

마이데이터 API G/W 설계 연구

독고세준¹, 최창원^{2*}

¹(주)비디 대표, ²한신대학교 컴퓨터공학부 교수

A Study On the Design of MyData API G/W

Sehjoon Dokko¹, Changwon Choi^{2*}

¹CEO, BD Inc., ²Professor, Division of Computer Engineering Hanshin University, **BD

요약 마이데이터 서비스를 이용하여 정보 주체인 개인이 본인의 정보를 적극적으로 관리 및 통제하여 이를 신용관리, 자산 관리 등에 능동적으로 활용할 수 있다. 마이데이터는 기업과 기관 중심의 개인 데이터 생태계를 데이터의 주인인 개인에게 자신의 데이터를 통제하고 관리하여 활용할 수 있는 권한을 부여하는 것이다. 마이데이터 서비스를 성공적으로 제공하기 위해서는 다양한 기관에서 제공되는 서로 다른 형식의 데이터를 표준 규격 형태로 변환하기 위한 API G/W의 개발이 필수적인 요소이다.

본 논문에서는 마이데이터 서비스의 API G/W 개발을 위해 검증(Validation) 기능, 관리(Throttling) 기능, 인증 및 권한(Authentication & Authorization) 기능, 중재(Mediation) 기능으로 주요 기능들을 도출하고 각 세부 기능별로 해당 서비스를 설계하였다. 설계된 API G/W의 기능들을 통해 다양한 형식의 요구들을 서비스할 수 있는 마이데이터 서비스를 안전하고 효율적으로 지원할 수 있었다.

주제어 : 마이데이터, API 게이트웨이, API 서비스

Abstract The MyData service makes anyone possible to apply the personal information for the personal credit management or the financial management by proactive managing his/her own information. The MyData means that the anyone is able to control or manage the its own information by changing from the company-oriented or the organization-oriented information to his/her own information. It is mandatory to develop the API G/W which transforms the different user format to the standard format to support the MyData service.

This study is to design the API G/W for the MyData service and the designed API G/W supports the 4 major functions - Validation function, Throttling function, Authentication&Authorization function, Mediation function. The designed API G/W make it possible to support the safely and efficient MyData service by serving the various queries with the different formats.

Key Words : MyData Service, API G/W, API Service

1. 서론

1.1 연구 배경 및 목적

마이데이터란 정보 주체인 개인이 본인의 정보를 적극

적으로 관리 및 통제하여 이를 신용관리, 자산 관리 등에 능동적으로 활용하는 것을 의미한다. 데이터의 주인인 개인이 데이터를 직접 소유하고 통제하는 '자기정보결정권'과 자신의 정보를 필요에 따라 제3자에게 이동 및 활

*교신저자 : 최창원(won@hs.ac.kr)

접수일 2023년 02월 24일

수정일 2023년 3월 24일

심사완료일 2023년 4월 2일

용할 수 있도록 하는 '자기정보이동권'을 핵심으로 한다. 마이데이터를 이용하면 은행, 보험회사, 카드사 등에 산재되어 있는 개인신용정보를 한곳에 모아 확인할 수 있고, 자신이 원하는 업체에 개인 데이터를 제공해 맞춤형 서비스를 추천받을 수 있다. 이러한 과정을 지원하는 산업이 '본인신용정보 관리업'이다. 즉, 개인의 동의를 받은 기업은 정보를 활용해 개인 맞춤 상품, 서비스를 제공하며 수익을 낼 수 있게 되었다[18].

개인의 금융 데이터는 금융기관이, 진료데이터는 의료기관이 갖고 있으나 이러한 개인정보의 주인은 그 데이터를 축적하여 관리하는 기관이나 기업이 아니라 그 개인인 것이다[1]. 마이데이터는 정보 주체인 개인에게 본인 데이터에 대한 자기 결정권을 부여함으로써, 개인이 자신의 데이터를 적극적으로 관리하고 통제하여 이를 다양한 분야에 능동적으로 활용하자는 일련의 과정으로 볼 수 있다. 한국데이터산업진흥원에서는 마이데이터를 정보 주체인 개인을 대상으로 개인 데이터에 대한 접근, 수집, 관리, 공유, 활용을 마이데이터 방식으로 지원하는 서비스라고 설명하고 있으며 정보의 주체인 개인이 본인의 정보를 적극적으로 관리, 통제하고 이를 신용관리, 자산관리, 나아가 건강관리까지 개인 생활에 능동적으로 활용하는 일련의 과정이라고 할 수 있다. 결국 마이데이터는 기업과 기관 중심의 개인 데이터 생태계를 데이터의 주인인 개인에게 자신의 데이터를 통제하고 관리하여 활용할 수 있는 권한을 부여하자는 패러다임으로 볼 수도 있을 것이다[17]. 마이데이터 서비스를 성공적으로 제공하기 위해서는 다양한 기관에서 제공되는 서로 다른 형식의 데이터를 표준 규격 형태로 변환하기 위한 시스템이 필수적이다. 이는 인터넷 환경에서 제공되는 다양한 형식을 처리할 수 있는 API G/W의 개발이 우선적으로 필요하다.

