https://doi.org/10.33778/kcsa.2024.24.1.035

멀티테넌시 환경에서 안전한 웹 사이트 개발을 위한 데이터 격리 방법 분석★

김 점 구*

요 약

멀티테넌시 아키텍처는 클라우드 기반 서비스와 애플리케이션에서 중요한 역할을 하며, 이러한 환경에서 데이터 격리는 중요한 보안 과제로 부각되고 있다. 본 논문은 스키마 기반 격리, 논리적 격리, 물리적 격리 등 다양한 데이터 격리 방법들을 조사하고, 각각의 장단점을 비교 분석하였다. 데이터 격리 방법들의 실질적인 적용 사례와 효과를 평가하고, 이를 통해 멀티테넌트 웹 사이트 개발 시 고려해야 할 보안 요소들과 데이터 격리 방법의 선택 기준을 제안하였다. 본 논문은 멀티테넌시 환경에서의 데이터 보안을 강화하려는 개발자, 아키텍트 및 시스템 관리자에게 중요한 지침을 제안하고, 효율적이고 안전한 멀티테넌트 웹 사이트의 설계와 구현을 위한 기초적인 프레임워크를 제안한다. 그리고 데이터 격리 방법의 선택이 시스템의 성능, 확장성, 유지관리 용이성 및 전반적인 보안에 어떻게 영향을 미치는지에 대한 통찰력을 제공하며, 이를 통해 멀티테넌트 시스템의 보안과 안정성을 향상시키는 방안을 모색하였다.

Analysis of Data Isolation Methods for Secure Web Site Development in a Multi-Tenancy Environment

Jeom Goo Kim*

ABSTRACT

Multi-tenancy architecture plays a crucial role in cloud-based services and applications, and data isolation within such environments has emerged as a significant security challenge. This paper investigates various data isolation methods including schema-based isolation, logical isolation, and physical isolation, and compares their respective advantages and disadvantages. It evaluates the practical application and effectiveness of these data isolation methods, proposing security considerations and selection criteria for data isolation in the development of multi-tenant websites. This paper offers important guidance for developers, architects, and system administrators aiming to enhance data security in multi-tenancy environments. It suggests a foundational framework for the design and implementation of efficient and secure multi-tenant websites. Additionally, it provides insights into how the choice of data isolation methods impacts system performance, scalability, maintenance ease, and overall security, exploring ways to improve the security and stability of multi-tenant systems.

Key-words: 멀티테넌시, 멀티테넌트, 데이터 격리, 웹 사이트, 클라우드

접수일(2024년 02월 05일), 수정일(1차: 2024년 03월 25일), (2차: 2024년 03월 29일), 게재확정일(2024년 03월 30일)

* 남서울대학교/컴퓨터소프트웨어학과

★ 본 논문은 2023한년도 남서울대학교 교내연구비 지원에 의해서 연구되었음

1. 서 론

최근 클라우드 컴퓨팅의 성장과 함께 멀티테넌트 웹 사이트의 중요성이 부각되고 있다. 멀티테넌시 아키텍처는 다수의 사용자(테넌트)가 단일 인스턴스의 애플리케이션 및 인프라를 공유하면서 각자의 데이터와 설정을 유지하는 방식을 제공한다[1]. 이러한 아키텍처는 효율성, 확장성 및 비용 절감 측면에서 많은 이점을 제공하지만, 동시에 데이터 보안과 격리 측면에서 중요한 문제점을 안고 있다.

멀티테넌시 환경에서 각 테넌트의 데이터 보안과 프라이버시를 보장하는 것은 필수적이다. 데이터 격리는 이러한 환경에서 중요한 보안 과제로, 테넌트 간 데이터 누출을 방지하고, 각 테넌트가 자신의 데이터에만 접근할 수 있도록 보장하여야 한다.

본 논문은 다양한 데이터 격리 방법을 분석하고, 이들의 효율성, 보안성, 관리 용이성, 그리고 멀티테넌시 환경에서의 적용 가능성을 평가하는 것이다. 이를 통해 멀티테넌트 웹 사이트 개발자와 관리자들이 보다 안전하고 효과적인 데이터 격리 전략을 선택할 수 있도록 지원하고자 한다.

