# 포그 컴퓨팅 환경에서 IoT 보안에 관한 연구 동향

우미애
세종대학교

mawoo@sejong.ac.kr

# Research trends on IoT security in fog computing environments

Miae Woo
Sejong Univ.

요 약

포그 컴퓨팅은 IoT 장비가 생성하는 많은 데이터를 효율적으로 처리하기 위하여 도입된 개념이다. 분산처리에 기반하는 포그 컴퓨팅의 특성과 자원이 한정적인 IoT 장비의 취약성으로 인해 여러 가지 보안에 관련된 문제가 발생한다. 본 논문에서는 포그 컴퓨팅의 특성을 고려한 보안 대책에 대한 연구 동향을 알아본다.

## Ⅰ. 서 론

IoT 장비는 매일 많은 양의 데이터를 생성한다. 이러한 데이터를 실시간으로 클라우드에 올려서 분석하는 것은 여러 가지 문제를 야기한다. 데이터의 처리, 저장, 관리, 보안을 좀 더 효율적으로 제공하기 위하여 클라우드와 IoT를 통합할 필요성이 대두되었고, 이를 위해서 2012년에 시스코가 포그 컴퓨팅 개념을 도입하였다. 포그 컴퓨팅은 클라우드 컴퓨팅을 확장하여 네트워크의 에지에서 서비스를 제공하는 것으로, 클라우드 컴퓨팅을 대체하기 보다는 보완하는 개념이다. 포그 컴퓨팅의 주된 목적은 보안을 증진시키고, 클라우드에 저장하는 데이터를 최소화하고 IoT 응용의 전반적인 효율을 증진시키는 데 있다. 그러나 포그 컴퓨팅은 태생적으로 분산처리에 기반하기 때문에 클라우드 컴퓨팅보다 더 많은 보안 관련 문제가 발생한다. 포그 컴퓨팅에서 보안을 위한 많은 연구결과가 있지만, IoT 장비가 가지고 있는 자원의 제약성과 이동성, 네트워크 에지에 있는 포그 노드들 간의 협업 필요성, 네트워크의 개방성 및 분산처리 문제 등으로 인하여 아직도 보안에 대한 대책이 완전하게 수립되지 않았다. 전 세계 기업의 85% 이상이 어떤 형식이든지 IoT 장비를 사용할 것으로 예측되는 가운데, 그러한 기업들 중 90%가 IoT 장비의 보안에 대한 확신을 갖고 있지 않다. 따라서 보안을 보장할 방안이 사용자가 만족할 만한 수준에서 제공되지 않는다면 IoT 응용이나 포그 컴퓨팅이 산업에 안착할 수 없을 것이다. 이에, 본 논문에서는 포그 컴퓨팅 환경에서의 보안 제공을 위한 IoT 장비와 포그 노드에서의 요구사항 및 연구 동향에 대하여 알아본다.

## Ⅱ. 포그 컴퓨팅에서의 보안 대책

IoT 장비는 방어를 충분히 할 수 없어 해킹, 파손, 도난에 취약하다. 인터넷에 연결된 장비의 70%가 공격에 취약하다는 연구 결과가 있다. 또한 연결된 IoT 장비의 수가 증가함에 따라, IoT 장비의 취약성은 사용자의 보안에 대한 우려를 가중시킨다. 따라서 효과적이고 효율적인 보안을 보장하는 메커니즘을 포그 컴퓨팅에서 구현해야 한다. 포그 컴퓨팅 특징 중 하나인 네트워크 개방성 때문에 다른 종류의 네트워크에서 사용하는 기존의 공격 대응 방안은 포그 컴퓨팅에 적절하지 않다. 이 장에서는 포그 컴퓨팅에서의 인증, 접근 제어, 신뢰 관리, 암호화, 침입탐지와 같은 보안 대책에 대하여 알아본다.

### 2.1 인증

IoT에서의 인증은 많은 사용자를 대상으로 하기 때문에 확장성, 효율성이 필요하고, 포그 컴퓨팅의 분산화, 실시간 서비스의 낮은 지연 요구, 사용자의 이동성은 인증 문제를 어렵게 한다. Octopus[1]는 느린 속도로 이동하는 IoT 장비가 하나의 마스터 비밀 키로 클라우드 서비스 제공자가 관리하는 포그 노드와 상호 인증할 수 있는 방법을 제안하였다. 고속 이동 시 인증에 대한 연구로 EU 규정인 eIDAS를 따르는 방안[2]이 있다.

