ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing

[1] Ch.Mounika, [2] N.Koteswar Rao, [3] P.Priya, [4] R.Bhargavi, [5] V.G.Kanya
[2] Associate professor
[1][2][3][4] Narayana Engineering College, Gudur

Abstract: Privacy has become a considerable issue when the applications of big data are dramatically growing in cloud computing. The benefits of the implementation for these emerging technologies have improved or changed service models and improve application performances in various perspectives. However, the remarkably growing volume of data sizes has also resulted in many challenges in practice. The execution time of the data encryption is one of the serious issues during the data processing and transmissions. Many current applications abandon data encryptions in order to reach an adoptive performance level companioning with privacy concerns. In this paper, we concentrate on privacy and propose a novel data encryption approach, which is called Dynamic Data Encryption Strategy (D2ES). Our proposed approach aims to selectively encrypt data and use privacy classification methods under timing constraints. This approach is designed to maximize the privacy protection scope by using a selective encryption strategy within the required execution time requirements. The performance of D2ES has been evaluated in our experiments, which provides the proof of the privacy enhancement.

INTRODUCTION

Introducing mobile cloud computing techniques has empowered numerous applications in people's life in recent years [1], [2]. Involving humans in the cloud computing and wireless connection loops becomes an alternation for information retrieval deriving from observing humans' behaviors and interactivities over various social networks and mobile apps [3]– [6]. Moreover, as an emerging technology, cloud computing has spread into countless fields so that many new service deployments are introduced to the public [7], such as mobile parallel computing [8], [9] and distributed scalable data storage [10]. Penetrations of big data techniques have further enriched the channels of gaining information from the large volume of mobile apps' data across various platforms, domains, and systems. Being one of technical mainstreams has enabled big data to be widely applied in multiple industrial domains as well as explored in recent researches.

Despite many benefits. This paper is an extended work of our research and prior work [16] focused on the general data encryption strategy of big data in cloud systems. Compare with our prior work, the crucial added value of this work is to improve the implementation adaption of the proposed approach by further solidifying the details of the mechanism. Our previous work [16] mainly represent the operating principle of the dynamic data encryption strategy and the implementation algorithm. In this paper, we have extended our work by enriching the mechanism design for each specific mode phase. Two crucial terms are designed for implementing the data encryption strategy, which includen Paired Data and Pairs Matching Collision. In addition, two crucial algorithms are proposed for supporting the implementation of D2D algorithm, which are Weight Modelization (WM) Algorithm and S Table Generation (STG) Algorithm. These two new algorithms further identify the methods of identifying privacy values when making a determination on encrypting the input data.

RELATED WORK

Mobile cloud is an inter-connective platform for mobile users, which supports information sharing among multiple parties across distinct infrastructure. Wireless communications between users usually carry personal information through a variety of channels, including social networking sites and infrastructure.

Securing data management, storage, and transmissions are three crucial aspects that have been explored in the prior researches. First, researches addressing the attacks in social networks have been paid attention by many scholars. Zhang et al. [17] proposed an approach named SCLPV for cloud-based Cyber Physical Social Systems (CPSS) to avoid malicious auditors.

This approach concurrently provisioned certificateless public verification as well as resistance against malicious auditors for the purpose of verifying the integrity of outsourced data in CPSS. Wang et al. [18] focused on

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

developing an approach offering a secure cloud system that could support privacypreserving public auditing. These research had explored the method of defining adversaries from the data storage side. However, the threats in the data transmissions were not addressed so that this type of solution might result in privacy leakages before the auditing operations.

CONCEPTS AND THE PROPOSED APPROACH

3.1 Problem Definition

We describe the main research problem in this section. Definition
The identified research problem that is Maximum Data Package under Timing Constraints (MDPuTC) problem. Definition 3.1. Maximum Data Package Under Timing Constraints (MDPuTC) Problem: Inputs: data package types fDig, the number of data for each data package type NDi , execution time when encrypting data for each single data TeD execution time without encryptions for each single data TnD the privacy weight value for each data type WDi . Outputs: a strategy determining which data will be encrypted. The proposed problem is finding out the approach that can gain the maximum total privacy weight value under a given timing constraint. As illustrated in Definition 3.1, the main inputs include five variables. First, input data include a group of packages that are classified into different types, represented as a set fDig. The number of data packages in each type Di is represented as NDi . Moreover, there are two kinds of execution modes, which include Operation with Encryptions (OwE) and Operation with Non-Encryption (OwNE). The execution time of each data package Di in OwE mode is TeD
i . Similarly, the execution time of each data package Di in OwNE mode is TnD
i . Furthermore, we introduce a parameter, Privacy Weight Value (PWV), for each data package type in order to calculate the beneficial acquisitions from encrypting data, represented as WDi .

The meaning of PWV is a criterion showing security significance levels. The acquisitions of PWV values that categorize security issues into multiple levels can be gained by various approaches, such as scorecard sheet [31], [32] and security measurement category [33]. In our proposed model, the PWV value represents the privacy importance for each data package. Therefore, the output is a encryption strategy that determines which data packages should be encrypted. Assume that the number of encrypted data packages for Di is NeD The object of our research problem is maximizing the sum of PWV values and the objective function is expressed in Eq. (1). In the function, we create a binary function s(i) to represent the selection. The encryption strategy is selected when s(i) = 1 and a non-encryption strategy is selected when s(i) = 0. Since unencrypted data packages do not earn any privacy weights, only encrypted data packages are counted in our model.

$$\text{Output} = \text{Max}(Xs(i)=1(\text{NeDi\_WDi})) = P \quad (1)$$

The condition is the total execution time is no longer than the required timing constraint Tc. The length of Tc must satisfy the following requirement, as shown in Eq. (2). The expression shows the minimum execution time of data operations, which excludes all encryptions.

Weight Modelization (WM) Algorithm

The WM algorithm is developed for modifying M Table using weight values. The purpose of this algorithm is to check whether a data package is a must-encrypted objective, when considering the relations between packages. Thus, the pairs matching collisions (Definition 3.3) are applied in this algorithm in order to detect the paired data (Definition 3.2). Inputs include an M Table and a Co-Table. The output of this algorithm is a modified M Table, which is represented as an M-Table'. MTable' is an input for both Algorithms 5.1 and 5.3. Moreover, a Co-Table refers to a table mapping all paired data, which is pre-defined by security policies or developers. The Co-Table is used to manipulate pairs matching collisions. Algorithm 5.2 presents the pseudo codes of WM algorithm.

CONCLUSIONS

This paper focused on the privacy issues of big data and considered the practical implementations in cloud computing. The proposed approach, D2ES, was designed to maximize the efficiency of privacy protections. Main algorithm supporting D2ES model was DED algorithm that was developed to dynamically alternative data packages for encryptions under different timing constraints. The experimental evaluations showed the proposed approach had an adaptive and superior performance.

REFERENCES

[1] S. Yu, W. Zhou, S. Guo, and M. Guo. A feasible IP traceback framework through dynamic deterministic

packet marking. IEEE Transactions on Computers, 65(5):1418–1427, 2016.

[2] S. Yu, G. Gu, A. Barnawi, S. Guo, and I. Stojmenovic. Malware propagation in large-scale networks. IEEE Transactions on Knowledge and Data Engineering, 27(1):170–179, 2015.

[3] S. Liu, Q. Qu, L. Chen, and L. Ni. SMC: A practical schema for privacy-preserved data sharing over distributed data streams. IEEE Transactions on Big Data, 1(2):68–81, 2015.