이 논문은 문헌 조사, 사례 연구, 전문가 인터뷰 등 다양한 방법론을 통해 데이터 격리 방법을 분석하였다.

멀티테넌트 웹 사이트의 보안을 강화하는 것은 기업과 조직에 있어 중대한 과제이다. 본 논문을 통해 도출되는 데이터 격리 방법의 분석 결과는 웹 사이트 개발 및 운영에 있어 실질적인 가이드라인을 제공할 것이다. 또한, 이 연구는 멀티테넌시 환경에서 데이터 보안과 관련된 최고의 환경을 정립하는 데 기여할 것으로 기대가 된다.

2. 관련연구

2.1 멀티테넌트 아키텍처

멀티테넌트 아키텍처는 클라우드 컴퓨팅 및 SaaS(Software as a Service) 모델에서 일반적으로 사용되며, 하나의 애플리케이션 인스턴스(instance)가 여러 사용자 또는 조직(테넌트)에 서비스를 제공하는 구조이다. 이러한 구조는 리소스를 공유함으로써 운영비용을 절감하고 관리 효율성을 높이는 장점을 가지고 있습니다[1].

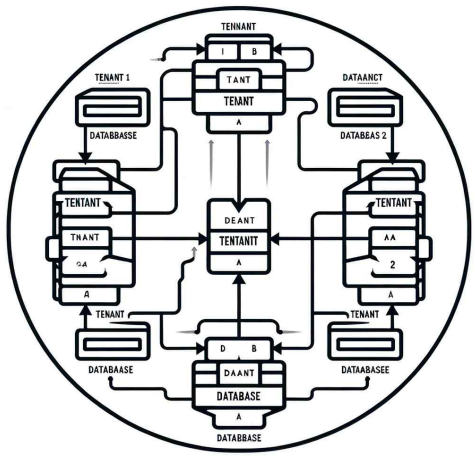

그림 멀티테넌트 구조

2.2 멀티테넌시 환경의 데이터 격리

멀티테넌트 환경에서 데이터를 효과적으로 격리하는 것은 기술적으로 복잡한 작업이다. 각 테넌트의 데이터는 서로 분리되어야 하며, 동시에 공유 리소스의 효율적 사용을 보장해야 한다. 데이터 격리는 스키마 기반 데이터 분리, 물리적 격리(개별 데이터베이스), 그리고 논리적 격리(공유 데이터베이스 내에서의 분리)까지 다양한 접근법이 있다.

2.3.1. 스키마 기반 데이터 분리

각 테넌트에 대해 데이터베이스 내에서 별도의 스키마를 할당하는 방식으로 각 테넌트의 데이터를 논리적으로 분리하면서도 하나의 데이터베이스 서버를 사용할 수 있어 효율적이다. 반면에 스키마 수가 많아질수록 관리가 복잡해질 수 있으며, 대규모 데이터베이스에서 성능 저하가 발생할 수 있는 단점이 있다[1][2].

2.3.2. 테넌트 ID 기반 데이터 분리

모든 데이터 레코드에 테넌트 ID를 추가하여 데이터를 구분하는 방식으로 간단하게 구현할 수 있으며, 스키마 기반 분리보다 관리가 용이한 장점이 있는 반면에 부적절한 쿼리 설계는 데이터 누출 위험을 증가시킬 수 있는 단점이 있다[2].

2.3.3. 물리적 데이터 분리

각 테넌트에 별도의 데이터베이스 서버 또는 인스턴스를 제공하는 방식으로 가장 높은 수준의 보안과 격리를 제공하지만 비용이 많이 들고, 리소스 활용도가 낮은 단점이 있다[3].

