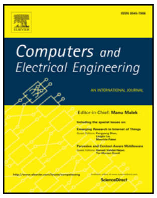
Computers and Electrical Engineering 000 (2017) 1–18

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng



Shifted Adaption Homomorphism Encryption for Mobile and Cloud Learning[☆]

G. Kalpana[a], P.V. Kumar[b], Shadi Aljawarneh[c,*], R.V. Krishnaiah[d]

[a] Computer Science & Engineering Department, DRK Institute of Science & Technology, Hyderabad 500085, India
[b] Computer Science & Engineering Department, Osmania University, Hyderabad 500007, India
[c] Software Engineering Department, Faculty of Computer and Information Technology, Jordan University of Science and Technology, Irbid, Jordan
[d] Computer Science & Engineering Department, Institute of Aeronautical Engineering, Hyderabad 500043, India

ARTICLE INFO

Article history:
Received 27 December 2016
Revised 18 May 2017
Accepted 19 May 2017
Available online xxx

Keywords:
Mobile and Cloud Learning
Public key
Shared key
Homomorphic Encryption
Inverted or reversed

ABSTRACT

Mobile learning when stored in a cloud server allows contents to be gathered and accessed using mobile devices connected with the cloud. The present problems of limited computing capacity and small space for storage in mobile phones has inspired the blend of mobile learning and cloud computing. This paper primarily focuses on Homomorphic Encryption to achieve privacy over encoded data or search the encrypted information, which is the current research area of majority of the knowledge experts. In this paper, we suggest Shifted Adaption Homomorphism Encryption (SAHE), which is regarded as the better option for all the current research going on. SAHE implements the smallest public key of 32 bit and is able to encrypt integer and real numbers. A major issue in this field of research is difficulty in protecting user's questions, which is addressed by conceiving a public key encryption technique which is based on the reversed index. Our schema preserves search efficiency using inverted index, by solving one time only search drawback encountered in earlier research works. This method is appropriate for mobile learning since the suggested algorithm will not use the mobile memory or power.

1. Introduction

In the current computing age, the cloud computing is a great area to conduct research, wherein the user can have access to cloud data in a protected form. Many researchers have recommended various algorithms dependent on Homomorphic Encryption (HE).

The communication tools which are in popular use are big data, social media and cloud computing. The progress in the field of smaller PDAs and devices capable of Internet made it possible to concentrate on the Cloud Mobile Learning via mobile devices. The drawbacks of mobile learning using cloud computing are in terms of low rate of network transmission, limited capacity for storage and its security problems.

This paper talks about the Shifted Adaption Homomorphism Encryption (SAHE) which has a central method based on the HE algorithm. It has become an appealing solution for several present day privacy issues related to cloud computing and

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. R. Varatharajan.

[*] Corresponding author.

E-mail addresses: kalpanamscis@gmail.com (G. Kalpana), pvkumar58@gmail.com (P.V. Kumar), saaljawarneh@just.edu.jo, saljawarneh@acm.org (S. Aljawarneh), r.v.krishnaiah@gmail.com (R.V. Krishnaiah).

http://dx.doi.org/10.1016/j.compeleceng.2017.05.022
0045-7906/© 2017 Elsevier Ltd. All rights reserved.

the applications executed on it as a part or whole. In SAHE, the support of numerical Homomorphic Encryption technique allows to perform infinite additions and multiplications on information which yields to the cipher text or C_{Text} by which the procedure attains the power to helically calculate in general any function on the encoded data [1–3].

In Gentry's FHE [1,2] study, the process starts with the development of Somewhat Homomorphic Encryption (SHE) where additions and only a few multiplications are allowed. The next stage is to squash the function of decryption and finally get the plaintext via bootstrapping. It can be determined simply that it is not practically useful due to its large computational complexities encountered in processing of plain text and cipher text [4–6,8].

The process of utilisation of data is regarded as one of the major issues of the data encryption procedure. The researchers of cloud computing proposed a few measures in the procedure of data utilisation, that is, first download the whole encrypted information set and then begin search in decrypted information. However, this is not accepted by majority of the experts as it needs more computations and low use of communication media and resources [21,22].

