프라이버시 보호를 위한 Self-Destructing 환경에서 강화학습 기반의 임계값 결정 방법

김영기○, 홍충선*
경희대학교 컴퓨터공학과
{qoo0144, cshong}@khu.ac.kr

Reinforcement Learning Based Threshold Estimation in Self-Destructing Scheme for Privacy Protection

Young Ki Kim○, ChoongSeon Hong*
Department of Computer Science and Engineering, Kyung Hee University

요 약

클라우드 컴퓨팅을 활용한 기술 및 서비스가 발전함에 따라 이를 사용하는 기업 또는 개인 사용자들이 점차 늘어나고 있다. 그러나 최근들어 클라우드 스토리지에 개인정보를 저장하고 활용하는 사용자들이 증가하면서 클라우드 환경에서의 프라이버시 보호 모델에 대한 연구가 더욱 중요시 되고 있다. 이를 위한 방법으로 분산 해시 테이블 네트워크를 이용하여 일정 시간이 지나면 암호화된 사용자의 데이터를 복호화할 수 없도록 하는 Self-Destructing Scheme이 제안되었다. 그러나 기존의 프라이버시 보호 모델에서는 데이터의 가용성과 보안성을 고려하여 임계값을 설정하는 방법에 대해서는 언급하고 있지 않다. 따라서 본 논문에서는 기계학습의 한 방법인 강화학습을 적용하여 프라이버시 보호 모델의 데이터 가용성과 보안성을 모두 고려한 최적의 임계값 찾는 방법을 제안한다.

1. 서 론

클라우드 환경에서의 프라이버시 보호 모델에 대한 연구가 더욱 중요시 되고 있는 가운데 이를 위한 방안으로 Threshold Secret Sharing[1]을 활용하여 암호화에 필요한 키를 여러 조각으로 나누고 이를 분산 해시 테이블 네트워크(Distributed Hash Table Network)를 이용하여 일정 시간이 지나면 암호화된 사용자의 데이터를 복호화할 수 없도록 하는 Self-Destructing Scheme이 제안되었다[2].

그러나 기존의 Self-Destructing Scheme에서는 암호화된 데이터에 대한 가용성과 보안성을 고려하는 임계값을 설정하기 위한 방법에 대해서는 언급하고 있지 않다.

따라서 본 논문에서는 노드들이 지속적으로 추가/삭제되는 분산 해시 테이블 네트워크의 특성을 고려하여 임계값을 결정하는 방법을 제안한다. 임계값을 결정하는 과정에서는 강화학습의 한 방법인 SARSA를 적용하여 데이터의 가용성과 보안성을 고려한 최적의 임계값을 예측한다.

이 논문은 2017년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (2015-0-00274,(ICBMS-2세부) ICBMS 플랫폼 간 정보 모델 연동 및 서비스 매쉬업을 위한 스마트 중재 기술 개발). 본 논문은 산업통상자원부 산업핵심기술개발사업으로 지원된 연구결과임 (10049079, 퍼스널 빅데이터를 활용한 마이닝 마인즈 핵심 기술 개발) *Dr. CS Hong is the corresponding author

2. 관련 연구

2.1 Self-Destructing Scheme

Self-Destructing Scheme은 2009년 Geambasu 등이 제안한 프라이버시를 보호하기 위한 모델이며 시스템의 구조는 그림 1과 같다.

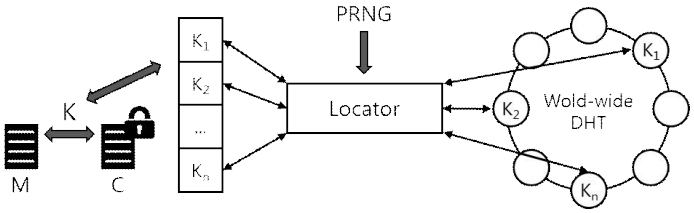

그림 1. Self-Destructing Scheme

Self-Destructing Scheme에서는 데이터를 암호화 하는데 사용되는 키를 여러 개의 조각으로 나누어 특정 기간이 지나면 데이터가 사라지는 분산 해시 테이블 네트워크에 분배하는 방식이다.