API G/W를 사용하는 주된 이유 중 하나는 여러 백엔드 서비스를 호출하고 결과를 집계할 수 있기 때문이다. 클라이언트는 개별 서비스에 대한 요청을 보내는 대신 API G/W로 보내 거기서 해당 요청을 관련 서비스로 전달할 수 있다. API G/W는 또한 각 클라이언트에 대해서도 다른 API를 제공할 수 있으며, 이는 오늘날 끊임없이 진화하는 환경에서 필요한 기능이다.

본 논문에서는 마이데이터 서비스를 위한 API G/W 개발을 위한 주요 기능들을 Validation(검증) 기능, Throttling(관리) 기능, Authentication & Authorization(인증 및 권한) 기능, Mediation(중재) 기능으로 도출하고 각 세부 기능별로 서비스를 설계하였다.

1.2 API G/W 기능 및 관련 연구

1) 인증

API G/W를 사용하여 API 호출을 인증할 수 있어야 한다. 클라이언트가 여러 서비스의 데이터에 접근할 경우, G/W에서 한 번만 인증하게 설계되면 대기 시간이 줄어들고 애플리케이션 전체에서 인증 프로세스가 일관되게 유지할 수 있다. 이를 위해 API G/W는 많은 공개 표준 중 하나를 사용하여 소비자(예를 들어 OAuth, JWT 토큰, API 키, HTTP 기본/다이제스트, SAML 등)의 ID 또는 유효성을 확인하거나 비표준 수단을 사용하여 메시지의 헤더 또는 페이로드에 자격 증명을 제공할 수 있다.

2) 메트릭 수집

모든 요청이 API G/W를 통과하기 때문에 이것은 데이터 분석을 수집하기에 이상적인 장소이다. 예를 들어 API G/W는 사용자의 요청 수 또는 개별 마이크로서비스에 전달되는 요청 수를 측정할 수 있고 API G/W를 사용하여 요청을 제한할 수도 있다. 사용자가 너무 많은 요청을 보내는 경우 G/W는 요청을 마이크로서비스 중 하나로 전달하는 대신 거부하도록 할 수 있다(Throttle 기능).

3) 입력 유효성 검사

입력 유효성 검사는 모든 클라이언트 요청에 요청을 완료하는 데 필요한 필수 정보가 포함되어 있고 올바른 형식으로 제공되는지 확인하는 API G/W의 필수 기능이다. 의심되는 것으로 보이면 G/W는 요청을 거부할 수 있다. 필요한 모든 정보가 포함된 경우에만 이 G/W는 요청된 정보 검색을 담당하는 마이크로서비스로 요청을 라우팅한다.

4) 응답 전환

응답 전환은 API G/W의 중요한 기능이며 정보의 전달자 역할을 담당한다. 예를 들어 백엔드 서비스가 XML로 응답을 포기하였지만, 요청자가 JSON으로 응답이 필요한 경우 API G/W가 이를 자동으로 처리할 수 있다.

5) API G/W의 이점

- ① 단일 인터페이스 접근 방식을 통해 API 및 백엔드 시스템을 더욱 안전하게 보장

- ② 보안 및 액세스 제어, 조절, 라우팅, 증개 및 SLA 관리를 위한 확장 가능한 정책을 사용하여 API 실행 환경을 완전히 제어
- ③ 서비스와 애플리케이션 사용자 모두를 위한 간단한 코드 작성
- ④ 더 적은 왕복 호출로 인해 시간이 지남에 따라 지연 시간 감소
- ⑤ 모든 마이크로서비스에 더 빠르고 쉽게 접근
- ⑥ 각 개별 마이크로서비스 또는 로드 밸런싱에 대한 워크로드 감소
- ⑦ 포괄적인 메트릭 수집

연구 [1]은 마이데이터 플랫폼이 필수적으로 갖추어야 할 기능들을 정의하고, 그 기능을 구현하기 위한 절차와 방법, 표준 등을 기술하고 제안한 플랫폼 모델을 응용 사례에 적용하여 마이데이터 생태계 활성화를 위한 플랫폼 모델을 제안하였으며 구체적인 마이데이터 서비스 제공을 위한 세부 내용들을 포함되지 않았다.

