B2B 시스템을 위한 JMS기반 안전한 데이터 교환 모델

이광재° 이경현
부경대학교 전산정보학과
haedongyi°@daum.net, khrhee@pknu.ac.kr

JMS Based Secure Data Exchange Model for B2B System

Kwang Jae Lee° Kyung Hyune Rhee
Dept. of Computer and Information Science, Pukyong National University

요 약

네트워크의 발전과 함께 인터넷을 통한 기업 활동이 점차로 증가하면서 기업들간(B2B)에 실시간 데이터를 안전하게 서비스하기 위하여 여러 개의 시스템이 거미줄처럼 연계되고 있다. 전통적으로 기업들간에는 EDI(Electronic Data Interchange) 시스템과 독자적인 부가가치 통신(VAN, Value-Added Network)을 통한 데이터 교환방식을 사용했으나, 이 모델은 초기비용이 비쌀 뿐만 아니라, 데이터를 실시간 이벤트가 아닌 일괄작업(batch)으로 처리하였다. 그러나, 현재 B2B 간의 데이터 교환 및 상호 작용 방법으로 인터넷, XML, 그리고 메시징 시스템을 사용하고 있으며 특히, 메시징 시스템은 소규모의 시스템이 B2B에 참여하거나 탈퇴하는 비즈니스 작업의 어려움을 덜어준다.

본 논문에서는 인터넷상에서 이루어지는 B2B간의 데이터 교환 및 상호 작용을 위하여 메시징 시스템중 대표적인 JMS를 기반으로 안전한 데이터 교환 모델을 설계 및 구현한다. 따라서, 본 논문에서 제시하는 메시징 모델을 B2B 시스템에 적용하면 기업들간 안전한 메시지 전송을 보장할 수 있다.

1. 서 론

인터넷/웹 비즈니스의 폭발적인 확산으로 인하여 웹은 현재 전자상거래 영역으로 활동분야를 넓혀 가고 있으며 이에 따라 디지털 컨텐츠와 부과 서비스도 늘어나고 있다. 또한, 기업과 고객간(B2C) 전자상거래의 상품 및 서비스 정보, 기업과 기업간(B2B) 전자상거래의 데이터 정보가 서로 분산되어 있지만, 상이한 플랫폼의 비즈니스 시스템을 통합하고 연동해주는 기술의 발달로 인하여 전자상거래는 더욱 더 활발히 늘어나고 있다.[1] 기업이 웹을 기반으로 한 비즈니스로 활동 무대를 옮겨 갈 때, 안전한 데이터 교환을 위해 인터넷/웹 서비스에 대한 보안과 기업간의 데이터 교환에 대한 보안은 필수적인 주요 요소들이다.

따라서, 본 논문에서는 웹 기반의 비즈니스 환경에서 B2B 데이터 교환상의 보안 문제점을 해결하기 위해 자바 메시지 시스템(JAVA MESSAGE SYSTEM)을 이용하여 기업간의 데이터 교환에 있어서 안전한 데이터 교환을 위한 보안 모델을 설계 및 구현한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구 및 기술에 대하여 소개하고, JMS 기반 B2B 시스템에서의 안전한 데이터 교환을 위한 보안 모델을 3장에서 제안한 후 4장에서 결론을 맺는다.

2. 관련 연구

2.1. 메시징 서비스

E-메일이 사람들 사이에서의 의사소통 수단이듯이 메시징은 소프트웨어와 소프트웨어 구성요소 사이에서의 의사소통 수단이다. 즉, 메시징 서비스를 사용하는 이유는 서로 다른 언어로 개발된 두 개의 시스템 사이의 연결(Connection)을 위한 것으로 서로 다른 언어로 개발된 두 개의 시스템은 프로시저 호출을 할 수 없지만, 메시징 서비스를 이용하게 되면 프로시저 호출과 동격인 메시지를 이용할 수 있게 된다. 따라서, 네트워크로 연결된 애플리케이션 컴포넌트사이의 메시징을 가능하게 하기 위해 E-메일에서 서버와 같은 역할을 하는 Message-Oriented Middleware(MOM)을 이용한다. 또한, MOM은 시스템내의 메시지 전송뿐만 아니라 트랜잭션 지원, 최대 허용량, 로드 밸러싱 그리고 메시지를 사용하는 거대한 기업을 위해 확장된 서비스들을 가능하게 해준다.