2.2 강화학습

강화학습은 기계학습의 한 영역으로, 특정 환경에서 정의된 에이전트가 현재의 상태를 인식하여 선택 가능한 행동들 중 보상을 최대화하는 행동을 선택하는 방법이다. 본 논문에서는 Self-Destructing Scheme에서 전체 Subkey의 개수와 복호화 하는데 필요한 최소한의 Subkey의 개수의 관계에서 최적의 임계값을 찾는 방법을 제안하고자 한다.

3. 기존 연구의 문제점 및 제안사항

[2]에 따르면 나누어진 키 조각의 전체 개수와 복호화 하기 위해 필요한 최소한의 개수는 데이터의 가용성 및 보안성과 관련되어있다.

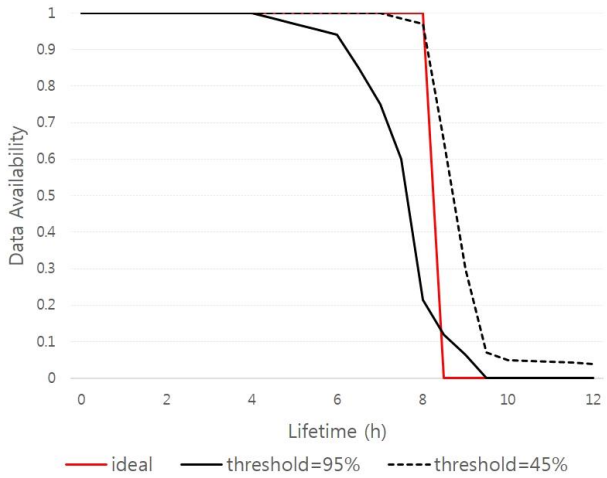

그림 2. Self-Destructing Scheme에서 데이터의 가용성

그림 2는 기존의 기법에서 N개의 같은 키 조각과 이를 복호화 하기 위해 필요한 임계값이 다른 두 그래프를 나타낸다. 임계값의 비율이 95%인 경우에는 데이터가 유지되어야 하는 시간을 충족하지 못했으며, 45%인 경우에는 일정 기간이 지난 뒤에도 키의 조각이 완전히 사라지지 않았으므로 보안상의 문제를 야기할 수 있다. 이러한 문제는 노드들이 지속적으로 추가/삭제되는 분산 해시 테이블 네트워크의 특수성 때문이며 이를 해결하기 위한 연구 또한 활발하게 진행되고 있다[3].

데이터의 가용성 및 보안성을 모두 고려하기 위해서는 이상적인 그래프와 가장 유사한 결과를 갖는 임계값을 찾아야 한다. 따라서 본 논문에서는 이를 해결하기 위해 그래프의 유사도와 임계값을 바탕으로 강화학습을 적용하여 최적의 임계값을 찾는 방법을 제안한다.

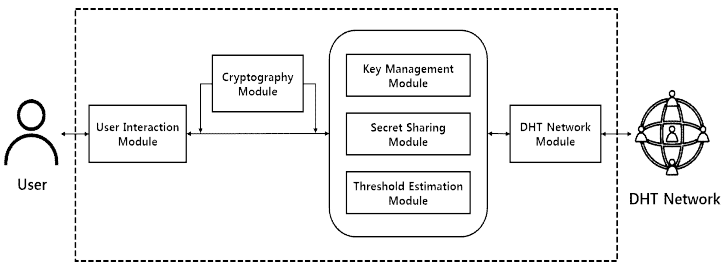

그림 3. 제안하는 시스템의 구조도

그림 3은 본 논문에서 제안하는 시스템의 구조도이다. 시스템의 구조는 사용자로부터 입력 값을 전달받기 위한 User Interaction Module, 암호화 및 복호화를 수행하는 Cryptography Module, 암호화 및 복호화를 수행하는데 필요한 키를 관리하는 Key Management Module 및 Threshold Secret Sharing을 수행하기 위한 Secret Sharing Module과 임계값을 예측하기 위한 Threshold Estimation Module로 구성된다.