### 2.2 접근 제어

접근 제어는 공인된 대상만이 IoT 장비나 수집한 데이터 같은 자원에 접근할 수 있게 하는 보안 기법으로 모든 신뢰 도메인에는 승인 구조가 있어야 하고 인증 메커니즘을 배치하여 관리자가 각각의 도메인의 접근 정책을 정의, 적용해야 한다. 검증된 사용자 접근을 정책기반으로 관리하는 방법[3]에서는 포그 노드가 접근 제어 리스트나 특정기반 접근 제어 같은 표준화된 접근 제어 모델을 사용하도록 하였다. 이동 장비 관리 프로토콜을 구현하여 BYOD(Bring your own device) 환경에서 여러 모바일 장비의 접근 제어를 지원하는 방안[4]이 제안되었다. 사용자 레벨의 키 관리와 업데이트 메커니즘을 사용하여 포그 저장 시스템에 대한 접근 제어를 제공하기 위하여 암호화된 데이터에 대한 중복제거 방안[5]이 제안되었다.

### 2.3 신뢰

신원 인증과 접근 제어로 가짜 포그 노드나 장비가 IoT 응용에 접근하는 것을 막을 수 있으나, 여전히 가입하는 대상을 완전히 신뢰할 수 있느냐는 다른 문제이다. 포그 컴퓨팅에서의 신뢰관리에 대해서는 시스템의 보안

요인과 감사 기반 요인 등을 포함하는 모든 참여 노드들의 보안 요인에 기반한 종단간 신뢰도 인지 방안[6]이 있다.

### 2.4 암호화

민감한 정보를 보호하기 위해서는 암호화 방안이 필요하다. 무인증서 종합 온라인/오프라인 서명 암호화 방안(CLAOSC)[7]은 온라인/오프라인 암호화와 무인증서 종합 서명암호화를 합쳐서 제안한 새로운 서명암호화 방안이다. IoT 환경에서 인증서 해지 배포를 효율적이고 효과적으로 개선하기 위하여, 포그 노드는 특정 인증기관이 발행하는 디지털 인증서를 사용하는 일련의 IoT 장비 그룹을 지원하도록 하여 인증서 해지를 일반화할 수 있게 한 방안[8]이 제안되었다. 이 방안은 블룸 필터를 사용하여 계산 오버헤드를 줄이고 해지 리스트를 효과적으로 단축시켜 저장 공간을 절약할 수 있다. 특성 기반 암호화 방안을 IoT 환경에서 사용할 수 있도록 개선한 방안들도 제안되었다. 포그 노드들 간에 인증된 기밀 데이터를 공유하기 위해서 암호문 정책 특성 기반 암호화 기반 효율적인 키 교환 프로토콜[9]이 제안되었다. 특성 기반 암호화와 프록시 재 암호화를 지렛대로 사용하여 포그를 사용한 IoT 응용에서 데이터 공유를 위한 세부적인 데이터 접근 제어와 효율적인 접근 권한 철회를 할 수 있게 한 제안[10]도 있다. 특성 기반 암호화에서 키 위임 남용이 발생한다는 것을 밝히고, 암호문 정책 특성 기반 암호화를 개선하여 이러한 남용 문제에 대한 보호를 할 수 있는 방안을 설계[11]하여 세부적인 데이터 공유를 가능하게 하였다. 유출에서 회복할 수 있는 기능적 암호화 방안[12]을 제안하여 접근 제어 정책과 사용자의 특성 간 대응을 사용하여 세부적인 접근 제어 정책을 수립하게 한 연구도 있다.

### 2.5 침입탐지

포그 컴퓨팅에서 해킹을 방지하기 위해서는 침입 탐지 메커니즘을 동작시켜 오동작하거나 악의적으로 동작하는 IoT 장비를 탐지하고, 정책을 위반하는 포그 노드를 발견해야 한다. 인접한 포그 노드들 간의 협업을 통하여 서비스에 대한 공격을 검출하고[13] 악의적인 공격 감지의 성공률을 개선할 수 있다. 클라우드렛 멤버들 간의 협업을 통해서 악성코드와 악의적인 공격, 다른 위험요소들을 감지하는 협업에 의한 공격 탐지 기술[14]은 포그 노드 간 IoT 환경과 주변 환경을 모니터링하는 데 사용할 수 있다. 공격 탐지 방안을 IoT 장비 쪽에 적용한 예로는 지능적 신호등 제어 시스템에 대한 DoS 공격 탐지를 위해서 계산적 Diffie-Hellman puzzle을 기반으로 하는 제어 방안[15]이 있다.