2.3.4. 컨테이너 및 가상화 기반 격리

각 테넌트를 별도의 컨테이너나 가상 머신에서 실행한 방식으로 강력한 격리를 제공하며, 각 테넌트의 환경을 독립적으로 관리할 수 있는 반면에 리소스 소비가 높을 수 있으며, 오버헤드 관리가 필요하다는 단점이 있다[4].

2.3.5. 암호화 기반 데이터 분리

각 테넌트의 데이터를 암호화하여 저장하고, 키 관리를 통해 접근을 제어하는 방식으로 데이터 보안성이 매우 높아진다. 특히 민감한 데이터에 적합한 방법인 반면에 암호화 및 복호화 과정이 성능에 영향을 줄 수 있으며, 키 관리가 중요한 단점이 있다.

2.3.6. 멀티테넌시 컨트롤 플레인

중앙집중식 관리 시스템을 사용해 각 테넌트의 데이터 접근 및 격리 정책을 제어하는 방식으로 일관된 데이터 접근 정책을 적용하고, 전체 시스템의 데이터 흐름을 효율적으로 관리할 수 있는 반면에 시스템의 복잡성이 증가하고, 중앙집중식 시스템에 대한 의존도가 높은 단점이 있다[4].

표 1 데이터 격리 방법 및 특징

데이터격리방법	특 징	장 점	단 점
스키마 기반 데이터 분리	데이터베이스 내에서 각 테넌트별 별도의 스키마 할당	하나의 DB 서버 사용, 효율적	스키마 수 증가 시 관리 복잡, 대규모 DB에서 성능 저하 가능
테넌트 ID 기반 데이터 분리	모든 데이터 레코드에 테넌트 ID 추가	간단한 구현, 관리 용이	부적절한 쿼리 설계 시 데이터 누출 위험 증가
물리적 데이터 분리	각 테넌트별 별도의 DB 서버/인스턴스 제공	높은 보안과 격리 수준	높은 비용, 낮은 리소스 활용도
컨테이너/가상화 기반 격리	각 테넌트를 별도의 컨테이너/가상 머신에서 실행	강력한 격리, 독립적 환경 관리	높은 리소스 소비, 오버헤드 관리 필요
암호화 기반 데이터 분리	각 테넌트 데이터를 암호화하여 저장, 키 관리로 접근 제어	높은 데이터 보안성, 민감한 데이터에 적합	암호화/복호화 과정이 성능에 영향, 키 관리 중요
멀티테넌시 컨트롤 플레인	중앙집중식 관리 시스템으로 데이터 접근 및 격리 정책 제어	일관된 데이터 접근 정책, 효율적 데이터 흐름 관리	시스템 복잡성 증가, 중앙집중식 시스템 의존도 높음

2.4 멀티테넌트 기반 데이터 격리 방법의 문제점

2.4.1 관리 복잡성

각 테넌트에 대해 별도의 스키마를 유지해야 하므로, 테넌트 수가 증가함에 따라 데이터베이스 관리가 복잡해질 수 있고, 데이터베이스 내에서 모든 데이터를 구분하기 위해 테넌트 ID를 사용하는 경우, 쿼리 설계와 실행이 복잡해질 수 있다.

2.4.2. 확장성 제한

데이터베이스와 서버 자원에 대한 부담이 증가하면서, 시스템의 확장성에 영향을 미칠 수 있다. 특히 물리적 격리 방식에서는 각 테넌트별로 별도의 인프라가 필요하므로 비용과 복잡성이 증가한다.

2.4.3 데이터 통합과 분석의 어려움

격리된 데이터는 전체적인 통합 분석을 어렵게 만들 수 있습니다. 이는 비즈니스 인텔리전스나 데이터 분석 작업에 제약을 줄 수 있다. 테넌트 간 데이터를 집계하거나 분석하는 복잡한 쿼리가 필요할 수 있으며, 이는 시스템의 성능에 영향을 미칠 수 있다.

2.4.4. 성능 저하

특히 스키마 기반 격리 방식에서는 데이터베이스의 오버헤드가 증가할 수 있으며, 이는 전체 시스템의 성능 저하로 이어질 수 있고, 물리적 격리 방식에서는 리소스가 과도하게 분산될 수 있으며, 이는 효율적인 리소스 활용을 방해할 수 있다.

