Cryptography Based Data Security in Internet of Things

An Abstract Submitted to the
Babasaheb Bhimrao Ambedkar University, Lucknow
in Fulfillment of Requirement for the Award of Degree of

Doctor of Philosophy

IN

COMPUTER SCIENCE

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
LUCKNOW
प्रज्ञा शील करूणा
ESTABLISHED 1996

BY

DILIP KUMAR

ENROLLMENT NO.-1086/17

UNDER THE SUPERVISION OF

DR. MANOJ KUMAR

ASSISTANT PROFESSOR

Department of Computer Science
School for Information Science and Technology
Babasaheb Bhimrao Ambedkar University
(A Central University)
Lucknow, Uttar Pradesh-226 025

2022

Abstract

In the current digital era, the Internet of Things (IoT) is a rapidly expanding technology that is likely to be used everywhere in the future. The IoT gives us the platform to link most of the devices and share data across them. Due to the ever-growing use of IoT technologies, various transmission modes are available for data exchange in a heterogeneous IoT environment. The challenging task within the IoT environment is to transmit the data securely and efficiently over both secure and insecure networks. Cryptographic techniques (symmetric or asymmetric) provide secure and fast transmission of data over the Internet. Attribute-Based Encryption (ABE) is a modern asymmetric key cryptographic scheme that provides security and an access control mechanism in an IoT environment. Key Policy Attribute-Based Encryption (KP-ABE) and Ciphertext Policy Attribute-Based Encryption (CP-ABE) have been proven to be secure modern cryptographic techniques to achieve data security in an IoT environment. For IoT resource-constrained devices, the complexity of the ABE decryption procedure is minimized. Elliptic Curve Cryptography (ECC) is used to reduce the computational cost, and a Linear Secret Sharing Scheme (LSSS) is used to express the access policy. In the thesis, various novel cryptographic techniques are introduced to achieve data security and reduce the computational complexity of resource-constrained devices connected in IoT environments.

At first, a KP-ABE scheme with outsourcing has been proposed to

reduce decryption overhead for resource-constrained devices connected in an IoT environment. The KP-ABE decryption process is outsourced to a cloud server for partial decryption. However, the complete decryption of ciphertext is not possible at the cloud server, even if the cloud server is malicious. The use of the operation of point scalar multiplication in ECC improves the computational efficiency of our KP-ABE scheme. An LSSS access structure has been used to share the secret. The computational complexity has been reduced by using ECC and an LSSS access structure. The Replayable Chosen Ciphertext Attacks (RCCA) model has been used to prove the security of the proposed KP-ABE scheme. The implementation of the scheme uses an elliptic curve Secp256k1 over a finite field with 128 bits of security. A computational analysis of the algorithms of KP-ABE has been done by comparing the different NIST-recommended elliptic curves (P-256, P-521, P-192, and P-224) over prime fields. The effectiveness of the proposed work is analyzed by comparing it with the existing works, and it is found that our work has reduced the decryption overhead for resource-constrained devices without compromising security.

In the KP-ABE schemes, attribute authority is responsible for generating keys for the data user and the data owner. On the other side, in CP-ABE, encryptors intelligently decide who will access the data and who will not. Therefore, a CP-ABE scheme with outsourcing has been presented to give control to the data owner about the access of data while reducing the decryption overhead for resource-constrained devices connected in an IoT environment. The proposed CP-ABE system lowers the user's processing burden for data decryption, which is necessary for lightweight devices. The ECC is employed to reduce computational complexity without compromising the system's security. The outsourcing of the lengthy CP-ABE computation

to the cloud server improves the performance of lightweight devices. The use of the operation of point scalar multiplication in ECC improves the computational efficiency of our CP-ABE scheme. The computational complexity has been reduced by using ECC and an LSSS access structure. The security of the proposed CP-ABE scheme depends on an elliptic curve discrete logarithm problem. The implementation uses a 256-bit prime field Weierstrass curve Secp256k1. This work is suitable for implementation in an environment where the encryptor has the privilege to decide who is going to access the encrypted data.

