생체인증의 에너지 효율을 위한 클라우드 기반의 통합인증 시스템†

송충건*, 최희석*, 강지훈*, 정광식**, 유헌창*
고려대학교 대학원 컴퓨터학과*, 한국방송통신대학교 컴퓨터학과**
{security0730, hsrangken, k2j23h, yuhc}@korea.ac.kr, Kchung0825@knou.ac.kr

Cloud-Based Consolidation Authentication System for Energy-Aware Biometric

ChungGeon Song*, Heeseok Choi*, Jihun Kang*, Kwangsik Chung**, Heonchang Yu*
*Dept of Computer Science & Engineering, Korea University
**Dept of Computer Science, Korea National Open University

요 약

최근 대규모 사용자를 대상으로 하는 응용 서비스에서 생체인증의 도입이 증가함에 따라, 생체인증을 수행하는 기반 시스템이 요구하는 연산 자원과 저장 능력이 높아지고 있다. 그러나 기존의 연구에서는 이러한 요구사항에 대하여 시스템의 정량적 확대만을 고려하고 있어 많은 컴퓨팅 비용과 에너지 소모를 야기한다. 따라서 본 연구에서는 대규모 사용자를 대상으로 하는 인증 시스템에서 매칭작업에 대한 연산량 최소화와 에너지 사용면에서의 효율성을 위하여 클라우드 기반의 통합인증 시스템을 설계하고 이를 효율적으로 운용하는 방법을 제시한다. 연구의 결과는 인증 서비스의 운용비용 감소와 탄소배출 감소를 이루어 생체인증 관련 산업발전에 기여할 것으로 기대된다.

1. 서론

최근 생체인증은 중요 기반시설에서 소수 사용자를 대상으로 수행하는 서비스에서 대규모 일반 사용자 대상의 서비스로 확대되고 있다. 특히 공중망을 통하여 금융거래를 수행하는 핀테크(FinTech) 분야에서 보안성 강화를 위해 기존의 패스워드 기반의 사용자 인증방식에서 생체인증 방식으로 이동하고 있다[1]. 이러한 트렌트에 따라 인증을 수행하는 기반 시스템은 높은 처리능력과 대용량의 템플릿을 저장할 수 있는 스토리지를 요구하고 있다. 변화된 요구사항을 만족하기 위하여 데이터 센터의 일정 자원을 임대하여 인증 시스템을 구축하는 방식이 새롭게 각광받고 있다.

그러나 시스템의 정량적 확대에 대해서만 고려될 뿐 다양한 서비스를 통합하고 에너지 효율을 고려한 관리 기법에 대한 연구가 이루어지지 않고 있다[2][3][4][5]. 기존의 소규모 템플릿을 이용한 생체인증 시스템 구조를 기반으로 대규모 사용자에 대한 서비스를 수행할 시 서브시스템들이 정적으로 운용되기 때문에 많은 컴퓨팅 자원과 에너지를 소모하게 된다.

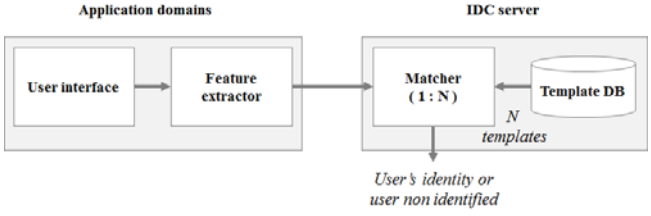
본 연구에서는 이러한 한계점을 보완하기 위해 각 서비스마다 독립적으로 구성되어 있는 생체인증 시스템을 클라우드 기술을 이용하여 통합하여 컴퓨팅 자원 절약과 에너지 효율을 이루는 통합인증 시스템 모델을 제안하고자 한다.

