CHRIST
(DEEMED TO BE UNIVERSITY)
BANGALORE · INDIA

Notice for the PhD Viva-Voce Examination

Ms Ancy P R (Registration Number: 1870078), PhD scholar at the School of Engineering and Technology, CHRIST (Deemed to be University), Bangalore will defend her PhD thesis at the public viva-voce examination on Saturday, 14 December 2024 at 11.00 am in Conference Room, Block I, Bangalore Kengeri Campus, Bengaluru 560074.

Title of the Thesis	:	**A Revocable Multi-Authority Attribute Based Encryption Scheme Based on Nonlinear Access Policy**
Discipline	:	**Computer Science and Engineering**
External Examiner - I	:	**Dr Sandeep Singh Rawat** Professor Room No. 122, C-Block New Academic Complex School of Computer and Information Sciences IGNOU, Maidan Garhi New Delhi - 110068
External Examiner – II	:	**Dr Anil Kumar** Professor Department of Analytics School of Computer Science & Engineering Vellore Institute of Technology, Vellore Tamil Nadu - 632014
Supervisor	:	**Dr Addapalli V N Krishna** Professor Department of Computer Science and Engineering School of Engineering and Technology CHRIST (Deemed to be University) Bengaluru – 560074 Karnataka

The members of the Research Advisory Committee of the Scholar, the faculty members of the Department and the School, interested experts and research scholars of all the branches of research are cordially invited to attend this open viva-voce examination.

Registrar

Place: Bengaluru
Date: 09 December 2024

ABSTRACT

Due to the tremendous increase of data, currently individuals and organizations are increasingly opting to store their data with third-party providers as a solution to their storage issues. Ciphertext Policy Attribute Based Encryption facilitates data outsourcing by encrypting the data at the source and uploading it to a third-party storage provider with some restricted access which is mentioned using access policy. In classical Identity-based Encryption (IBE), when a data owner needs to transmit a message to a data user, they would send it together with the data user's specific identity, such as their email address. This ensures that only the intended recipient can access and read the message. The primary issue is that the data owner must possess knowledge of the identity of each user. Other than the traditional IBE, a data owner can utilize attribute-based encryption to deliver a message to a group of individuals who have the same attributes. Here, the data owner does not need to be aware of every user's identity; instead, he can send messages using the attributes and access policies that have been provided, such as which users can access this message.

This research work primarily focuses on three CP-ABE aspects: access policy, number of attribute authority, and revocation. The current access policies are insecure due to their linear character, as they always calculate shares using the same linear equation. For this particular issue in this work, a non-linear secret sharing model that enhances the security of the model is proposed. For addressing the key escrow problem, a solution using multiauthority systems were introduced. These systems involve multiple attribute authorities, each responsible for holding a specific subset of attributes for each user. And access policy will be based on non-linear secret sharing scheme. In the third aspect related to revocation, this work has addressed both user and attribute revocation so that it will make this model a perfect implementation model in terms of improved security. Some of the existing approach for revocation are re-encryption, periodic updating of ciphertext instead this work used a polynomial called Lagrange polynomial which helps to address this problem in less complex and more efficient way. These features will make the proposed scheme a real model that is secure and can be implement in any organization.

Keywords: Access policy; Multi-Authority Ciphertext policy attribute-based encryption; Elliptic curve cryptography; Lagrange interpolation; Revocation.

Publications:

1. **Ancy. P. R** and A. V N Krishna, "An Efficient Nonlinear Access Policy Based on Quadratic Residue For Ciphertext Policy Attribute Based Encryption," *Journal of Theoretical and Applied Information Technology*, vol. 15, no. 21, 2021
2. **Ancy. P. R**, A. V N Krishna, Balachandran K, Balamurugan M "An Efficient Access Policy With Multi-Linear Secret-Sharing Scheme in Ciphertext-Policy Attribute-Based Encryption," *Journal of Theoretical and Applied Information Technology*, vol. 15, p.1404-1411. 2022
3. **P. R. Ancy** and A. V. N. Krishna, "Machine Learning Techniques for Resource-Constrained Devices in IoT Applications with CP-ABE Scheme," *Congress on Intelligent Systems,* Springer Nature Singapore, pp. 557–566, 2023.
4. V N Krishna and **Ancy. P. R**, "Revocable and Secure Multi-Authority Attribute- Encryption Scheme", International Journal of Intelligent Systems And Applications In Engineering, vol. 11, pp.52-58,2023
5. V. N. Krishna and **P. R. Ancy**, "Security Analysis for a Revocable Multi-Authority ABE-Attribute-Based Mechanism," *SSRG International Journal of Electronics and Communication Engineering*, vol. 11, no. 3, pp. 24–30, 2024