애플리케이션 컴포넌트사이의 일어나는 메시징 시스템은 점대점 연결 메시징 모델과 발행/구독 메시징 모델의 두 가지 모델이 존재를 한다.[2][5]

2.1.1. 점 대점(Point-to-Point) 방법

점 대점 연결 메시징 모델은 송신자가 보낸 메시지를 MOM의 메시지 큐(Queue)라고 알려진 가상 채널을 통해 동기적 또는 비동기적으로 메시지를 교환 할 수 있다. 또한, 전통적으로 수신자에게 메시지를 자동으로 전달하는 방식에 따라 큐를 통한 풀 기반(pool-base) 모델과 폴링 기반(polling-base) 모델으로 분류된다. 메시지는 수신자가 메시지를 읽어갈 때까지, 유효시간이 경과되기 전에 저장된다. 다수의 수신자가 주어진 하나의 큐를 통하여 메시지를 수신받을 수 있지만 메시지는 오직 한 수신자에게만 허락된다.[3][5]

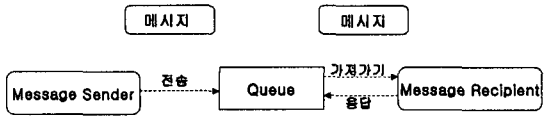

그림 1. 점 대점 연결 메시징 모델

2.1.2. 발행/구독(Publish/Subscribe) 메시징 모델

발행/구독 메시징 모델에서는 메시지 발행자가 토픽(Topic)

이라 불리는 가상채널을 통해 다수의 메시지 구독자에게 메시지를 전달한다. 발행/구독 메시징 모델은 구독자가 새로운 메시지를 받기 위해 토픽에 요청할 수 있으며 토픽에서 메시지를 가져오지 않아도 소비자에게 메시지를 자동적으로 브로드캐스트해 주는 큰 규모의 푸시 기반(push-based) 모델이다.

또한, 선택적으로 JMS 클라이언트는 발행/구독 메시징 모델을 사용하여 지속적 구독을 할 수 있는데, 클라이언트가 접속을 끊은 후 다시 접속한 뒤 끊어진 동안 발행된 메시지를 모아서 받을 수 있기 때문에 발행/구독 메시징 모델에서 메시지를 보내는 발행자는 메시지를 받는 구독자에게 의존하지 않는다.[3][5]

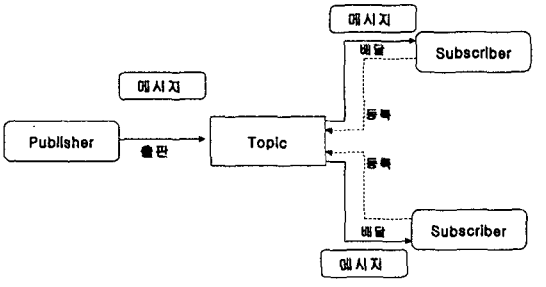

그림 2. 발행/구독 메시징 모델

2.2. JMS에서 제공하는 보안 서비스

2.2.1. 인증(Authentication)

메시징 시스템에 대한 사용자의 신원 확인과 서버의 신원을 JMS 클라이언트에게 확인하는 절차로 JMS에서는 사용자명과 암호를 넣어 JNDI API로 초기화를 만들 때 뿐만 아니라, JMS API로 연결을 생성할 때 명시적으로 인증 서비스가 지원된다.[4]

인증은 사용자 그룹에 할당되어 그룹과 개별 사용자는 어떤 토픽, 큐, 연결 팩토리를 사용 할 수 있는지를 승인을 받으며 승인(permission)은 지정된 특정 구성원을 제외한 그룹의 모든 구성원을 승인하도록 구성될 수 있고, 특정 구성원을 제외한 그룹의 구성원을 거부하도록 구성 될 수도 있다. 일부 JMS는 전달되는 모든 메시지의 접근 제어를 검사하도록 선택될 수도 있고, 단순히 JMS가 JNDI 이름 공간의 통해 얻는 연결 팩토리나 목적지만 제어 할 수도 있다.