제안하는 강화학습을 적용한 임계값 결정은 Threshold Estimation Module에 포함되며 다음과 같은 과정을 통해 수행된다.

Algorithm : Reinforcement Learning Based Threshold Estimation

1: Initialize $Q(s, a)$
2: **Repeat** (for each episode)
3: Initialize s
4: Choose a from s using Q (ε-greedy)
5: **Repeat** (for each step of episode)
6: Take action a, observe r, s'
7: Choose a' from s' using Q (ε-greedy)
8: $Q(s, a) \leftarrow Q(s, a) + \alpha[r + \gamma Q(s', a') - Q(s, a)]$
9: $s \leftarrow s'; a \leftarrow a'$
10: **Until** s is terminal

그림 4. 강화학습을 적용한 임계값 예측 과정

본 논문에서는 데이터의 가용성과 보안성을 고려하여 임계값을 예측하기 위한 방법으로 강화학습의 한 종류인 SARSA를 적용한다. 학습과정이 시작되면 초기 State 및 Action을 행렬형태로 구조화하고 현재 State 및 Action, 다음 State 및 Action과 Reward를 바탕으로 행렬을 갱신한다. 이 때, 필요한 매개변수 즉, State, Action, Reward는 다음과 같이 정의한다.

표 1. 강화학습을 위한 매개변수

State	N, T
Action	Select N, T
Reward	Similarity with Ideal Graph

N은 Threshold Secret Sharing 과정에 필요한 전체 Subkey의 개수이며, T는 Key K를 얻기 위해 필요한 임계값을 의미한다. 또한 Reward는 선택된 N, T를 바탕으로 데이터의 가용성 그래프를 측정하여 앞서 언급한 이상적인 그래프와의 유사도로 정의한다. 그리고 학습과정을 통해 Reward를 최대화하는 N, T를 찾아 적용한다.

4. 성능평가

표 2. 실험 환경

Cryptographic Algorithm	AES-CBC
Key Size	128 bit
Num. of Dataset	100
Num. of Total Subkeys	10
DHT Network Protocol	BitTorrent
Num. of DHT Nodes	1000

표 2는 본 논문에서 성능 평가를 위해 구축한 실험 환경이다. 암호화 및 복호화 알고리즘으로는 128bit 크기의 Key를 사용하는 AES-CBC[4]를 사용했으며, 강화학습을 적용하기 위해 임의로 만든 100개의 데이터를 활용한다. 각각의 데이터는 50개의 Subkey, $K_1, K_2, \ldots, K_{10}$로 구성된다. 또한 DHT Network 환경은 Peersim Simulator에서 Kademlia Protocol을 활용한 Bit Torrent를 기반으로 구축하였다[5].

본 논문에서의 성능 평가를 위한 시나리오는 다음과 같다. 먼저 각 데이터별로 암호화하기 위한 Key K를 생성하고 Threshold Secret Sharing을 활용하여 50개의 Subkey를 생성한다. 그리고 설정된 임의의 임계값을 바탕으로 DHT Network에서의 데이터 가용성 그래프를 측정하여 이상적인 그래프의 결과와 비교한다.

표 3. DHT Network에서의 LOOKUP 연산

Timeout (ms)	Delay (s)	Reply (%)
1000	4.59	34.7
2000	5.78	44.8
3000	6.92	48.7
4000	7.24	47.8
5000	7.97	47.2

표 3은 분산 해시 테이블 네트워크에서 LOOKUP 연산의 성능을 측정한 결과이다. Timeout은 네트워크를 구성하는 노드의 테이블에 데이터가 저장되어있는 시간을 의미한다. 또한 Delay는 인접한 10개의 노드에 LOOKUP 연산을 수행하는데 걸리는 시간을 의미하며, Reply는 노드로부터 정상적인 응답을 받은 비율을 의미한다. 측정된 결과에 따르면 timeout이 클수록 delay와 reply가 증가하며 이는 시스템을 사용하는 사용자의 측면에서 만족도와 연관된다.