† "본 연구는 미래창조과학부 및 정보통신기술진흥센터의 ICT/SW창의연구과정지원사업(SW중심대학)의 연구결과로 수행되었음" (R2215-15-1007)

본문의 구성으로 2장에서는 기존의 네트워크 기반 생체인증 시스템에 대한 소개와 한계점에 대하여 설명하고 3장에서는 제안하는 통합 인증시스템에 대한 설명을 진행한다. 4장에서는 제안 모델이 기존의 방식과 차별화되는 성능을 보이기 위한 성능 모델을 만들어 비교하였다. 마지막으로 본문의 5장에서는 본 연구의 결론과 향후 연구방향에 대하여 서술한다.

2 네트워크 기반의 생체인증과 한계점

네트워크 기반의 생체인증 시스템은 (그림 1)과 같은 구조를 가진다[1]. 사용자 인터페이스를 통해 수집된 생체이미지는 Feature Extractor를 통하여 특징점이 추출된다. 그 후 특징점을 네트워크를 통하여 Matcher에 전달되고 사전 등록 단계에서 저장된 N개의 템플릿과 비교하여 식별을 수행한다.



(그림 1) Network-based Biometric System

이러한 네트워크 기반의 생체인증 시스템에서는 다양한 어플리케이션의 이용패턴에 따라 적응적으로 동작하지 못하여 시스템

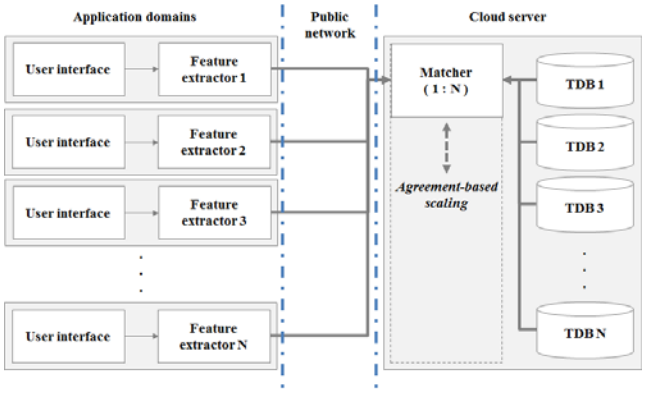
내부에 있는 모든 구성요소들이 항시 런타임 상태에서 운용된다. 따라서 생체인증을 이용하는 어플리케이션의 수에 비례하여 불필요한 컴퓨팅 자원 사용과 많은 에너지 소비가 발생한다.

3. 제안 통합인증 시스템

3장에서는 기존 네트워크 기반 인증시스템에 클라우드 시스템을 도입한 제안 통합인증 시스템을 제시한다. 처음으로 제안 통합인증 시스템 모델에 대하여 제안하며, 시스템 위에서 수행할 수 있는 다양한 서비스 유형과 Matcher의 연산 최소화 기법을 제안한다.

3.1 제안 통합인증 시스템 모델

기존 인증시스템이 가진 단점을 해결하기 위하여 클라우드 기반의 통합인증 시스템을 설계하고 이를 효율적으로 운용하는 서비스 모델을 제시한다. 제안 모델에서 사용하는 시스템 구조는 (그림 2)와 같다. 본 구조에서는 전체 생체인증 시스템의 User Interface와 Feature Extractor로 구성된 서브시스템을 어플리케이션 도메인에 운용하며 나머지 서브시스템들을 클라우드 기반의 서버에 통합하여 동적으로 할당하는 형태를 가진다.

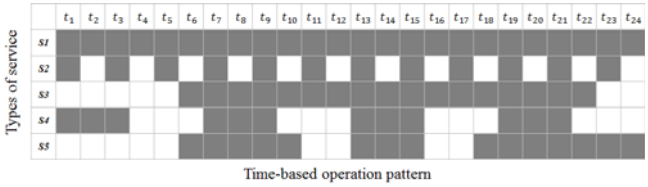


(그림 2) Cloud-based biometric system model

어플리케이션 도메인은 임베디드 형태의 단말기로 구현되며, 먼저 사용자의 생체정보를 수집하고 특징점을 추출하는 기능을 수행한다. 그 후 수집된 특징점을 공중망을 이용하여 실시간으로 클라우드 서버에게 전송한다. 단순함을 위하여 공중망을 통해 이동하는 데이터는 안전한 채널을 사용하는 것을 가정한다. 클라우드 서버는 Matcher를 가상머신 형태로 구성하고 서비스 요구사항에 따라 동적으로 자원을 확장한다. TDB는 등록 단계에서 수집된 특징점을 보관하는 저장소로 클러스터로 통합된 구조적인 특징을 가진다. 또한 통합된 구조적 특징을 활용하여 단일 사용자가 추가적인 인증키 등록절차 없이 타 서비스에 대한 인증을 수행하는 기능을 제공할 수 있다.

