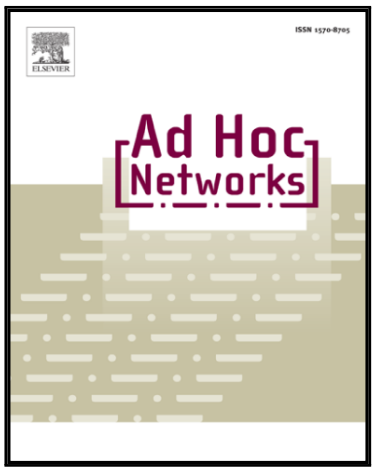

An Efficient Queries Processing Model Based on Multi Broadcast Searchable Keywords Encryption (MBSKE)

Belal Ali Al-Maytami , Pingzhi Fan , Abir Jaafar Hussain , Thar Baker Shamsa , Panos Liatsis

PII: S1570-8705(19)30588-8
DOI: https://doi.org/10.1016/j.adhoc.2019.102028
Reference: ADHOC 102028

To appear in: *Ad Hoc Networks*

Received date: 22 June 2019
Revised date: 29 September 2019
Accepted date: 15 October 2019

Please cite this article as: Belal Ali Al-Maytami , Pingzhi Fan , Abir Jaafar Hussain , Thar Baker Shamsa , Panos Liatsis , An Efficient Queries Processing Model Based on Multi Broadcast Searchable Keywords Encryption (MBSKE), *Ad Hoc Networks* (2019), doi: https://doi.org/10.1016/j.adhoc.2019.102028

An Efficient Queries Processing Model Based on Multi Broadcast Searchable Keywords Encryption (MBSKE)

Belal Ali Al-Maytami[1], Pingzhi Fan[1], Abir Jaafar Hussain[2], Thar Baker Shamsa[2] and Panos Liatsis[3]

[1] Institute of Mobile communication, Southwest Jiaotong University, Chengdu, China
[2] Liverpool John Moores University, Department of Computer Science, Liverpool, L33AF, UK
[3] Department of Electrical Engineering and Computer Science, Khalifa University of Science and Technology, Abu Dhabi, UAE

Abstract

Cloud computing is a technology which has enabled many organizations to outsource their data in an encrypted form to improve processing times. The public Internet was not initially designed to handle massive quantities of data flowing through millions of networks. Thus, the rapid increase in broadcast users and growth in the amount of broadcasted information leads to a decrease in the speed of sending queries and receiving encrypted data from the cloud. In order to address this issue, Next Generation Internet (NGI) is being developed, capable of high speeds, while maintaining data privacy. This research proposes a novel search algorithm, entitled Multi-broadcast Searchable Keywords Encryption, which processes queries through a set of keywords. This set of keywords is sent from the users to the cloud server in an encrypted form, thus hiding all information about the user and the content of the queries from the cloud server. The proposed method uses a caching algorithm and provides an improvement of 40% in terms of runtime and trapdoor. In addition, the method minimizes computational costs, complexity, and maximizes throughput, in the cloud environment, whilst maintaining privacy and confidentiality of both the user and the cloud. The cloud returns encrypted query results to the user, where data is decrypted using the user's private keys.

Keywords: Data encryption, Cryptography, Coding and information theory

1. INTRODUCTION

Cloud services based on cloud servers gained major popularity in recent years. Benefits of cloud servers include scalable and elastic storage and computation resources through the internet to users. One of the main features of outsourcing data services is that cloud infrastructures are physically hosted and maintained by the cloud servers to reduce risk and hide information [1]. Cloud computing and Next Generation Internet (NGI) are still concerned with security of personal data and transparency. Moreover, they aim to provide better services and greater data sharing. At present, the focus is on designing a new form of internet, re-designing and re-engineering the procedures of transparency, privacy, cooperation, and protection of data.

Research into NGI can be summarized in two broad areas. The first focus area relates to the Internet inter-networking core, which includes architectural innovations addressing the fundamental issues of inter-domain routing