연구 [3]은 국내외 마이데이터 현황과 장래 발전에 대한 연구를 진행하였으며, 과학기술 연구자들의 연구 정보(Science and Technology Knowledge)를 활용하기 위한 API G/W 설계 연구를 수행하였다. 이 연구들은 과학기술 지식 인프라를 통합하기 위해 다양한 서비스를 API 단위로 정의하고 이를 처리할 수 있는 API G/W를 개발하였다. API G/W는 클라이언트와 end-point 중간에 API G/W가 미들웨어의 역할을 하며 API를 사용자에게 서비스하기 위해 인증, 라우팅, 에러처리 등 기능이 포함되어 있도록 설계하였다[4][6][9].

연구[7]과 연구 [8]은 Open API를 활용한 서비스의 설계를 수행하였으며, 내부 API간의 latency를 감소시키고 성능을 향상시키기 위해 gRPC(Google API) API와 REST API를 외부 API와 연동시키고 내부 API는 gAPI에 연동되도록 제안하였다[15][16]. 연구[19]는 증가하는 IoT 장치들과 사용자들에 대해 불필요한 네트워크 트래픽과 컴퓨팅 자원의 소비를 줄이기 위한 자동 caching API G/W를 제안하고 클라이언트나 서비스 인스턴스 사이의 요청 및 응답을 캐싱하도록 하였다.

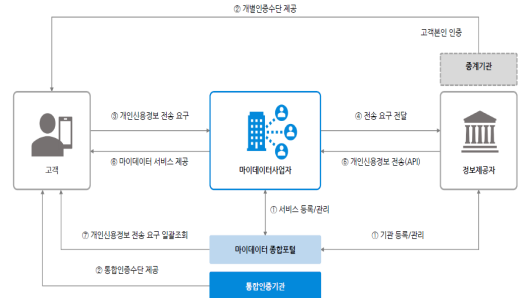
2. 서비스 설계

API G/W는 실제 백엔드 서비스 또는 데이터와 접속하고 API 호출에 대한 정책, 인증 및 일반 액세스 제어를 적용하여 중요한 데이터를 보호하는 트래픽 관리자이다.

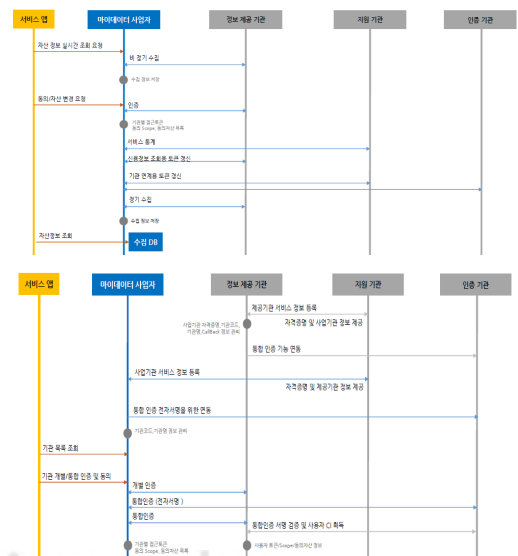
API G/W는 백엔드 시스템 및 서비스에 대한 접근을 제어하는 방법이며 외부 클라이언트와 백엔드 서비스 간의 통신을 최적화하여 클라이언트에게 원활한 경험을 제공하도록 설계되어야 한다.

2.1 마이데이터 서비스 구조

마이데이터 서비스는 개인이 금융상, 관공서, 병원, 빅테크, 통신사 등에 흩어져 있는 자신의 신용 정보를 특정 마이데이터 사업자에게 제공하고, 이를 토대로 맞춤형 자산 관리와 금융 컨설팅 등을 받을 수 있는 서비스이다. 마이데이터 서비스는 신용 정보법을 기반으로 정보 주체가 신용 정보 전송 요구권 수행을 위한 참여자 역할 및 절차에 대해 가이드를 제공했으며 그에 대한 서비스 구성 요소들과 서비스 내용은 [Fig. 1]과 같으며 서비스 구성 요소 간의 서비스 흐름은 [Fig. 2]와 같다.



