Accepted Manuscript

Secure policy execution using reusable garbled circuit in the cloud

Masoom Alam, Naina Emmanuel, Tanveer Khan, Abid Khan, Nadeem javaid, Kim-Kwang Raymond Choo, Rajkumar Buyya

PII: S0167-739X(17)31527-3
DOI: https://doi.org/10.1016/j.future.2017.12.067
Reference: FUTURE 3905

To appear in: *Future Generation Computer Systems*

Received date : 11 July 2017
Revised date : 16 October 2017
Accepted date : 31 December 2017

Please cite this article as: M. Alam, N. Emmanuel, T. Khan, A. Khan, N. javaid, K.R. Choo, R. Buyya, Secure policy execution using reusable garbled circuit in the cloud, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2017.12.067

Secure Policy Execution using Reusable Garbled Circuit in the Cloud

Masoom Alam, Naina Emmanuel, Tanveer Khan, Abid Khan, Nadeem javaid, Kim-Kwang Raymond choo, *Senior Member, IEEE*,, Rajkumar Buyya, *Fellow, IEEE*

***Abstract*—While cloud computing is fairly mature, there are underpinning data privacy and confidentiality issues that have yet to be resolved by existing security solutions such as cross domain access control policies. The latter necessitates the sharing of attributes with a Trusted Third Party (TTP), which in turn raises data privacy concerns. In this paper, we present a Privacy Aware Cross Tenant Access Control (PaCTAC) protocol for cross domain cloud users, based on reusable garbled circuit. We also propose the concept of a privacy aware Cloud Policy Decision Point (CPDP) that can be offered by cloud service providers. CPDP plays the role of a trusted third-party among its different tenants. We then formally specify PaCTAC to demonstrate its security.**

***Index Terms*—Cross tenant access control, Formal specification, Cloud computing, Reusable garbled circuits**

I. Introduction

Cloud computing has been the subject of active research and innovation in both academia and industry in the last decade [1], [2], as evidenced by the continuing interest in designing secure and efficient solutions for different cloud computing applications and scenarios. For example, cloud service providers (CSPs) have been working collaboratively with researchers to design solutions that allow cloud users to access the resources of the host CSP, as well as those of a collaborative CSP, efficiently and securely. Such collaboration allows the cloud computing and related industries to offer more sophisticated and advance services. However, such a collaborative distributed environment complicate efforts to ensure the privacy of data, services and infrastructure. One particular research direction is to design efficient techniques to preserve user privacy from (honest-but-curious or malicious) CSPs. Encryption for data-at-rest technique is an effective approach [3], but this limits the capability to provide other services. For example, how to effectively search on encrypted data remains a topic of ongoing research at the time of this research [4], [5].

Achieving fine-grained and flexible access control is also another topic that is being explored in the literature, such as the scheme reported in [6]. The general requirement is for both the service provider and the data owner to be in the same trusted environment, which is not usually the case in practice. Presently, single sign-on methods are being used by CSPs to provide authentication and simple authorization in a collaborative cloud environment; however, fine grained authorizations are not fully supported. Role Based Access Control (RBAC) has been used in many diverse applications. However, RBAC does not support the extent of collaboration required by contemporary multi-tenant cloud computing environment. Unsurprisingly, the RBAC model has been extended in the literature in order to achieve effective access control in a collaborative environment [7], [8]. However, these extended models require the existence of a centralized authority. In a collaborative cloud computing deployment where users are from different independent administrative domains, such a requirement may not be realistic. Electronic Health Record (EHR) is used to share health information via a cloud-based platform. However, data shared over the or stored in the cloud may be targeted by cyber criminals to violate a patient's privacy [9]. Existing privacy protection techniques can be broadly categorized into the following domains: privacy by cryptography, privacy by statistics, and privacy by police [10]. A number of (practical) solutions for EHR sharing have also been proposed in the literature, such as those that rely on a classification of the patient's attributes.

In this paper, we introduce the concept of secure policy execution in the cloud using a Reusable Garbled Circuit (RGC). RGC-based techniques allow computation to be performed over encrypted data, and include fully homomorphic encryption technique [11–13], functional encryption technique [14], [15], and attribute based encryption technique [13], [16–18]. In 2013, Goldwasser *et al*. [13] proposed a RGC using fully homomorphic encryption techniques. Another recent RGC-based approach is presented by Wang *et al*. [18] in 2016, who use random linear coding. In our protocol, the approach of Wang *et al*. [18] is used for garbling the policy. We remark that there has been no practical implementation of RGC on multi-party policy execution environment in the literature, at the time of this research. Also, in this paper, we construct the Privacy Aware Cross Tenant Access Control (PaCTAC) protocol for cross domain users. The protocol achieves secure policy execution and its storage at a privacy aware Cloud Policy Decision Point (CPDP) that can be offered by cloud service providers. In a typical RBAC scheme, if the centralized authority acts maliciously then the security of the system would be compromised. Thus, we propose a garbling scheme to act as roles under a secure manner in the untrusted

Masoom Alam, Naina Emmanuel, Tanveer Khan, Abid Khan, Nadeem javaid are with Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan

Kim-Kwang Raymond Choo is with the Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249 USA (e-mail: raymond.choo@fulbrightmail.org).

Rajkumar Buyya is with *Cloud Computing and Distributed Systems (CLOUDS) Laboratory, School of Computing and Information Systems, The University of Melbourne, Australia.*