Another problem in cloud data availability with a cloud owner is that when he/she desires to check the information, they may obtain it without user's knowledge and start executing various decryption algorithms, which may fail or succeed. Therefore, the data in the cloud may be considered to be at risk. In order to protect user data, SAHE preserves it blindly and it becomes tough to know if the data is provided by the cloud or not. The data in Blind Storage is randomly stored. In Blind Storage, the address of the location is generated with the hash function. Using this blind storage process, the information is safe and it is not known by anyone where actually the data is stored.

The Boolean function is devised in a secured way, where we conduct a round operation and generation of quotient on test values, given by X_1 and X_2, which are arbitrary values in real or integer form, denoting the set A. Therefore, we suggest a novel process for trapdoor generation where the query acquires the inverted list of data being demanded and handles all kinds of guessing attacks. Private and secure data matching is accomplished using the infused query trapdoor.

Our contributions to this research are:

(1) Practical shifted and reversed index based public key searchable encoding scheme is suggested which overcomes the drawback of one time only search. It can be done by executing multi-keyword conjunctive search, which uses the single trapdoor approach.
(2) We have developed a probabilistic Blind Storage algorithm to prevent the data leakability of cloud by maintaining the index and trapdoor privacy. This technique guarantees robust security for execution of the transfer protocol that has a tendency to hide the patterns of access.
(3) We evaluated existing encryption schemes based on public key that conducts search and executes hardbound pairing operations, and confirmed that our schema is superior in implementation.
(4) This paper also offers the theoretical assessment and a simulation-based research in the academic environment dataset. Moreover, to evaluate the obtained performance and verify the acquired results, the scheme is executed using MATLAB.

The remaining portion of this paper is organised as follows: Section 2 talks about the review of associated work on Homomorphic Encryption techniques in cloud storage. Section 3 describes preliminaries and formal terms. Construction of our method is given in Section 4. Section 5 explains cloud storage structure and arrangement of file blocks. Thorough description, implementation and assessment of SAHE are included in Section 6. Section 7 introduces the Avalanche effect and analyses the performance of SAHE. We wrap this paper up with a relevant conclusion in Section 8.

2. Related work

The notion of Homomorphic Encryption (HE) was initially proposed by Ronald Rivest, Leonard Adleman and Michael Dertouzos in 1978 [1]. Many researchers have performed research on this technique since the last 30 years. In 1982, Shafi Goldwasser and Silvio Micali suggested a provable scheme for security encryption, which was a huge success in the field of privacy but it encrypts each of the bits individually in plain text (a single bit at a time). In 1999, Pascal Paillier recommended a provable scheme for security encryption which is derived from additive homomorphic encryption.

In 2005, researchers Dan Boneh, Eu Jin Goh and Kobi Nissim suggested a proven scheme for security encryption, which performs infinite additions with just one multiplication.

In [2,3], the cloud computing methodology based on encryption has been suggested for fine grained access protocol that manages all the encrypted data. These techniques are based on Access Control Policies (ACPs) and information is encrypted with distinct symmetric keys. Every user is provided with one key for encryption and decryption so as to reduce the number of keys to be provided. Users were exploited with hierarchical and other relationships amid data items, which have multiple drawbacks.

In reference [7] Schlitter proposed the concept of horizontal slicing technique for privacy maintenance based on the scheme of BPN network learning. It allows two or more number of users to perform learning process without revealing their identity and corresponding private datasets. The proposed technique only tackles the horizontal partitioned information and this will not secure the intermediate results. This technique may expose sensitive information in between the learning process.

In reference [9], Chen and Zhong suggested a vertical approach for maintenance of privacy using Back Propagation Network (BPN)-based network learning technique for dual user scenarios. This technique provides strong security for all the

Please cite this article as: G. Kalpana et al., Shifted Adaption Homomorphism Encryption for Mobile and Cloud Learning, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.05.022