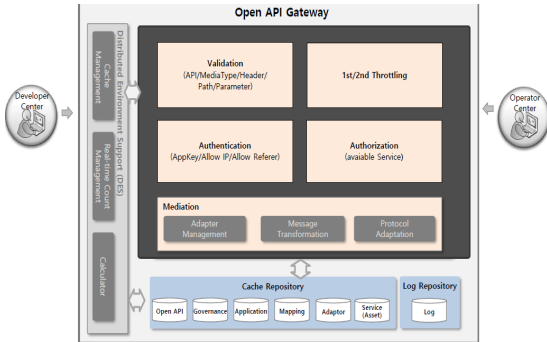
[Fig. 1] The MyData Service Component



[Fig. 2] The MyData Service Process

2.2 마이테이터 API G/W 기능

마이테이터 Open API G/W는 Open API 요청과 응답 및 Validation, Throttling, Authentication & Authorization, Mediation을 연결하는 역할을 담당하며 Operator Center에서 관리되는 API 정보는 DES(Distributed Environment Support)를 통해서 Local Cache Repository로 동기화하여 관리한다.

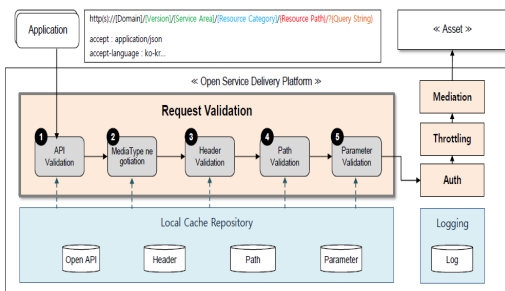


[Fig. 3] Open API G/W Functions

3. 마이테이터 API G/W 세부 설계

3.1 Validation(검증)

마이테이터의 요청 검증 기능은 Open API 호출시 전달받은 정보를 기반으로 API 검증, 미디어 유형 교섭, 헤더 검증, 경로 검증, 파라미터 검증 5 단계로 수행하도록 설계하였다.



[Fig. 4] Request Validation

1) API 검증

주어진 URL과 매칭되는 Open API URL을 검색

2) 미디어 유형 교섭

Accept response 유형에 대한 교섭을 수행

3) 헤더 검증

헤더 내에 필수 요소가 있는지 검증

4) 경로 검증

경로 파라미터의 매칭 여부를 확인

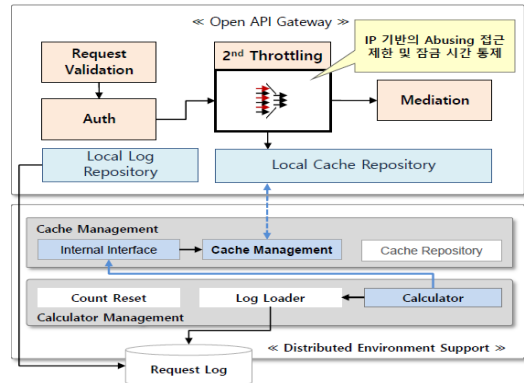
5) 파라미터 검증

Query 내의 파라미터 검증을 수행

3.2 Throttling(부하 제어)

Open API 네트워크의 스위치, 서버의 분산 처리, Cache Repository를 이용한 데이터 관리를 통해 부하 분산 및 제어를 수행한다.

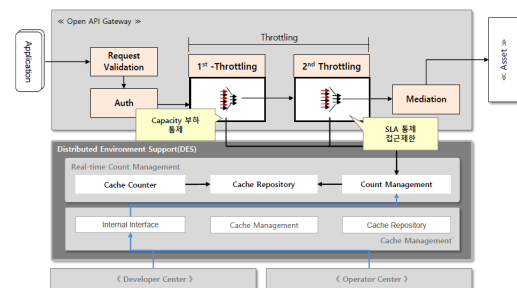
1) L7 스위치 사용 또는 IP 접근 제어



[Fig. 5] IP Access Control

2) WAS 서버

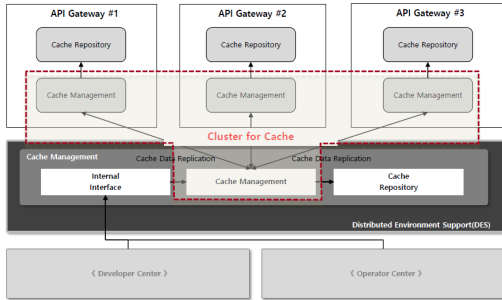
- API 분산 처리
- API G/W 및 Asset의 QoS 보장을 위한 Capacity에 따른 부하 제어
- Application 별 SLA 정책에 따른 부하 제어