3.2 오토 스케일링을 위한 서비스 모델

기존 네트워크 기반 인증 시스템에서 클라우드 시스템 구조를 도입하여 얻을 수 있는 대표적인 기능으로 Matcher에 대한 오토 스케일링이 있다. 본 장에서는 사용자 SLA를 위배하지 않는 선에서 전체 에너지 소비를 최소화하는 오토 스케일링 수행 시 기준이 되는 5가지 서비스 모델을 제시한다. (그림 3)은 오토 스케일링을 통한 시스템 최적화를 위하여 인증 서비스 등록 시 선택할 수 있는 서비스의 유형에 따른 동작패턴을 나타내고 있다.



(그림 3) Types of cloud-based biometric service

대규모 사용자에 대한 생체인증을 활용하는 어플리케이션에 따라 요구하는 속성이 다양하다. 이러한 특징 중 가용성과 인증 서비스를 요청하는 시간의 표준편차를 고려하여 기준을 확립하였다. 제시한 5가지 서비스 모델에 대한 소개와 특징은 다음과 같다.

1) 서비스 유형 1

S1은 항시 서비스를 런타임 상태에 두는 방식을 나타낸다. 이러한 유형은 서비스에 대한 높은 가용성을 요구하면서 인증 요청 시간이 넓게 분포된 경우가 선택한다.

2) 서비스 유형 2

S2는 서비스의 가용시간이 짝수 시간과 홀수 시간에 번갈아가며 런타임과 유휴상태로 변경하는 경우를 말한다. 상대적으로 낮은 가용성을 허용하면서 인증 요청시간의 분포가 넓은 경우 선택한다.

3) 서비스 유형 3

S3은 전체 24시간 중 시작 시간과 종료 시간의 범위를 사용자가 선택하여 범위에 속한 시간에만 서비스를 가용상태로 두는 방식을 나타낸다. 특정 범위의 시간에 높은 가용성을 요구하는 경우 선택한다.

4) 서비스 유형 4

S4는 S2와 같이 런타임과 유휴 상태를 주기적으로 변경하지만 일정 시간을 사용자가 입력하여 주기를 설정하는 형태를 나타낸다. 이러한 방식은 주기적으로 높은 가용성을 요구하는 경우 선택한다.

5) 서비스 유형 5

S5는 서비스 등록 시 사용자로부터 이용시간에 대한 구체적인 정보를 수집하여 서비스 가용상태를 관리하는 방식을 나타낸다.

제안 서비스 유형을 활용할 시 24시간을 기준으로 단위

시간 마다 SLA 보장을 위한 오토 스케일링을 수행하며 특정 시간에 요구되는 Matcher 연산 자원을 계산하는 알고리즘은 (그림 4)에서 나타내고 있다.

Algorithm 1 Time-based matcher SLA generation

```
generateSLA(int time)
1:  List bookedServiceList
2:  List s3Period, s4Period;
3:  List s5TupleList
4:  int SLA = 0;
5:  int s2State = 0;
6:  int s4State = 0;
7:  int i = time;
8:    // Add service type 1
9:    SLA += S1 * n1;
10:   // Add service type 2
11:   if ( i / 2 == s2State ) then
12:       SLA += S2 * n2;
13:   end if
14:   // Add service type 3
15:   for j=1 to j<=S4.length do
16:     if ( i > s4Period[j].start && i < s3Period[j]end )
17:       SLA += S3;
18:     end if
19:   end for
20:   // Add service type 4
21:   for j=1 to j<=S4.length do
22:     if ( i % s4Period[j] == 1 ) then
23:       if ( s4State == 1 ) then
24:         s4State = 0;
25:       elif ( s4State == 0 ) ) then
26:         s4State = 1;
27:       end if
28:     end if
29:     if ( s4Stae == 1 ) then
30:       SLA += S4;
31:     end if
32:   end for
33:   // Add service type 5
34:   for j=1 to j<=S5.length do
35:     for x=1 to x<=S5.length do
36:       if ( i > s5TupleList[j].s5tuple[x].start &&
37:            i < s5TupleList[j].s5tuple[x].end )
38:         SLA += S5;
39:       end if
40:   end for
42: return SLA;
```

