사물인터넷에서 개인 정보 보안 강화를 위한 위협 및 대응방안

임지수*, 박재경O
*한국폴리텍대학 사이버보안과,
O한국폴리텍대학 사이버보안과
e-mail: jisoo040630@gmail.com*, jakypark@kopo.ac.krO

Threats and countermeasures for strengthening personal information security in the Internet of Things

Jisu-Lim*, Jaekyung-ParkO
*Dept. of Cybersecurity, Korea-Polytechnics University,
ODept. of Cybersecurity, Korea-Polytechnics University

● 요 약 ●

본 논문은 사물인터넷 환경에서 개인 정보 보안을 강화하기 위해 개인 정보 위협과 대응방안을 조사하는 것을 목표로 한다. 개인 정보의 위협으로는 무단 액세스, 데이터 위반, 데이터 집계 및 프로파일링, 추적 및 감시가 있다. 이에 대한 대응방안으로는 암호화, 개인 정보 보호 데이터 처리, 보안 통신 프로토콜 등을 연구되고 있다. 또한, 실증적 연구를 통해 사물인터넷 사용자의 개인 정보 보호 문제와 기존 전략의 효과를 평가하고 권장 사항을 도출한다. 본 논문은 사물인터넷 생태계에서 개인 정보 보안을 강화하기 위한 정보를 제공하며, 개인정보를 활용하는 사용자에게 도움을 줄 것으로 기대한다.

키워드: 사물인터넷(IoT), 개인정보(Privacy), 보안 강화(Security Enhancement)

I. Introduction

본 논문은 빠르게 확장되는 사물인터넷(사물인터넷) 생태계에서 프라이버시 보안의 중요성을 조사한다. 개인 정보 위협을 식별 및 분류하고 기존 대응 전략을 평가하며 그 효과를 평가하는 것을 목표로 한다. 또한 사물인터넷에서 개인 정보 침해의 결과를 조사하고 개인 정보와 민감한 정보를 보호해야 할 필요성을 강조하고자 한다. 본 논문의 결과는 사물인터넷 환경에서 프라이버시와 보안을 우선시하는 개인정보 사용자에게 도움을 줄 것으로 판단한다. 전반적으로 이 논문은 사물인터넷의 프라이버시 문제에 대한 이해를 높이고 상호 연결된 시대에 개인과 조직을 보호하기 위해 실행 가능한 대응방안을 제공하고자 한다.

II. Preliminaries

1. Related works

1.1 Privacy threats and mitigation strategies

프라이버시 위협에는 무단 액세스, 데이터 위반, 데이터 집계 및 프로파일링, 추적 및 감시가 있다. 무단 액세스는 민감한 사용자 데이터의 손상으로 이어질 수 있으며 데이터 위반은 개인 정보에 위험을 초래한다. 데이터 집계 및 프로파일링으로 인해 사용자 동의 없이 개인 정보 침해 및 대상 광고가 발생할 수 있다. 센서와 카메라가 장착된 사물인터넷 장치는 개인 정보 보호 및 감시 데이터 오용 가능성에 대한 우려가 있다. 완화 전략으로는 다음과 같은 방안이 있다.

- 암호화 및 인증: 강력한 암호화 알고리즘 및 인증 메커니즘을 구현하여 데이터 전송을 보호한다.
- 개인 정보 보호 데이터 처리: 차등 개인 정보 보호, 익명화, 안전한 데이터 집계와 같은 기술을 사용하여 무단 데이터 노출 및 프로파일링의 위험을 최소화하여 개인정보 보호를 강화한다.
- 보안 통신 프로토콜: 보안 통신 프로토콜을 배포하여 사물인터넷 장치 간에 전송되는 데이터를 가로채거나 무단 액세스로부터 보호한다.
- 개인 정보 영향 평가: 사물인터넷 시스템의 설계 및 개발 단계에서 개인 정보 영향 평가를 수행하여 개인 정보 위험을 사전에 식별하고 해결한다.
- 규정 준수: GDPR과 같은 관련 개인 정보 보호 규정 및 표준을 준수하여 사용자 데이터 관리에 대한 개인 정보 보호 조치 및

조직의 책임을 설정한다.