2.2.2. 권한 부여(Authorization)

권한부여는 사용자가 시스템에서 무엇을 할 수 있고, 할 수 없는지를 규정하는 보안 정책을 적용하는 것으로써 주로 시스템 관리자가 접근제어 리스트로 설정한다. 권한부여 정책은 중앙에서 관리 할 수 있기 때문에 중앙 집중형 메시징 시스템에 더욱 적합하다.[4][7]

3. B2B 시스템을 위한 JMS 기반 안전한 데이터 교환 모델

본 장에서는 제조 회사와 자재 공급 회사를 모델로 한 B2B 시스템을 위한 JMS기반 안전한 데이터 교환 모델을 제안한다.

3.1. 용어 정리

본 논문에서는 아래와 같은 용어를 사용한다.

- $P1$: 제조 회사
- $P2$: 자재 공급 회사
- MOM : $P1$ 과 $P2$ 간의 데이터를 중계하는 미들웨어
- $M1$: 제조 업체의 입찰 공고 메시지
- $M2$: 자재 공급 업체의 제시 가격
- K : 메시지 암호화를 위한 대칭키
- $E_K(M)$: 메시지 M 에 대칭키 K 를 통한 암호화
- $D_K(M)$: 메시지 M 에 대치킹 K 를 통한 복호화

3.2. 시스템 모델

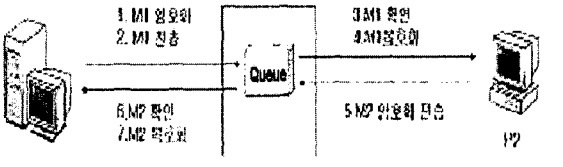

그림 3. 시스템 모델

그림 3.은 본 논문에서 제안하는 JMS 기반의 안전한 데이터 교환 모델의 전체적인 구조를 보여주고 있다. 제안 모델은 제조 회사, 자재 공급 회사, 그리고 기업간의 데이터를 중계하는 미들웨어로 구성된다.

제안 모델에서의 데이터 교환 절차는 다음과 같다. 제조 회사는 메시지를 전달하기 위해 MOM 의 큐에 대한 연결을 시도하여 연결 세션 객체를 생성하고 실제 전달할 메시지와 메시지 암호화를 위한 대칭키 K 를 생성한다. 그리고, 대칭키 K 를 사용하여 메시지에 대한 암호화를 수행한 후 전달 받는 자재 공급 회사의 공개키를 이용하여 대칭키 K 에 대한 암호화를 수행한 후 메시지에 대한 암호문 $E_K(M1)$ 와 암호화된 대칭키를 자재 공급 회사에게 전송한다. 메시지를 전송받은 자재 공급 회사는 자신의 비밀키를 사용하여 대칭키 K 을 획득한 후 대칭키 K 를 사용하여 $E_K(M1)$ 을 복호화하여 메시지를 획득한다. 마찬가지로, 제조 회사에 대한 자재 공급 회사의 메시지 전송은 위의 절차와 동일하게 구현된다.

3.3. 데이터 교환 단계

3.3.1. 초기화 단계

제조 회사와 공급 회사는 메시지를 주고받기 위한 목적지(Destinations)를 생성하며 서로에 대한 공개키를 교환한다. 이 때, 가상 채널인 목적지를 찾는 작업은 JNDI(JAVA NAMING AND DIRECTORY INTERFACE)를 이용하여 구현된다.

3.3.2. 메시지 전송 단계($P1 \Rightarrow MOM$)

제조 회사는 MOM의 큐를 통해 입찰 공고 데이터를 자재 공급 업체에 전송하기 위하여 커넥션(Connection), 세션

(Session), 메시지 생산자(Message producer), 메시지 객체를 이용한다. 제조 회사는 전달할 메시지(M1)를 작성 후 대칭키를 사용하여 메시지를 암호화한 후 대칭키는 공급 회사의 공개키를 사용하여 암호화한다. 그리고, 암호화된 메시지 $E_K(M1)$ 과 암호화된 대칭키를 함께 MOM에게 전달한다.