[Fig. 6] API Access Control

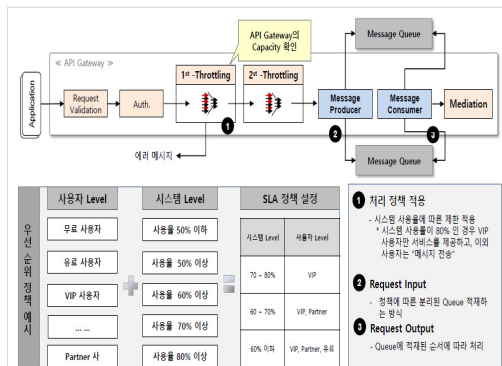
3) Cache

- 서비스, 인증키 등의 정보를 cache
- 실시간 Request Count 연산을 위한 cache
- Asset 부하를 줄이기 위한 응답 데이터 cache
- Abusing IP 처리를 위한 cache



[Fig. 7] Cache Control

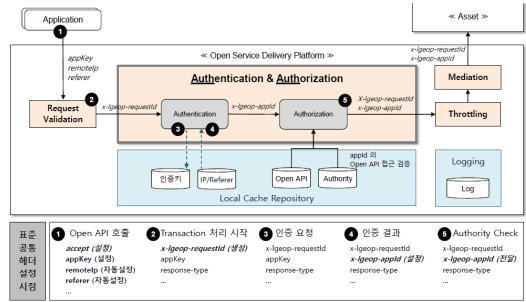
그 외에 Request 처리에 대한 우선 순위를 조정하는 기능을 포함시키고 API G/W의 Capacity가 한계치에 도달할 경우를 대비하여 유료, 무료 API 호출 시 큐를 분리하거나 무료 API 호출은 재시도를 유도하는 방법들을 설계하였다.



[Fig. 8] Request Priority Control

3.3 Authentication & Authorization

개발자 센터에서 발급받은 appKey를 application 호출 시 HTTP header를 이용하여 전달하고 인증 키에 대한 application 인증을 처리한다. Authorization은 전달받은 Application ID를 이용하여 Open API에 대한 접근 권한을 통제하도록 설계하였다.

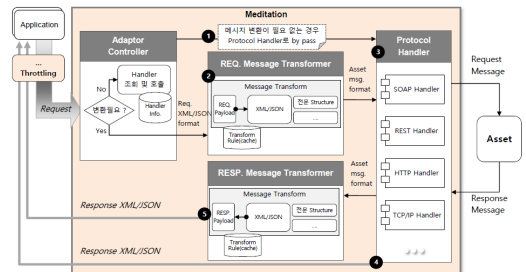


[Fig. 9] Authentication & Authorization

3.4 Mediation

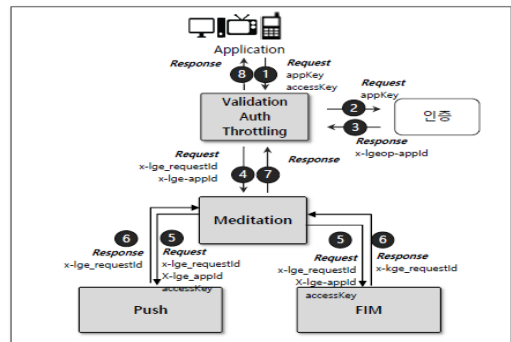
1) 메시지 변환

Open API 호출을 통하여 API G/W로 전달된 서비스 요청을 Asset으로 전달하고 그 결과를 요청한 서비스로 반환하는 Mediation의 처리 과정은 [Fig. 10]과 같이 수행된다.



[Fig. 10] Message Transformation

API G/W의 표준 연동 규격에서 사용하는 공통 헤더의 유형은 <Table 1>과 같으며 [Fig. 11]은 공통 헤더를 처리하는 과정이다.