강화학습을 통한 임계값의 예측은 학습이 진행되면서 그래프의 모양이 지속적으로 변한다는 것과 데이터의 크기 및 키 조각의 개수에 따라 최적의 임계값이 다르기 때문에 중요한 의미를 갖는다.

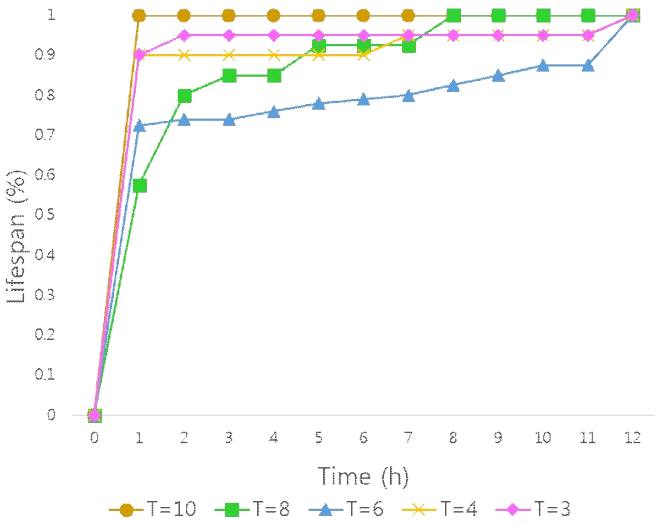

그림 5. 추정된 임계값에 따른 데이터의 가용성

그림 5는 전체 키 조각의 개수가 10일 때 임계값을 3에서 10까지 변화하며 강화학습을 통해 추정한 임계값을 바탕으로 데이터의 가용성 그래프를 측정한 결과이다. 측정된 결과에 따르면 임계값이 너무 높거나 낮은 경우 데이터의 수명이 짧은 것으로 측정되었다. 따라서 사용자의 요구사항을 충족시키기 위해서는 강화학습을 통해 60에서 80사이의 임계값이 추정될 것으로 예상된다.

5. 결론 및 향후 연구계획

본 논문에서는 Self-Destructing Scheme에서 강화학습을 적용하여 데이터의 가용성과 보안성을 모두 고려한 최적의 임계값을 찾는 방법을 제안했다. 또한 추정된 임계값의 그래프를 비교하여 성능을 검증했다. 그러나 본 논문에서는 학습과정에 많은 시간이 요구되는 한계를 갖고 있다. 따라서 추후에는 병렬처리 및 클러스터링 기법을 적용하여 학습과정에 필요한 시간을 최적화하는 연구와 더불어 SARSA(lambda)를 적용하여 강화학습 알고리즘을 효율적으로 개선하는 연구가 진행될 것으로 예상한다.

참 고 문 헌

[1] B. Poettering, "Shamir's Secret Sharing," [Online], Available: http://point-at-infinity.org/ssss/, 2006.

[2] R. Geambasu, T. Kohno, Amit A. Levy, Henry M. Levy, "Vanish: Increasing Data Privacy with Self-Destructing Data," USENIX Security Symposium, pp.299-316, June 2009.

[3] S. Rhea, D. Geels, T. Roscoe, J. Kubiatowicz, "Handling Churn in a DHT," USENIX Annual Technical Conference, December 2003.

[4] J. Daemen, V. Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard," Information Security and Cryptography, 2002.

[5] P. Maymounkov, D. Mazieres, "Kademlia: A peer-to-peer information system based on the XOR metric," International Workshop on Peer-to-Peer Systems, pp.53-65, March 2002.