Furthermore, the CP-ABE scheme shows great security using bilinear pairing. But using bilinear pairing increases the computational complexity. On the other hand, Advanced Encryption Standard (AES) is a symmetric key cryptography technique that provides security in the IoT. Therefore, a secure outsourcing of CP-ABE decryption using the bilinear pairing for the IoT has been proposed. The proposed system reduces the computational cost of decryption for the data user, which is required for lightweight devices. Joux's three-party Diffie-Hellman key exchange protocol is used to share the secret among the participating entities like attribute authority, data owner, and data user. The CP-ABE scheme has been adopted to achieve a reliable security level in the IoT environment. The outsourcing of the lengthy CP-ABE computation over the cloud server improves the performance of lightweight devices. Again, a hybrid cryptographic approach is proposed to achieve the data security using AES and ECC. This scheme is appropriate for lightweight IoT devices with limited storage and computational processing capabilities. Storage of ciphertext on a cloud server reduces storage overhead for data owners and the users. The performance of resource-constrained devices in the IoT has been enhanced by applying the lightweight properties of ECC.

The message authentication code (MAC) is used to achieve confidentiality and authenticity of the transferred message. The encryption and decryption processes of CP-ABE are expensive operations that are not suitable for lightweight IoT devices. Therefore, outsourcing of encryption and decryption can reduce the computational complexity and make it usable on lightweight devices. Another way to reduce computational complexity is through the use of lightweight cryptographic approaches like AES and ECC. The hybrid approach can also reduce computational complexity and make it usable on resource-constrained devices.

Due to the ever-growing use of IoT in the healthcare industry, several vulnerabilities are found when sensitive medical data is transmitted from one device to another. ABE is a public-key cryptographic technique that provides access control as well as security in the healthcare environment. Therefore, first, a Personal Health Records Access Control (PAC) scheme based on KP-ABE has been proposed to secure the sharing of Personal Health Records (PHR). This scheme is appropriate for lightweight medical devices with limited storage and computational processing capabilities. Ciphertext storage on the PHR server reduces storage overhead for PHR owners and users. ECC provides better security with a smaller key size compared to other existing cryptographic techniques. The KP-ABE scheme has been adopted to achieve reliable security for sharing PHR in the Internet of Medical Things (IoMT) environment. Second, an Attribute-Based Data Sharing (ABDS) scheme with role delegation has been proposed to share Electronic Health Records (EHR) in a smart healthcare environment. It also provides a hierarchical approach to the treatment of patients in the smart healthcare system. CP-ABE provides better security and efficiency for EHR sharing in a smart environment. The Diffie-Hellman key exchange algorithm is used to share a

delegation among the central hospital authority and doctors. The role delegation technique provides efficient results for performing the treatment of patients in a smart healthcare environment. Therefore, the proposed ABDS scheme is applicable in the smart healthcare system for secure data sharing and role delegation. It is concluded that KP-ABE and CP-ABE are applied in the smart healthcare environment to achieve medical data security for IoT devices connected to the smart healthcare environment.

The methodologies proposed in this thesis have the potential to achieve security in an IoT environment while enabling new applications. We have explored KP-ABE and CP-ABE schemes based on ECC in order to use them in an IoT environment. The decryption overhead of ABE schemes has been reduced by outsourcing the decryption process. A hybrid approach also reduces the computational overhead as compared to other existing works.

The techniques described in this thesis have been implemented on the Anaconda platform using Python programming. Some of them are implemented using the charm framework. The effectiveness of the proposed techniques has been compared with existing and state-of-the-art methods in this field. The proposed methodologies are novel and superior to existing ones in terms of computational and communicational overheads. Still, there is scope for considering new applications of attribute-based encryption in the Internet of Things while reducing the communicational and computational overhead for IoT devices in the IoT environment.