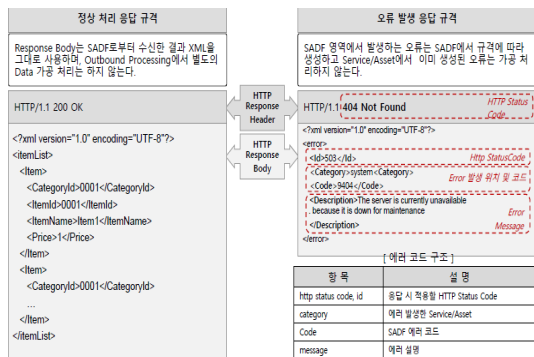


[Fig. 11] Common Header Process Flow

<Table 1> Common Header Types

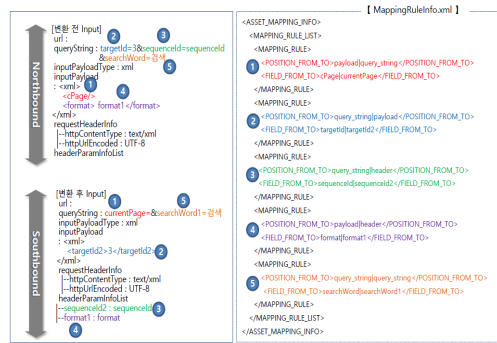
Header	Description
x-lgeop-requestId	Transaction Id for management of replies
x-lgeop-applId	Unique Id for identifying request application
content-length	Message Length(exceptHeader) RFC 2616 ex) 320
content-type	Resource content-type ex)text/xml; charset=utf8
accept	Applicable Media Type ex) application/json
accept-language	Default Language ex) ko-kr
date	Message Request Date/Time ex) Tue, 27 Dec 2011 12:00:00 GMT
host	Server URL ex)api.lgeop.com
remoteIp	ClientIP
referer	HTTP Referer (pre-reference address)
appkey	Key for identifying request application
accessKey	Key for identifying Asset user

API G/W의 표준 응답 규격은 정상 응답과 오류 응답으로 구분할 수 있으며 Asset, Service Asset Adaptation, Service Access & Delivery에서 생성된 응답은 데이터의 가공없이 전달되도록 설계하였다.



[Fig. 12] Standard Response Format

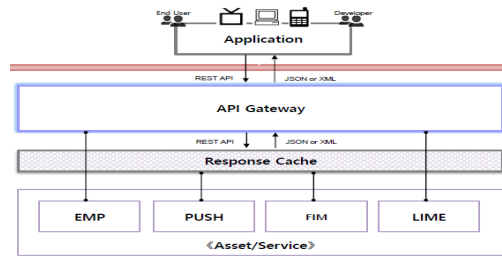
[Fig. 13]은 실제로 메시지가 변환되는 예를 코드를 이용하여 나타내었다.



[Fig. 13] Message Transformation Example

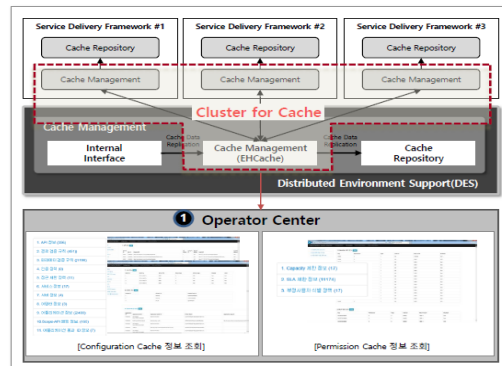
2) Cache 관리

조회성 업무에 대해서는 응답 Cache에 Time Based Cache를 적용하여 API G/W와 Asset 간의 Latency를 줄이도록 하였다.



[Fig. 14] Response Cache

또한 각 서비스에서 제공되는 Cache 데이터가 정상적으로 로딩되어 동작하는지 확인하기 위해 DES 내부 인터페이스를 통해 Operation Center에서 데이터를 모니터링할 수 있는 기능을 제공하도록 설계하였다[Fig. 15].



[Fig. 15] Cache Monitoring

Operation Center에서 cache 데이터를 조회할 수 있는 항목들은 설정 cache 기능과 허가(permission) cache로 나누어 구성된다.