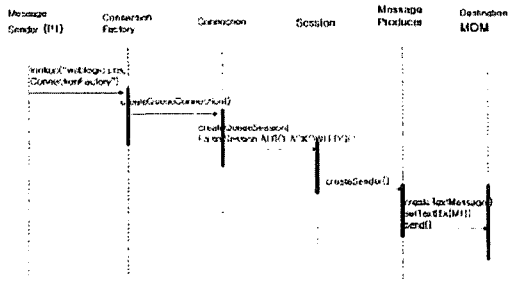

그림 4 메시지 전송 단계($P1 \Rightarrow MOM$)

3.3.3. 메시지 수신 단계($MOM \Rightarrow P1$)

공급 회사는 MOM의 큐를 통해 데이터를 전송받은 후 자신의 개인키로 대칭키 K 를 복호화한 후 암호화된 메시지 $E_K(M1)$ 을 복호화한다. $P2$ 에서 $P1$ 으로의 메시지 교환 또한 위와 같은 방식으로 이루어진다.

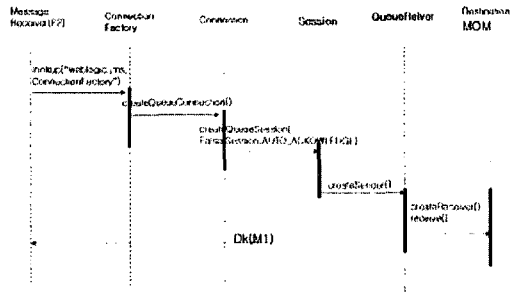

그림 5. 메시지 수신 단계($MOM \Rightarrow P1$)

3.3.4. 구현 예

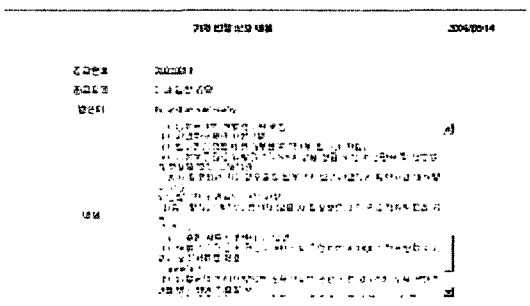

그림 6. 메시지 전송 화면

그림 6.과 그림 7.은 제안 모델에 대한 구현 화면과 제안 모델에서 사용하는 메시지 암호화를 보여주고 있다.

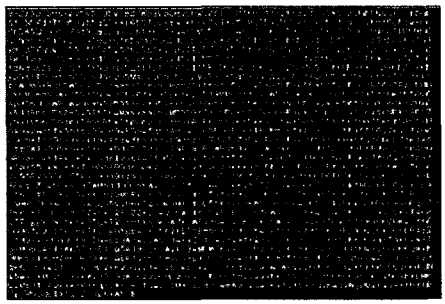

그림 7. 암호화된 메시지

4. 결 론

기업간에 전자 거래가 활발해 짐에 따라 서로 다른 환경의 응용 프로그램간의 데이터 교환이 많이 발생이 되고 있다. 그러나, 전통적으로 기업체간에는 EDI(Electronic Data Interchange) 시스템을 통해 데이터를 교환해왔다. 그러므로, 이러한 모델은 초기비용이 비쌀 뿐만 아니라, 데이터를 실시간 이벤트가 아닌 일괄작업(batch)으로 처리하였다.

따라서, 본 논문에서는 기업간의 전자 거래시 데이터 교환이 쉽게 이루어 질수 있도록 JMS를 이용한 데이터 교환 시스템을 설계함과 동시에 데이터 교환에서 중요한 문제인 보안를 해결하기 위한 시스템을 설계 및 구현을 하였다. 그러므로, 본 논문에서 제안하는 메시징 모델을 B2B 시스템에 적용하면 기업들간 안전한 메시지 전송을 보장할 수 있을 것으로 기대된다.

5. 참고문헌

[1] 이상복, 김창수, 김진수, 정회경 "B2B 기반의 통합형 E-Catalog Registry 시스템 설계 및 구현" 한국정보처리학회 논문지 D 2003

[2] 김성박 "알기 쉽게 풀어 쓴 웹로직과 EJB" 한빛 미디어 2004

[3] 박천구, 문창수 "EJB & WebLogic" 가메 출판사 2002

[4] 리차드 몬스 해펠, 데이브드"Java Message Service (자바 메시지 서비스)" 한빛 미디어 2001

[5] IBM JMS(Java Message Service) "http://www-903.ibm.com/developerworks/kr/java/library/j-jmsvendor.html"

[6] 정헌, 박해우, 강병욱 "JMS를 이용한 XML 문서교환 RPC 모델 구현방법에 관한 연구" 2003

[7] WebLogic EJB Homepage "http://www.weblogic.co.kr/"