(그림 4) 시간 기반의 Matcher SLA 도출 알고리즘

(그림 4)의 7~41에서는 매개변수로 입력받은 시간 데이터를 기반으로 해당 시간에 필요한 SLA를 계산하여 도출하는 과정을 보인다. 1~6의 데이터는 사용자로부터 입력받아 최적화된 SLA를 계산하는 작업에 활용된다. 제안 통합인증 시스템을 기반으로 인증 서비스를 수행할 시 등록된 서비스 정보에 대한 입력 값으로 가용시간이 결정되고 소비된 만큼 요금이 책정한다. 따라서 이용자는 공정하고 합당한 방식으로 책정된 비용을 청구 받을 수 있다.

3.3 Markov Chain을 이용한 1:N Matcher 최적화

Matcher에서 소모되는 에너지는 각 어플리케이션에 대응되는 TDB(Template Data Base)의 크기에 영향을 받는다. TDB에 등록된 사용자 수가 늘어날수록 1:N 식별과정에서 비교를 수행하는 연산량이 늘어나고 요구되는 컴퓨팅 자원의 규모도 증가한다. 등록된 사용자 템플릿의 수가 N이라고 가정했을 때 인증 요청하는 시점마다 최대 N번의 비교 연산을 수행해야 한다. 이러한 한계점을 해결하기 위하여 k-means 알고리즘을 이용하여 요청된 시간을 기준으로 대상 템플릿들을 그룹으로 구분하며, 이를 Markov Chain으로 모델링하여 Matching 연산에서 소비되는 컴퓨팅 자원을 절약하는 기법을 제안한다. 제안하는 최적화 기법은 다음과 같이 2단계로 나누어진다.

1) Training 단계

일정 기간 동안에 수집한 요청 로그를 분석하여 Markov Chain을 구성하는 단계이다. k-means 알고리즘을 통하여 구분된 k개의 그룹은 하나의 상태가 되며, 다른 상태로 전환하는 사건에 대한 확률 데이터를 도출한다. 제안 시스템은 공중망으로 연결된 분산 시스템 형태를 가정하기 때문에 어플리케이션 도메인과 클라우드 서버에서 각각 다른 시간을 보관한다. 제안 기법에서는 SLA를 보장을 기반으로 클라우드 서버에서 이루어지는 최적화 작업이기 때문에 클라우드 서버 시간을 기준으로 정한다.

2) Matching 단계

어플리케이션에서 인증을 요청할 경우 클라우드에 도착한 시간을 기준으로 Training 단계에서 분류된 그룹과 비교하여 근사한 그룹을 선택한다. 만약 지정된 그룹에서 식별 가능한 템플릿을 검색한 경우 인증을 성공하며, 실패 시 다른 그룹에서 템플릿을 검색한다. 여기서 다음 그룹을 선택하는 작업은 Markov Chain에 저장된 확률 정보를 기준으로 우선순위를 결정한다.

4. 성능분석

4장에서는 본 연구에서 제안한 클라우드 통합인증 모델의 에너지 효율을 검증하기 위하여 Cloudsim을 통하여 시뮬레이션을 수행하였다[6]. 4.1장은 실험을 수행한 환경에 대하여 설명하며, 4.2장에서는 실험 결과와 이에 대한 분석을 설명한다.