## Ⅲ. 결론

본 논문에서는 포그 컴퓨팅 환경에서 네트워크의 개방성, 분산 처리 특성, 사용자의 이동성, IoT 장비의 자원 제약 등을 고려한 보안에 대한 다양한 대책들에 대하여 알아보았다. 그러나 아직도 보안 대책이 완전하게 수립되지 않았다. 그러므로 앞으로도 지속적인 연구를 통하여 효과적이고 효율적인 보안 메커니즘을 포그 컴퓨팅에 구현하여 사용자가 IoT 응용을 많이 이용하게 하여야 포그 컴퓨팅이 성공적으로 정착할 수 있을 것으로 사료된다.

## 참 고 문 헌

[1] M. H. Ibrahim, “Octopus: An Edge-Fog Mutual Authentication Scheme,” International Journal of Network Security, vol.18, no.6, pp.1089-1101, Nov. 2016.

[2] F. Buccafurri, G. Lax and A. Russo, “Exploiting Digital Identity for Mobility in Fog Computing,” Proc. Fog and Mobile Edge Computing (FMEC) 2019, pp. 155-160, 2019.

[3] C. Dsouza, G.-J. Ahn, and M. Taguinod, “Policy-Driven Security Management for Fog Computing: Preliminary Framework and a Case Study,” Proc. 15th Int’l Conf. Information Reuse and Integration, pp. 16 - 23, 2014.

[4] P. Steiner, “Going beyond mobile device management,” Comput. Fraud Security, vol. 2014, no. 4, pp. 19-20, 2014.

[5] D. Koo and J. Hur, “Privacy-preserving deduplication of encrypted data with dynamic ownership management in fog computing,” Future Generat. Comput. Syst., vol. 78, part 2, pp. 739-752, Jan. 2018.

[6] Z. Su, F. Biennier, Z. Lv, Y. Peng, H. Song, and J. Miao, “Toward architectural and protocol-level foundation for end-to-end trustworthiness in cloud/fog computing,” IEEE Trans. on Big Data, May, 2017.

[7] M. Cui, D. Han and J. Wang, “An Efficient and Safe Road Condition Monitoring Authentication Scheme Based on Fog Computing,” IEEE Internet Things J., vol. 6, no. 5, pp. 9076-9084, 2019.

[8] A, Alrawais, A, Alhothaily, C, Hu and X. Cheng, “Fog Computing for the Internet of Things: Security and Privacy Issues,” IEEE Internet Computing, vol. 21, issue 2, pp. 34 - 42, 2017.

[9] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, X. Cheng, “An attribute-based encryption scheme to secure fog communications,” IEEE Access, vol. 5, pp. 9131-9138, 2017.

[10] A. Alotaibi, A. Barnawi and M. Buhari, “Attribute-based secure data sharing with efficient revocation in fog computing,” Int. J. Inf. Security, vol. 8, no. 3, pp. 203-222, 2017.

[11] Y. Jiang, W. Susilo, Y. Mu and F. Guo, “Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing,” Future Gener. Comput. Syst., vol. 78, pp. 720-729, Jan. 2018.

[12] Z. Yu, M. H. Au, Q. Xu, R. Yang and J. Han, “Towards leakage-resilient fine-grained access control in fog computing,” Future Gener. Comput. Syst., vol. 78, pp. 763-777, Jan. 2018.

[13] R. Roman, J. Lopez and M. Manbo, “Mobile edge computing fog et al.: A survey and analysis of security threats and challenges,” Future Gener. Comput. Syst., vol. 78, pp. 680-698, Jan. 2018.

[14] Y. Shi, S. Abhilash and K. Hwang, “Cloudlet Mesh for Securing Mobile Clouds from Intrusions and Network Attacks,” Proc. 3rd IEEE Int’l Conf. Mobile Cloud Computing, Services, and Eng., pp. 109 - 118, 2015.

[15] J. Liu et al., “Secure intelligent traffic light control using fog computing,” Future Gener. Comput. Syst., vol. 78, pp. 817-824, Jan. 2018.