2.4.5. 비용 증가

물리적 격리는 각 테넌트마다 별도의 인프라가 필요하기 때문에 높은 비용을 유발할 수 있고, 데이터 격리와 관련된 추가적인 관리 작업은 운영비용을 증가시킬 수 있다.

2.4.6. 유연성 감소

각 테넌트의 개별적인 요구사항에 맞춤 설정을 제공하는 것이 어려울 수 있다. 특히, 표준화된 데이터 격리 방식에서는 각 테넌트의 독특한 요구를 수용하기 어렵다.

3. 멀티테넌시 환경에서 안전한 웹사이트 개발을 위한 데이터 격리 방법 분석

3.1. 멀티테넌시 환경의 데이터 격리 방법에 대한 문제 해결책

3.1.1. 자동화 및 관리 도구 사용

데이터베이스 관리와 관련된 일상적인 작업을 자동화하는 도구를 사하는 것이다. 즉, 스키마 변경, 백업, 모니터링 등을 자동화하여 관리 복잡성을 줄일 수 있다. 모든 스키마의 성능과 상태를 모니터링할 수 있는 중앙 집중식 관리 대시보드를 사용한다.

3.1.2. 모듈화 및 표준화

재사용 가능한 데이터 모델과 구성 요소를 개발하여 관리와 확장을 용이하게 하고, 스키마 관리와 관련된 표준 운영 절차를 개발하고 이를 문서화하여 일관성을 보장한다.

3.1.3. 데이터 통합 및 분석 도구

다양한 스키마의 데이터를 통합하고 분석할 수 있는 플랫폼과 도구를 사용하고, 비즈니스 인텔리전스(BI) 도구 또는 데이터 웨어하우스 솔루션을 포함할 수 있으며, 각 스키마에서 데이터를 추출, 변환 및 로드(ETL 프로세스)하는 기능을 제공한다.

3.1.4. 성능 최적화 전략

자주 접근하는 데이터에 대한 캐싱을 구현하여 성능을 향상시키고, 데이터베이스와 서버의 리소스 할당을 지속적으로 모니터링하고 최적화하여, 과부하 상황을 예방하고 전체 시스템의 성능을 개선한다.

3.1.5. 유연한 아키텍처

가능하다면 마이크로서비스 기반의 아키텍처로 전환하여 각 서비스의 데이터를 더 효율적으로 관리하고, 서비스 간의 결합도를 낮추고, 각 서비스가 독립적으로 확장될 수 있게 하여, 전체 시스템의 확장성을 향상시킨다.

3.1.6. 지속적인 모니터링 및 개선

정기적인 시스템 모니터링을 통해 성능 저하의 원인을 파악하고, 필요한 조치를 취한다. 그리고 사용자와 개발자의 피드백을 수집하고 분석하여, 시스템을 지속적으로 개선한다.

3.2 데이터 격리 실증 사례 분석

멀티테넌시 환경에서 데이터 분리를 효과적으로 구현한 몇 가지 사례를 분석하였다. 이 사례들은 다양한 산업 분야에서의 멀티테넌트 아키텍처 적

용을 보여주며, 각각의 접근 방식은 해당 환경과 요구 사항에 따라 다를 수 있다.

3.2.1 Salesforce

CRM (고객 관계 관리) 분야에 주로 활용되고 있는 방식으로 멀티테넌트 아키텍처의 선구자 중 하나이다. Salesforce는 각 테넌트에 대해 고유한 식별자를 사용하여 데이터를 분리하고, 이를 통해 모든 테넌트의 데이터를 단일 데이터베이스 인스턴스에 안전하게 저장하며 관리한다. 이 방식은 높은 효율성과 확장성을 제공하면서도 강력한 데이터 보안을 유지한다.

