Privacy-Preserving Data Encryption Strategy

[1] Bairysetti prasad babu
[1] Assistant.professor ,Department of computer science and engineering. Ramachandra College Of Engineering. Eluru.

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.

Index Terms—Privacy-preserving, data encryption strategy, big data, mobile cloud computing, cybersecurity F

INTRODUCTION

Introducing mobile cloud computing techniques has empowered numerous applications in people's life in recent years. 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. Moreover, as an emerging technology, cloud computing has spread into countless fields so that many new service deployments are introduced to the public, such as mobile parallel computing and distributed scalable data storage. 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 of using mobile cloud computing, there are great concerns in protecting data owners' privacy during the communications on social networks or mobile apps. Despite many benefits of using mobile cloud computing, there are great concerns in protecting data owners' privacy during the communications on social networks or mobile apps. One of the privacy concerns is caused by unencrypted data transmissions due to the large volume of data. Considering an acceptable performance level, many applications abandon using cipher texts in mobile cloud data transmissions. This phenomenon can result in privacy leakage issues since plain texts are unchallenging for adversaries to capture information in a variety of ways, such as jamming, monitoring, and spoofing. This privacy issue is exigent because it faces to a contradiction between the security levels and performance that is usually attached to timing constraints.Fig. 1: High level architecture of mobile cloud computing illustrating the balance between privacy protection and transmission efficiency. This paper addresses the issue of contradictions between data transmission efficiency and protection. To solve the problem, we propose a novel approach that selectively encrypts data in order to maximize the volume of encrypted data under the required timing constraints. The proposed model is calle Dynamic Data Encryption Strategy (D2ES) model, which is designed to protect data owners' privacy at the highest level when using the applicable devices and networking facilities. Fig. 1 shows the high level architecture of mobile cloud with the illustrations of addressing the privacy protections.

The crucial issue is that most contemporary wireless transmissions carry plain-texts due to the workload volume and real-time service concerns. The implementation of big data further stops transmission from carrying cipher texts. The target protection location is represented by the broken-line box in the figure, which depicts that the data transmissions between physical infrastructure and mobile computing in mobile cloud need to be protected. Two major techniques used in D2ES are: (1) classifying data packages according to privacy level and (2) determine whether data packages can be encrypted under the timing constraints. We design and propose an algorithm, Dynamic Encryption Determination (DED) algorithm, which relies on the timing constraints and facilities' capacities to determine the data encryption alternatives. Detailed descriptions of D2ES are given in

Section 3. This paper is an extended work of our research and prior work 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 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 include 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.

Descriptions of these two algorithms are stated in Section 5.2 and 5.3. Moreover, our research is significant for generating an adoptive solution to protecting data owners' privacy. The main contributions of this work are threefold: 1) This work proposes a novel approach that selectively encrypts data packages to maximize the privacy protection level under timing constraints in big data. Two working modes are considered when creating the transmission strategy, including encryption and non-encryption modes. 2) The proposed algorithm offers an optimal solution providing the maximum value of total privacy weights. Research problem and describes operating principle of D2ES. Next, Section 4 provides a motivational example explaining the mechanism of the proposed approach in the given operating scenario. In addition, Section 5 illustrates the main algorithm designed for supporting D2ES. Furthermore, our experimental configurations as well as a few experimental results are given in Section 6. Finally, conclusions are drawn in Section 7.

involved constraints are execution time and privacy levels. 3) The findings of this research provide big data-based solutions with an adaptive transmission approach focusing on protecting privacy. The proposed method can be also implemented in the distributed storages in cloud computing. The rest of this paper is organized by the following order: Section 2 displays a summary of related research work in CPSS as well as its privacy issues. Section 3 defines the main

CONCEPTS AND THE PROPOSED APPROACH

3.1 Problem Definition

We describe the main research problem in this section. Definition 3.1 shows 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 i , execution time without encryptions for each single data TnD i , 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.

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. IEE 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.