Copyright is owned by the Author of the thesis. Permission is given for a copy to be downloaded by an individual for the purpose of research and private study only. The thesis may not be reproduced elsewhere without the permission of the Author.

Novel Lightweight Ciphertext-Policy Attribute-Based Encryption for IoT Applications

A thesis presented in partial fulfilment of the requirements
for the degree of

Master of Information Science

at Massey University, Auckland, New Zealand

Ping LI

2018

Abstract

As more sensitive data are frequently shared over the Internet of Things (IoT) network, the confidentiality and security of IoT should be given special consideration. In addition, the property of the resources-constraint nodes raises a rigid lightweight requirement for IoT security system. Currently, the Attribute-Based Encryption (ABE) for fine-grained access control is the state-of-the-art technique to enable the secure data transmission and storage in the distributed case such as IoT. However, most existing ABE schemes are based on expensive bilinear pairing with linear size keys and ciphertexts. This results in the increase of the memory and computational requirement on the devices, which is not suitable for the resource-limited IoT applications.

Leveraging on the advantages offered by the Ciphertext-Policy ABE (CP-ABE), this thesis proposes two constructions of lightweight no-paring cryptosystems based on Rivest–Shamir–Adleman (RSA). One realized work is a construction of AND-gate CP-ABE to achieve both constant-size keys and ciphertexts. The result of the evaluation shows that it reduces the storage and computational overhead. The other construction supports an expressive monotone tree access structure to implement the complex access control as a more generic system. Both have respective advantages in different contexts and are provably secure to guarantee the sharing of data, as well as more applicable and efficient than the previous scheme. In this thesis, practical issues are also described about implementations and evaluations of both proposals.

Acknowledgments

I would like to thank my supervisor Associate Professor Julian Jang-Jaccard of Massey University for making the IoT projects possible and supervising my research. Her extensive industry and academic experiences have been extremely valuable in contributing to the successful completion of my projects and thesis. I also want to express my appreciation to Associate CISSP Tim McIntosh for reviewing my thesis.

Table of Contents

List of Tables

List of Figures