장점으로는 고유한 식별자를 사용한 데이터 격리는 데이터를 중앙집중화하여 관리 효율성을 높였고, 대규모 사용자 기반을 지원할 수 있는 뛰어난 확장성을 제공하며, 각 테넌트의 데이터를 안전하게 격리하여 보안과 프라이버시를 강화하였다. 단점으로는 대규모 데이터와 다수의 테넌트를 관리하는 것은 복잡할 수 있다. 그리고 표준화된 플랫폼은 일부 사용자에게 맞춤형 요구 사항을 충족시키는 데 한계가 있을 수 있다.

3.2.2. AWS 멀티테넌트 서비스

클라우드 컴퓨팅 서비스 환경에서 데이터 분리 방식으로 Amazon Web Services(AWS)는 여러 멀티테넌트 서비스를 제공하며, 이들 서비스에서는 논리적 격리 방식을 사용해 테넌트 데이터를 분리한다. 즉, Amazon RDS (관계형 데이터베이스 서비스)는 각각의 데이터베이스 인스턴스를 멀티테넌시 환경 내에서 격리하여 운영한다.

장점으로는 AWS의 견고한 클라우드 인프라는 높은 성능과 안정성을 보장하고, 다양한 서비스와 리소스 옵션이 테넌트의 다양한 요구를 충족시킨다. 단점으로는 리소스 사용량에 따른 비용이 예측하기 어려울 수 있고, 때로는 예상치 못한 비용이 발생할 수 있으며, AWS 서비스의 설정과 관리가 복잡할 수 있다. 특히 클라우드 인프라에 익숙하지 않은 사용자에게는 어려움을 줄 수 있다.

3.2.3. Microsoft Office 365

엔터프라이즈 소프트웨어 및 서비스의 데이터 분리 방식으로 Microsoft Office 365는 멀티테넌트 클라우드 서비스로, 각 기업의 데이터를 별도로 격리하여 관리한다. Office 365는 사용자 데이터를 보호하기 위해 고급 암호화 및 엄격한 접근 제어 메커니즘을 사용한다.

장점은 다양한 업무용 애플리케이션을 하나의 플랫폼에서 제공하고, 클라우드 기반 서비스로 어디서나 데이터에 접근할 수 있는 편리함을 제공한다. 단점은 서버 다운타임이나 기술적 문제가 발생할 경우, 모든 테넌트에 영향을 미칠 수 있으며, 일부 테넌트에 특화된 맞춤형 요구 사항을 충족시키기에는 제한적일 수 있다.

3.2.4. Google Cloud Platform (GCP)

클라우드 컴퓨팅 서비스의 데이터 분리 방식으로 Google Cloud Platform은 다양한 멀티테넌트 서비스를 제공하며, 높은 수준의 보안 및 데이터 격리를 보장한다. GCP는 클라우드 리소스를 여러 테넌트 간에 물리적으로 분리하고, 강력한 네트워크 격리 및 암호화를 통해 데이터 보안을 강화한다.

장점은 머신러닝, 빅데이터 분석 등 최신 기술을 활용한 서비스를 제공하고, 업계 최고 수준의 보안 기능으로 데이터를 보호한다. 단점은 다양한 서비스와 옵션은 사용자에게 복잡하게 느껴질 수 있으며, 사용량 기반 요금제는 예산 관리 및 비용 예측을 어렵게 만들 수 있다.

3.2.5. Shopify

전자상거래 분야에서 사용하는 방식으로 전자상거래 플랫폼으로, 각 온라인 상점을 별도의 테넌트로 취급하여 데이터를 격리한다. Shopify는 각 상점의 데이터를 별도의 스키마에서 관리하며, 이를 통해 상점별 맞춤형 서비스를 제공하면서도 각 테넌트의 데이터 보안과 무결성을 유지한다. 이 접근 방식은 사용자에게 높은 수준의 데이터 격리와 개별화된 사용 경험을 제공한다.

