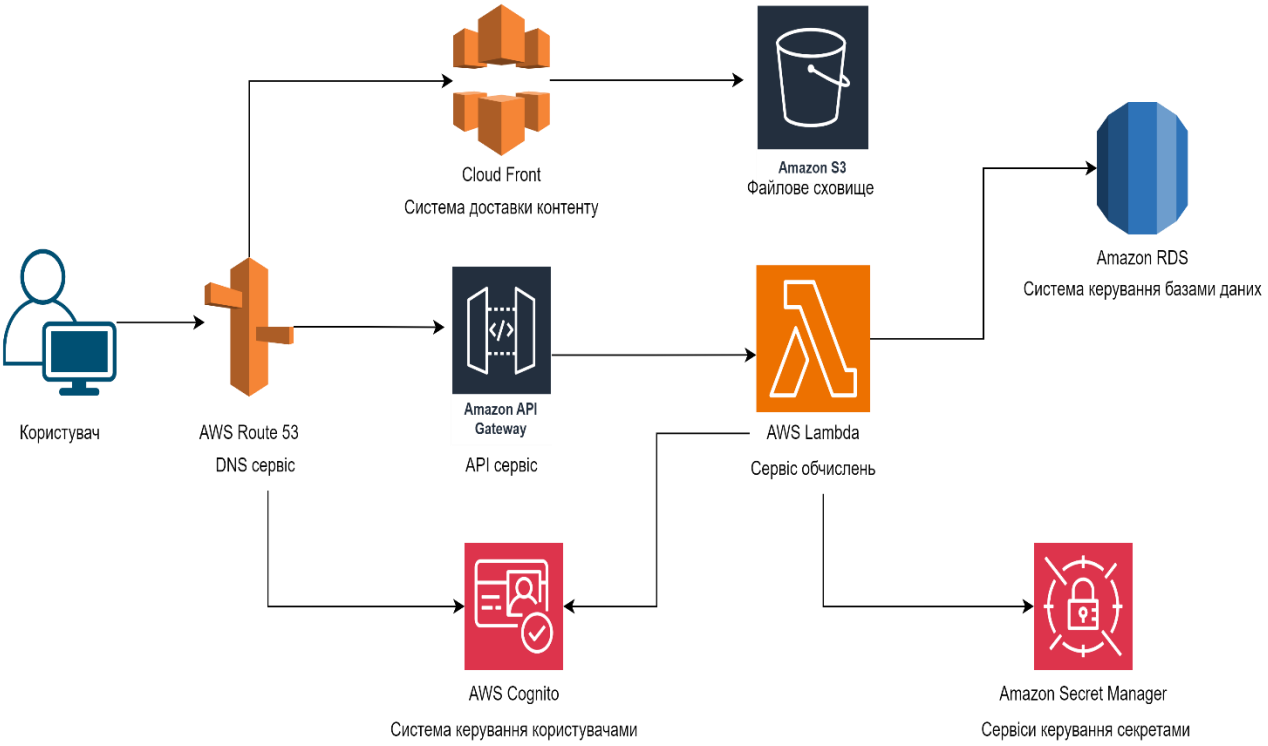

Рисунок 1 – Архітектура системи

Починаючи з Amazon S3, статичний веб-контент, як-от файли HTML, CSS і JavaScript, зберігатиметься в надійній службі зберігання. Глобальне охоплення та доступність S3 гарантують, що вміст веб-програми резервовано зберігається на кількох пристроях у кількох приміщеннях, захищаючи від втрати даних. Крім того, точні засоби контролю доступу S3 та інтеграція з AWS Identity and Access Management (IAM) дозволять безпечно керувати доступом до вмісту веб-програми.

Amazon Cognito забезпечить ідентифікацію користувача та службу синхронізації даних, яка забезпечить безпечний доступ та автентифікацію користувачів. За допомогою Cognito веб-додаток забезпечить реєстрацію та вхід користувачів. Він також підтримує об'єднання з постачальниками ідентифікаційної інформації через SAML 2.0 або OpenID Connect, що означає, що є можливість легко інтегрувати функції входу сторонніх постачальників, таких як Google, Facebook і Amazon, покращуючи взаємодію з користувачем, надаючи більше варіантів входу.