① 설정 cache

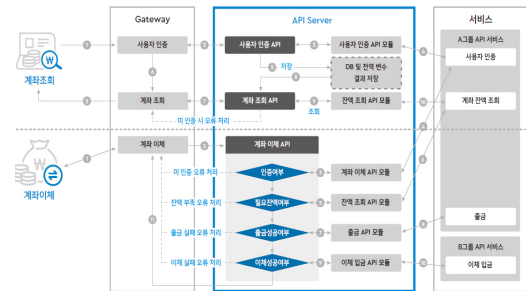
API 정보, 경로 검증 규칙, 파라미터 검증 규칙, 인증 정책, 접근 제한 정책, 서비스 정보, 서버 정보, 어댑터 정보, 어플리케이션 정보, 어플리케이션 통과 ID 정보 등

② 허가 cache

Capacity 제한 정보, SLA 제한 정보, 부정 사용자 식별 정책 등

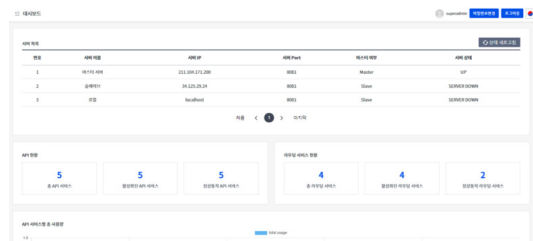
앞에서 기술한 마이데이터 서비스를 위해 설계된 API G/W를 구현하여 실제로 운용되는 서비스에 적용하였다. 운영 결과 사용자들에게 보안성과 편의성을 제공하고 신규 API의 개발이나 기존 API의 개선 기능들도 큰 어려움 없이 적용할 수 있다.

[Fig. 16]은 설계된 API G/W를 적용한 마이데이터 서비스의 처리 과정이다.

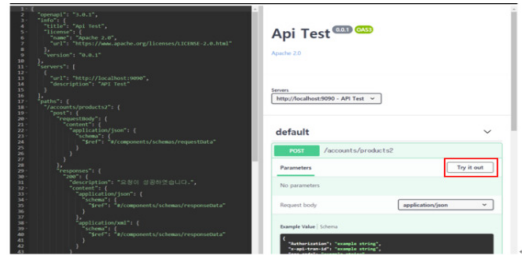


[Fig. 16] MyData Service Flow with API G/W

아울러 마이데이터 서비스 사용자에게 편의성을 제공하기 위해 사용자 인터페이스를 제공하였으며 [Fig. 17]는 전체 서비스를 직관적으로 파악할 수 있는 대시보드 화면이다. [Fig. 18]은 API 테스트를 지원하는 기능이다.



[Fig. 17] MyData Service Dashboard



[Fig. 18] MyData API Test

4. 결론 및 향후 연구

마이데이터 서비스를 이용하여 정보 주체인 개인이 본인의 정보를 적극적으로 관리 및 통제하여 이를 신용관리, 자산 관리 등에 능동적으로 활용할 수 있다. 마이데이터는 기업과 기관 중심의 개인 데이터 생태계를 데이터의 주인인 개인에게 자신의 데이터를 통제하고 관리하여 활용할 수 있는 권한을 부여하는 것이다. 마이데이터 서비스를 성공적으로 제공하기 위해서는 다양한 기관에서 제공되는 서로 다른 형식의 데이터를 표준 규격 형태로 변환하기 위한 API G/W의 개발이 필수적인 요소이다. 본 논문에서는 마이데이터 서비스의 API G/W 개발을 위해 검증(Validation) 기능, 관리(Throttling) 기능, 인증 및 권한(Authentication & Authorization) 기능, 중재(Mediation) 기능으로 주요 기능들을 도출하고 각 세부 기능별로 해당 서비스를 설계하였다. 설계된 API G/W의 기능들을 통해 다양한 형식의 요구들을 서비스할 수 있는 마이데이터 서비스를 안전하고 효율적으로 구축할 수 있다.

다양한 분야에서 마이데이터 서비스가 활용되고 사용자들이 증가할수록 관리 기능이 고도화되어야 하며 개인 정보 보안에 대한 중요성이 더욱 커질수록 인증 및 권한 기능의 강화가 필요해졌다. 따라서 향후 블록체인 등을 활용한 인증 및 권한 기능을 제공하고 대용량의 마이데이터를 처리할 수 있는 관리 기능이 향상된 시스템을 설계할 계획이다.