장점은 사용하기 쉬운 인터페이스와 간단한 설정 과정을 제공하며, 다양한 플러그인과 통합 옵션

을 통해 맞춤형 쇼핑 경험을 제공한다. 단점은 표준 플랫폼으로서 일부 고급 기능이나 매우 특화된 요구 사항을 충족시키지 못할 수 있으며, 고급 기능이나 특정 통합 서비스를 사용하기 위해서는 추가 비용이 발생할 수 있다.

표 2 데이터 격리방법 사례 분석

특징/서비스	Salesforce	AWS 멀티테넌트 서비스	Microsoft Office 365	Google Cloud Platform (GCP)	Shopify
산업분야	고객 관계 관리 (CRM)	클라우드 컴퓨팅 서비스	엔터프라이즈 소프트웨어 및 서비스	클라우드 컴퓨팅 서비스	전자상거래
주요기능	고객 데이터 관리, 영업 자동화	컴퓨팅, 스토리지, 데이터베이스 서비스 등	문서 작성, 이메일, 협업 도구	컴퓨팅, 빅데이터, 머신러닝 서비스 등	온라인 상점 구축 및 관리
데이터 격리 방식	스키마 기반 데이터 격리	논리적/물리적 격리	데이터 격리 및 보안 정책	물리적 및 논리적 격리	데이터베이스 및 애플리케이션격리
보안	강력한 데이터 보안 및 프라이버시 관리	고급 보안 기능 및 서비스	엔터프라이즈 급 보안 및 규정 준수	엄격한 보안 및 프라이버시 보호	안전한 결제 처리 및 고객 데이터보호
확장성	높은 확장성, 대규모 사용자 및 데이터 관리 가능	매우 높은 확장성, 다양한 서비스와 리소스 제공	사용자 수에 따른 확장 가능	대규모 인프라 및 서비스 확장성	다양한 규모의 상점에 적합, 확장 용이
사용성	직관적인 사용자 인터페이스	다양한 서비스에 대한 전문 지식 필요	사용자 친화적인 인터페이스	복잡한 서비스 구성이 필요할 수 있음	사용하기 쉬운 플랫폼, 빠른 설정
특화기능	CRM 및 영업 자동화에 특화	광범위한 클라우드 서비스 제공	업무 협업 및 커뮤니케이션에 특화	데이터 분석, 머신러닝에 강점	온라인 상점 관리 및 마케팅 도구 제공
규모 및 가용성	글로벌 시장에서 널리 사용됨	전 세계적으로 광범위한 인프라 및 서비스 제공	전 세계적으로 높은 접근성 및 가용성	글로벌 데이터 센터와 네트워크	전 세계적으로 이용 가능한 전자상거래 플랫폼

이 사례에서 공통점 및 핵심 요소로 데이터 격리와 보안관점에서 이 사례들은 모두 데이터 격리와 보안을 강화하는 데 중점을 두고 있다. 모두 각기 다른 방법으로 데이터 격리를 구현하지만, 그 핵심 목적은 동일하다. 멀티테넌트 아키텍처를 통해 이들 서비스는 효율적인 리소스 관리와 규모의 경제를 실현하고 있다. 멀티테넌시 환경에서 각 테넌트의 고유한 요구 사항을 충족시키기 위한 유연성과 커스터마이제이션 능력도 중요한 요소이다. 마지막으로 개인정보 보호와 관련된 법적 요구 사항을 충족시키는 것은 멀티테넌트 서비스에 있어 필수적이다. 이러한 사례들은 멀티테넌시 환경에서 데이터 격리를 성공적으로 구현한 예시로, 다양한 산업에서의 멀티테넌트 서비스 제공에 있어 중요한 참고점을 제공하고 있다.

4. 분석 결과 및 시사점

4.1 분석결과

멀티테넌트 기반 데이터 분리 사례를 분석한 결과, 몇 가지 주요한 시사점을 도출할 수 있었다. 이러한 분석은 다른 기업이나 조직이 멀티테넌시 환경을 구축하고 관리할 때 유용한 가이드라인을 제공할 것이다.