이러한 대응 전략을 구현함으로써 사물인터넷 시스템의 개인 정보 보호 및 보안을 강화하여 무단 액세스, 데이터 위반, 데이터 집계 및 추적과 관련된 위협을 효과적으로 해결할 수 있다. 그림 1은 마이데이터 시대의 개인정보의 보안 위협과 대책에 대해서 나타내고 있다.

Fig. 1. Privacy Threats and Defence Strategy

III. The Proposed Scheme

본 논문의 조사는 사물인터넷 생태계의 프라이버시 보안을 조사하기 위해 설문 조사, 인터뷰 및 실험을 활용하는 혼합 방법 연구 접근 방식을 채택한다. 수집된 데이터는 통계 및 주제별 분석 기술을 사용하여 분석되어 사물인터넷 사용자 간의 일반적인 개인 정보 보호 문제를 식별하고 기존 완화 전략의 효과를 평가한다. 조사 결과를 바탕으로 윤리적, 법적 함의를 고려하여 사물인터넷 생태계의 개인 정보 보호를 개선하기 위한 권장 사항을 제공할 것이다. 그림 2에서와 같이 온라인 상에서 개인정보가 매우 중요하다고 조사되었으며 또한 온라인 전자상거래시 개인정보 유출에 대한 불안이 매우 크다고 조사되었다. 따라서 본 논문은 사물인터넷 개인 정보 보호 분야에서 개인정보를 활용하는 사용자에게 보다 효과적인 대응방안을 제시하는 것을 목표로 조사를 진행하였다.

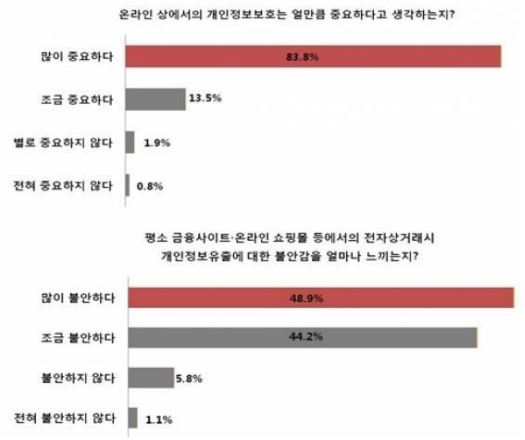

Fig. 2. Privacy survey

IV. Conclusions

본 논문은 빠르게 확장되는 사물인터넷의 프라이버시 보안의 중요성을 조사했다. 개인 정보 위협을 식별하고 대응 전략을 평가하여 효과를 분석함으로써, 개인정보 보호와 민감한 정보의 보안을 강조하고자 하였다. 조사 결과, 무단 액세스, 데이터 위반, 데이터 집계 및 프로파일링, 추적 및 감시 등 다양한 프라이버시 위협이 사물인터넷 생태계에서 발생할 수 있음을 확인하였고 이를 완화하기 위해 암호화 및 인증, 개인 정보 보호 데이터 처리, 보안 통신 프로토콜, 개인 정보 영향 평가, 규정 준수 등의 다양한 전략을 제안하였다. 본 연구는 사물인터넷의 프라이버시 문제에 대한 이해를 높이고, 상호 연결된 시대에서 개인과 조직을 보호하기 위한 실행 가능한 대응방안을 제공하였다. 앞으로의 연구와 현실적인 시행을 통해 더욱 효과적인 사물인터넷 개인정보 보호 방안을 개발할 수 있을 것으로 기대된다.

REFERENCES

[1] E. Smirni, and G. Ciardo, "Workload-Aware Load Balancing for Cluster Web Servers," IEEE Trans. on Parallel and Distributed Systems, Vol. 16, No. 3, pp. 219-232, March 2005.

[2] Kdhong, "An Efficient Dynamic Workload Balancing Strategy," Journal of The Korea Society of Computer and Information, Vol. 15, No. 1, pp. 1-10, Nov. 2010.

[3] D.H.Ballard, "Computer Vision," Prentice-Hall, pp.76-79, 1991.

[4] Kdhong,, "C Programming Language" Korea-Press, pp.100-120, 1991.

[5] SIMGRID Project, *http://simgrid.gforge.inria.fr*