

Improving Security of Customer Personal Identifiable Information (PII) on IoT Enabled Mobile Applications

R. Allirani

Department of Computer Science, Auxilium College of Arts and Science for Women, Pudukkottai, India

*Corresponding author: allirani29vasuki@gmail.com

ABSTRACT

The term Internet of Things (IoT), that make reference to the collaborative network of interconnected devices and the technology that foster communication between devices and cloud. IoT devices are typically fixed with technology such as sensors and software and can include mechanical and digital machines and consumer objects. IoT is interconnected to physical devices such as home appliances, wearable, vehicles that are lodged with software, sensors and other apparatus. IoT and Security are intertwined to prevent from various Threats and attacks. Catering different privacy risks, our anonymization process takes advantage of the disseminate and collaborative nature of the friend's network. In the group of various attributes of consumer data are those which can be used to unambiguously identify the consumer – the set of such data is called Personally Identifiable Information (PII). Personally Identifiable Information includes name, email address, contact number, address, and other data's related with the individual's. In this Paper, we used Advanced Encryption Standard (AES) algorithm, which can strongly ensure the customer or consumer privacy for PII in IoT enabled Mobile Apps. Advanced Encryption Standard (AES) 256 is a virtually impermeable symmetric encryption algorithm that uses a 256-bit key for encryption. It's obvious quantum computers are on the horizon, and AES 256 is the only way to base your secure file transfer infrastructure on a future-proof framework. Through choosing AES 256, security of customer data can be ensured.

Keywords: Anonymization, Personal Identifiable Information, Future Proof Framework