Salesforce, AWS, GCP 등의 사례에서 볼 수 있듯, 멀티테넌시 환경에서 강력한 데이터 보안과 프라이버시 보호는 필수적이다. 이들은 각기 다른 방법으로 데이터를 격리하고 보호함으로써 사용자 데이터의 안전성을 보장한다.

AWS와 GCP는 클라우드 기반 서비스를 통해 높은 확장성과 유연성을 제공한다. 이를 통해 사용자는 자신의 비즈니스 요구에 맞춰 서비스를 확장하거나 조정할 수 있다.

그리고 Shopify와 Microsoft Office 365는 사용자 친화적인 인터페이스와 맞춤형 옵션을 제공하

여 사용자 경험을 강화한다. 이를 통해 각 사용자 또는 테넌트가 개별적인 요구사항을 충족할 수 있게 된다.

멀티테넌시 환경은 데이터 관리와 시스템 운영의 복잡성을 증가시킨다. Salesforce의 경우, 스키마 기반 데이터 격리는 관리 복잡성을 낳지만, 이를 효과적인 도구와 자동화를 통해 관리할 수 있다.

4.2 시사점

모든 멀티테넌시 환경에서 데이터 보안과 프라이버시는 최우선 고려사항이다. 각 테넌트의 데이터를 안전하게 격리하고 보호하는 메커니즘의 구현이 필수적이다. 비즈니스의 성장과 변화하는 요구사항에 대응하기 위해, 시스템은 확장 가능하고 유연해야 한다. 이를 기반으로 클라우드 서비스는 이러한 요구를 충족시키는 효과적인 방법을 제공한다.

최종 사용자에게 우수한 경험을 제공하기 위해 인터페이스의 사용 용이성과 개인화 옵션을 고려해야 한다. 사용자의 특정 요구사항을 만족시키는 커스터마이제이션 기능은 서비스의 경쟁력을 높일 수 있다.

데이터 격리 방법 선택 시 보안 수준과 비용의 균형을 고려해야 한다. 높은 보안이 필요한 경우 물리적 격리나 암호화가 적합할 수 있으나, 비용과 자원 효율성도 중요한 고려사항이다.

데이터 격리 방식은 시스템의 성능에 영향을 미칠 수 있으므로 성능 저하 없이 데이터 보안을 유지하는 방안을 고려해야 한다. 그리고 멀티테넌시 환경이 확장됨에 따라 데이터 격리 방법도 이에 맞게 조정되어야 한다. 확장성이 높은 방법을 선택하는 것이 중요하다.

데이터 보호 규정 준수도 중요한 요소이다. GDPR(General Data Protection Regulation), HIPAA(Health Insurance Portability and Accountability Act) 등의 규정에 맞춰 데이터를 안전하게 관리하고 보호할 수 있는 방법을 선택해야 한다. 멀티테넌시 환경에서의 데이터 분리 방안은 각 조직의 특정 요구사항, 기술적 능력, 보안 요구, 비용 예산 및 운영 효율성에 맞춰 신중하게 선택되어야 한다. 선택된 데이터 격리 방식은 웹 사이트의 성능, 보안, 확장성 및 유지관리 측면에 큰 영향을 미칠 수 있으므로, 이러한 요소들을 충분히 고려하여 최적의 방안을 결정하는 것이 중요하다.

5. 결론

멀티테넌시 환경에서 안전한 웹사이트를 개발하기 위한 데이터 격리 방법을 분석한 결과, 데이터 격리는 이러한 환경에서 중요한 보안 과제임이 명확해졌다. 각 테넌트의 데이터 보안과 프라이버시를 보장하고, 데이터 누출 및 교차 접근을 방지하는 데 필수적인 역할을 하고 있음을 알 수 있다.

스키마 기반 격리, 논리적 격리, 물리적 격리 등 다양한 데이터 격리 방법이 존재하며, 각각은 고유한 장단점을 가지고 있고, 이러한 방법들 중에서 적합한 방법을 선택하는 것은 특정 환경의 요구사항, 보안 수준, 비용, 그리고 운영의 편의성을 고려하여 결정되어야 한다. 즉, 높은 보안이 필요한 환경에서는 물리적 격리가 적합할 수 있지만, 비용과 유연성을 고려한다면 논리적 격리나 스키마 기반 격리가 더 효과적일 수 있다.