REFERENCES

[1] S. Lee et. al., "Designing a Platform Model for Building MyData Ecosystem," pp.123-131, Journal of Internet Computing and Services, 2021.4.

[2] Jooseok Park, "A Comparative Study of Big Data, Open Data, and My Data", The journal of Bigdata, Vol.3, No.1, pp.41-46, 2018.

[3] Shim Youn Sook, "Domestic and Foreign Status of Using MyData and Measures for Vitalization", The Journal of the Convergence on Culture Technology, Vol.6, No.4, pp.553-558. 2020.

[4] S. Lee et. al., "API Gateway Design for Sharing Science and Technology Knowledge Infrastructure A Study on the API Gateway for human resources management modules extensions in ERP," Journal of the Korea Society of Computer and Information, Vol.26, No.2, pp.79-88, 2021.

[5] Gorenflo, Christian et al. "FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second." ICBC 2019 - IEEE International Conference on Blockchain and Cryptocurrency. Institute of Electrical and Electronics Engineers Inc., 2019.

[6] S. Lee et. al., "API Gateway Design for Sharing Science and Technology Knowledge Infrastructure," Journal of Digital Contents Society, Vol.22, No.4, pp.719-725, 2021.4.

[7] Hyun, Mi-Hwan. "A Study on the Design of OpenAPI for Common-Using Document Delivery Service," Proceedings of the Korea Contents Association Conference, pp.253-254, 2012.

[8] Hyun, Mi-Hwan. "Design and Implementation of an LinkResolver OpenAPI for Resource Linking Service," Proceedings of the Korea Information Processing Systems Conference, pp.1318-1320, 2012.

[9] Kim, Kwang-Young et. al., "A Study on Knowledge Open Platform for Science and Technology Information Service: With a Focus on Data, Technology Software and Utilization-Case," Journal of Digital Contents Society, Vol.18, No.6, pp.1183-1191, 2017.

[10] Jeon, Dong-cheol et. al., "Design and Implement of Smart Gateway Interface API for Real-time Monitoring in Smart Factory." Journal of Korea Multimedia Society, Vol.2, No.5, pp.601-612, 2019.

[11] IANA, Hypertext Transfer Protocol Status Code Registry, <https://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml>.

[12] BALDINI, Ioana, et al., "Serverless computing: Current trends and open problems. In: Research Advances in Cloud Computing," Springer, Singapore, pp.1-20, 2017.

[13] Scott Hendrickson, et al. "Serverless Computation with OpenLambda", HotCloud'16 Proceedings of the 8th USENIX Conference on Hot Topics in Cloud Computing, pp.33-39, 2016.

[14] L. Li, et, al., "Design Patterns and Extensibility of REST API for Networking Applications," IEEE Transactions on Network and Service Management, Vol.13, No.1, pp.154-167, 2016.

[15] Ji-Woo Kang et. al., "Design of Low Latency API Gateway Architecture For Cloud Service Based on Serverless Computing," Proceeding of IEIE, pp.1542-1544, 2018.

[16] Y. Lee, "Resource Matchmaking for RESTful Web Services," Journal of Korean Institute of Information Technology, Vol. 11, No.8, pp.135-143, 2013.

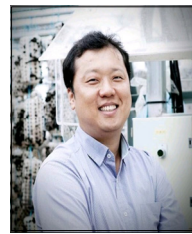
[17] https://www.kdata.or.kr/kr/contents/mydata_01/view.do

[18] <https://www.mhns.co.kr/news/articleView.html>

[19] Sangmin Lee et. al., "Proposed Caching Automation of API Gateway for MSA Optimization in IoT Environment," Proceeding of KSOCI, pp.150-151, 2022.

독고 세준(Dokko, Sehjoon)

[중심회원]



- 고려대학교 전산과학과 석사
- (주)LG전자 핵심망연구소 선임연구원
- (주)인크로스시스템 사업실 이사
- 2013년 ~ 현재 : (주)비디 대표이사

<관심분야>

사물인터넷, 웹 기반 솔루션, 블록체인

최 창 원(Choi, ChangWon)

[중심회원]



- 고려대학교 전산과학과 학사/석사/박사
- 1996년 ~ 현재 : 한신대학교 컴퓨터공학부 교수

<관심분야>

사물인터넷, 유무선 네트워크 및 보안, 시스템 분석