4.1 실험환경

<표 1> 실험환경

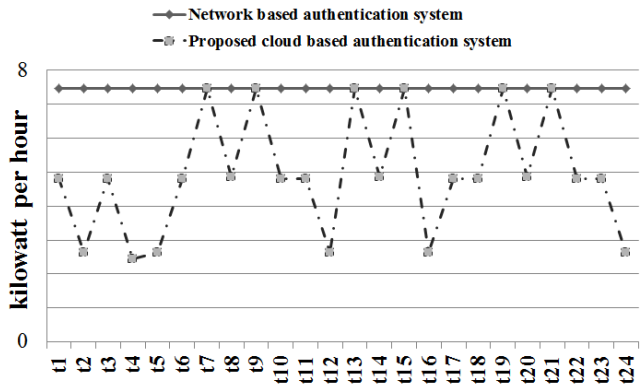
Host Machine	Virtual Machine
MIPS : 1860 PES : 2 Memory : 2GB Bandwidth : 1 Gbit/s Storage : 1GB Power Model : Xeon 3040 1860 MHz, 2 cores	MIPS : 2500 PES : 50 Memory : 1GB Bandwidth : 100 Mbit/s VM Size : 2.5GB

<표 1>은 Cloudsim을 활용한 시뮬레이션에서 설정한 시스템 환경을 나타내고 있다. 실험에서 호스트 머신은 50개로 설정하여 대규모 클라우드 서버 형태를 구성하였으며, 가상머신은 특정 시간에 도출된 요구사항에 따라 동적으로 1~5개 범위를 가지고 동적으로 할당하는 방식으로 구성하였다.

4.2 제안 통합인증 시스템 모델의 에너지 효율

본 실험은 단위 시간을 24시간으로 하여 소비된 총 에너지를 측정하는 실험을 수행하였다. 가로축은 실험을 수행한 단위 시간을 나타내며, 세로축은 단위 시간마다 소비된 에너지를 킬로와트로 나타내고 있다. 실험 대상은 (그림 3)과 같이 5가지 유형의 서

비스가 1개씩 등록된 시스템을 가정하였다.



(그림 5) 단위 시간의 에너지 소비량

실험 결과 기존 네트워크 기반의 인증 시스템은 오토스케일링 기능을 활용하지 않아 7.46 kWh의 일정한 값을 유지한다. 이에 비해 제안 통합인증 시스템은 단위 시간마다 요구되는 SLA에 최적화하여 오토스케일링을 수행하면서 kWh의 수가 33.95%로 개선된 에너지 효율을 보이고 있다.

5. 결론

본 연구에서는 생체인식 시스템의 에너지 효율을 위하여 클라우드 기반의 통합인증 서비스 모델을 제안하였다. 제안 시스템의 효과를 나타내기 위하여 구조적 특징을 성능 모델로 도출하고 비교분석하였다. 연구의 결과는 인증 서비스의 운용비용 감소와 탄소배출 감소를 이루어 생체인증 관련 산업발전에 기여할 것으로 기대된다. 향후 제안 통합인증 모델을 기반의 시스템을 대상으로 기계학습 기법을 활용하는 성능튜닝 기법을 연구하고자 한다.

참고문헌

[1] P. Barham, “An Introduction to Biometric Recognition”, SOSP, 2004, page 164-177.

[2] Li-Hua Li, Juon-Chang Lin, Min-Shiang Hwang, A Remote Password Authentication Scheme for Multiserver Architecture Using Neural Networks, IEEE TRANSACTIONS ON NEURAL NETWORKS, Vol. 12, No. 6, 2001, page 1498-1504.

[3] Leslie Lamport, Password Authentication with Insecure Communication, Communication of the ACM, Vol. 24, No. 11, 1981, page 770-720.

[4] Min-Shiang Hwang, Li-Hua Li, A New Remote User Authentication Scheme Using Smart Cards.

[5] Anul K. Jain, Lin Hong, Sharath Pankanti, Ruud Bolle, An Identity-Authentication System Using Fingerprints, PROCEEDINGS OF THE IEEE, Vol. 85, No. 9, 1997, page 1365-1388.

[6] http://www.cloudbus.org/cloudsim/