데이터 격리 방법은 보안 강화와 시스템 성능 간의 균형을 맞추는 데 중요하다. 효율적인 데이터 관리와 시스템의 빠른 응답성을 유지하면서 필요한 보안 수준을 확보하는 것이 중요하다. 또한, 데이터 격리 전략은 시간이 지남에 따라 변화하는 보안 요구사항과 기술 발전에 맞춰 지속적으로 관리되고 개선되어야 한다. 정기적인 보안 평가, 취약점 분석, 그리고 최신 보안 위협에 대응하기 위한 업데이트가 필수적이다. 더불어, 멀티테넌시 환경에서 데이터 보호 및 프라이버시 관련 법률과 규정의 준수도 매우 중요하다. GDPR, HIPAA 등의 규정에 따라 데이터 처리 및 보호 조치를 적절히 수행하는 것이 필요하다.

종합적으로, 데이터 격리는 멀티테넌시 환경에서의 보안을 강화하는 한 방법에 불과하다. 따라서, 데이터 격리와 함께 암호화, 접근 제어, 감사

로깅 등의 다른 보안 조치들도 통합적으로 고려되어야 한다. 이러한 포괄적인 보안 접근 방식은 멀티테넌시 환경에서의 안전한 웹사이트 개발 및 운영에 있어 필수적인 요소로 작용하며, 데이터 관리 및 보안 전략 수립에 있어 중요한 기준을 제공한다.

참 고 문 헌

[1] “Search for specific papers or topics related to multi-tenant architecture and data isolation”. IEEE Xplore Digital Library, Retrieved from https://ieeexplore.ieee.org/, 2021.

[2] “AWS Whitepapers”, Retrieved from https://aws.amazon.com/whitepapers/, 2020.

[3] “Google Cloud Architecture Center”, Retrieved from https://cloud.google.com/architecture, 2021

[4] “Microsoft Azure Documentation”, Retrieved from https://docs.microsoft.com/en-us/azure/, 2022

[5] “Cloud Security Alliance. Cloud Security Alliance Resources”. Retrieved from https://cloudsecurityalliance.org/, 2020.

[6] “Search for specific papers or topics related to multi-tenant architecture and data isolation”, ACM Digital Library. Retrieved from https://dl.acm.org/, 2021.

[7] “Search for specific papers or topics related to multi-tenant architecture and data isolation”, Retrieved from https://link.springer.com/, Springer, 2021.

[8] “Search for specific papers or topics related to multi-tenant architecture and data isolation”. Retrieved from https://www.elsevier.com/, Elsevier. 2021.

[10] Gartner, Now is the time for security at Application Level, 2020.

[11] 행정안전부, 소프트웨어 개발 보안 가이드, 2021.

[12] 박상노, 클라우드 컴퓨팅 서비스의 보안 전략 방안에 관한 연구, 배재대학교 대학원, 2013.

[13] 김점구 외1, 네트워크 보안 이벤트 감사를 위한 연관 규칙 알고리즘 개발, 융합보안논문지, 2021.

[14] SaaS 플랫폼 기술 및 개발 동향, ETRI, 전자통신동향분석 제26권 제5호, 2011.

[15] OWASP Top 10. Retrieved from https://owasp.org/www-project-top-ten/ 2021.

[16] KISA, 웹서버구축 보안점검 안내서, 2022.

[17] 행정안전부, 웹 응용프로그램 개발 보안가이드, 2022.

〔저자소개〕

김 점 구 (Jeom Goo Kim)

1990년 2월 광운대학교 전자계산학과 이학사

1997년 8월 광운대학교 전자계산학과 석사

2000년 8월 한남대학교 컴퓨터공학 박사

1999년 3월~ 현재 남서울대학교 컴퓨터소프트웨어학과 교수

email : jgoo@nsu.ac.kr