Для RESTful API шлюз Amazon API діятиме як вхідні двері, полегшуючи обробку запитів і відповідей, а також керування трафіком, керування версіями API та моніторинг. Використовуючи безсерверну модель виконання AWS Lambda для серверних служб, код буде запускатися без підготовки та керування серверами. Ця безсерверна архітектура є високомасштабованою та економічно ефективною, оскільки оплата відбувається лише за витрачений обчислювальний час.

Amazon RDS підтримає вимоги до бази даних, забезпечуючи змінний розмір реляційної бази даних галузевого стандарту та керуючи трудомісткими завданнями адміністрування бази даних. RDS підтримує кілька механізмів баз даних, включаючи Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database і SQL Server.

За допомогою AWS Secrets Manager відбудеться автоматизація ротації секретів, таких як облікові дані бази даних, ключі API та інша конфіденційна інформація. Це допоможе дотримуватися найкращих практик управління секретами та значно зменшить потенційний ризик зламу облікових даних.

Впровадження Amazon CloudFront, надасть можливість зменшити час завантаження та покращити безпеку. CloudFront розповсюджуватиме веб-додаток по всьому світу за допомогою мережі

периферійних місць, надаючи вміст із меншою затримкою. Цей CDN кешуватиме статичні активи веб-програми, зменшуючи кількість прямих запитів до сегментів S3, покращуючи взаємодію з користувачем завдяки швидшому часу завантаження. Крім того, інтеграція CloudFront із брандмауером веб-застосунків AWS (WAF) і AWS Shield забезпечує надійний захист від різноманітних типів атак, включаючи DDoS-атаки на мережевому та прикладному рівні, що забезпечує доступність програми та безпеку користувачів.

Щоб доповнити CloudFront, буде використано Amazon Route 53, який запропонує маршрутизацію трафіку на рівні DNS до веб-програми. Здатність Route 53 підключати запити користувачів до інфраструктури, що працює в AWS, наприклад сегмента Amazon S3, екземпляра Amazon EC2 або Elastic Load Balancer, надає високодоступну та масштабовану хмарну веб-службу системи доменних імен (DNS).

Безпека має першочергове значення, і всі дані, що передаються, будуть зашифровані за допомогою сертифікатів безпеки транспортного рівня (TLS), керованих диспетчером сертифікатів AWS, який також керуватиме процесом оновлення.

Висновки

Кульмінацією цього процесу стане сучасний адаптивний веб-додаток, який не тільки відповідає поточним вимогам, але й надійно розроблений для майбутнього масштабування та вдосконалення. Стратегічне використання послуг AWS створить міцну основу, яка оптимізує доставку цінностей, менше акцентуючи увагу на тонкощах управління інфраструктурою. Ця збірка ретельно розроблена з урахуванням масштабованості, продуктивності та підвищеної безпеки, що забезпечує стабільну стійкість додатків перед обличчям коливань вимог і нових загроз безпеці. Завдяки впровадженню цих розширених заходів безпеки та використанню безпечної інфраструктури AWS за своєю суттю програма буде добре обладнана для захисту як від внутрішніх, так і від зовнішніх вразливостей. Ця проактивна та комплексна система безпеки гарантує, що веб-програма залишається безпечною та надійною, що є першорядним у сучасній цифровій екосистемі. Це підкреслює прихильність до безпеки, яка йде рука об руку з прагненням до інновацій, забезпечуючи таким чином конкурентну перевагу на цифровому ринку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. AWS® Essentials for Dummies, Abound Academy. 2022. 225 с.
2. Andreas Wittig, Michael Wittig. Amazon Web Services in Action, Manning Publications Co 2022. 426 с.
3. 14 Best AWS Security Tools and Services for 2023. URL : https://sonraisecurity.com/blog/aws-security-tools/ (дата звернення: 17.10.2023) .

Радзіховський Дмитро Юрійович — студент групи 1БС-22м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: Dimaradvin@gmail.com.*

Radzikhovskiy Dmytro Y. — Department of Information Techologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, email : Dimaradvin@gmail.com.

Шелепало Галина Василівна — к. фіз.-мат. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна.

Shelepalo Halyna V. — PhD (Eng), Associated Professor of Data Protection Department in Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine..