Proceedings of the International Conference on Industrial Engineering and Operations Management
Bangkok, Thailand, March 5-7, 2019

Privacy and Security aware Cryptographic Algorithm for Secure Cloud Data Storage

B.Muthulakshmi
Department of Computer Applications
Kalasalingam Academy of Research and Education
Anand Nagar, Krishnankoil-626126
selvamayil2010@gmail.com

M.Venkatesulu
Department of Information Technology
Kalasalingam Academy of Research and Education
Anand Nagar, Krishnankoil-626126
venkatesulum2000@gmail.com

Abstract

Cloud computing is an effective framework to enable on demand network access for sharing configurable computing resources such as applications, network, servers, services, and storages. Cloud technology offers the users to store and retrieve their data easily in a remote manner. However, privacy and security are considered as the most challenging concerns in cloud data storage. In this paper, a novel Privacy and Security aware Cryptographic Algorithm (PSCA) for data storage is proposed which is based on Invertible Non-linear Function (INF). In proposed technique, the encrypted data is only stored at the cloud storage without key and the encryption is done by the data authorities who also secure the decryption key. The end user has to send request to the data authority and after all verification process the encrypted data is given and with the obtained key and the knowledge of inverse INF the decryption is performed. Thus, both the internal and external attacks are avoided and its detailed analysis is given in the proposed security evaluation. In experimental results, the file size is plotted against encryption time, decryption time, uploading time, and downloading time respectively. The observed results are plotted and the proposed technique is compared with the existing AES and RSA techniques. From the results, it is observed that the proposed PSCA has better performance in terms of reduced time in all four parameters.

Keywords
Cloud computing, Privacy and Security, Cloud Service Provider, Data Authority, End User.

Acknowledgements
The first author is thankful to Kalasalingam Academy of Research and Education for supporting the research work.

Biographies
B.Muthulakshmi is a research scholar in Kalasalingam Academy of Research and Education. She received her Bachelor as well as Master degrees from Madurai Kamaraj University. Her area of interests are Cloud Computing Cryptography and Data Security.

M.Venkatesulu received the postgraduate degree in Mathematics from Sri Venkateswara University, Tirupati, India, in 1975, and the Ph.d degree in mathematics from Indian Institute of Technology, Kanpur, India, in 1979. He

worked as a faculty member at Shri Sathya Sai University, Prashanthinilayam, India Between 1983 and 2003. He also worked as a consultant for Satyam Computers, Hyderabad, India, for short period. He was Visiting Professor at University of Missouri, Kansas City, between August 2006 and May 2007. Currently he is working as a Senior Professor and Head of the Department of Information Technology at Kalasalingam University, Krishnankovil, Srivilliputtur, Tamil Nadu, and India. His area of interest includes differential equation, Image Processing, Cryptography, Bioinformatics, Big Data Analytics and Distributed Computing.