Resource Allocation of Virtual Machine in Cloud Fog Using Hash Algorithm

Ramathilagam A
Department of Computer Science Engineering
P.S.R.Engineering College, Sivakasi, India

Sheirly Twinkle C
Department of Computer Science Engineering
P.S.R.Engineering College, Sivakasi, India

Ramani R
Department of Computer Science Engineering
P.S.R.Engineering College, Sivakasi, India

Thiruselvan P
Department of Computer Science Engineering
P.S.R.Engineering College, Sivakasi, India

Abstract

Cloud computing is used as a potential substitute for catering storage service in the field of computer science and information technology. But at the same time security concerns of cloud storage are the potential threats in its widespread implementation. Privacy breach, malicious variation and data losses are the few emerging cyber threats against cloud storage. Nowadays, fog server based three-layer architecture is used for safe storage employing multiple clouds. The Hash-Solomon code and customized hash algorithm are used in order to attain the goal. However, it resulted in loss of lesser percentage of data to cloud servers and failed to offer enhanced modification detection and data recoverability.

Keywords: Cloud Computing, Fog Server, Hash Algorithm

I. Introduction

Recently, cloud computing has become an increasingly popular service for its flexibility and scalability, which motivates many organizations, institutions and companies to prefer to outsource data services to cloud platform [1]. At the same time, much attention has been paid to cope with the special security and privacy problems in outsourced cloud [2], [3]. On one hand, to protect the data confidentiality, the data owner (DO) encrypt the sensitive information of his outsourced data, such as income level, health records, personal photos before the dataset is uploaded to the cloud [4], [5]. On the other hand, data owner may plan to rely on cloud platform for querying of the datasets stored in cloud, not just for storage and management. Therefore, a large amount of secure schemes has been proposed. The secret keys used by data sources to make names won't be traded to clients for the result affirmation; for the most part, a malicious client with the private keys can plan with the server to change the data and make relating names to mislead distinctive clients. In this paper, we focus on the affirmation of the outsourced figuring over open data streams, while sensitive data protection is outside the degree of our work.

II. Related works

Ramathilagam and Vijayalakshmi [6] have done an extensive review on various algorithms found in literatures to solve scheduling problems in cloud environment. The limitations along with the benefits of those algorithms were also presented. Yan et. al [7], proposed a scheme to deduplicate encrypted data stored in cloud based on ownership challenge and proxy re-encryption. It integrates cloud data deduplication with access control. They evaluated its performance based on extensive analysis and computer simulations. The results show the superior efficiency and effectiveness of the scheme for potential practical deployment, especially for big data deduplication in cloud storage. Yu et.al in their research [8] proposed a propose a dynamic resource allocation strategy to counter DDoS attacks against individual cloud customers. When a DDoS attack occurs, they employed the idle resources of the cloud to clone sufficient intrusion prevention servers for the victim in order to quickly filter out attack packets and guarantee the quality of the service for benign users simultaneously. They established a mathematical model to approximate the needs of our resource investment based on queueing theory. Through careful system analysis and real-world data set experiments, we conclude that we can defeat DDoS attacks in a cloud environment. Priyalatha and Ramathilagam [9] developed a new task scheduling LCGA algorithm in cloud computing environment. This paper focused on task scheduling in hybrid cloud environment with the explicit aim of resource s cost minimization. This goal was achieved by a graph-based task scheduling algorithm which considers resources from both the private clouds and public clouds. The simulation results proved that on average, our algorithm optimizes cost savings better when compared to the other proposed algorithms. Ramathilagam and Vijayalakshmi [10] proposed an improved Artificial Bee Colony (ABC) based on IaaS Cloud Partial Critical Path (IC-PCP) with Replication algorithm to attain the lesser price even as allocating a deadline set by the user in cloud scheduling. The outcome demonstrated the scheduler can discover excellent schedules of deadlines being satisfied and declining the complete execution time of application as the planned cost obtainable for imitation increases.

III. PERTAINING ANTHOLOGIES

The k-nearest neighbors (k-NN) query is a fundamental primitive in spatial and multimedia databases [11]. It has extensive applications in location-based services, classification & clustering and so on. With the promise of confidentiality and privacy, massive data are increasingly outsourced to cloud in the encrypted form for enjoying the advantages of cloud computing (e.g., reduce storage and query processing costs). Recently, many schemes have been proposed to support k-NN query on encrypted cloud data. However, prior works have all assumed that the query users (QUs) are fully-trusted and know the key of the data owner (DO), which is used to encrypt and decrypt outsourced data. The assumptions are unrealistic in many situations, since many users are neither trusted nor knowing the key [12]. The general shortcomings of the existing systems are reportedly; uploading a single data at a given time. Moreover, only a single key for security of each parameter is produced.

IV. PROPOSED SYSTEM

The propose a novel scheme for secure k-NN query on encrypted cloud data with multiple keys, in which the DO and each QU all hold their own different keys, and do not share them with each other; meanwhile, the DO encrypts and decrypts outsourced data using the key of his own. Our scheme is constructed by a distributed two trapdoors public-key cryptosystem (DT-PKC) and a set of protocols of secure two-party computation, which not only preserves the data confidentiality and query privacy but also supports the offline data owner. Our extensive theoretical and experimental evaluations demonstrate the effectiveness of our scheme in terms of security and performance.

Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources. Since an Inter Cloud is a large scale distributed and interconnected computer system, interactions among its sub components (i.e., Clouds) and among stakeholders (i.e., consumers and Cloud providers) can be complex. In an Inter Cloud, computing resources owned and administered by different Cloud providers are pooled to serve multiple consumers, and applications and data are available to and shared by a broad group of cross enterprise and cross platform users. Inter Cloud resource pooling and sharing involve 1) combining resources through cooperation among Clouds, 2) mapping and Scheduling shared resources through coordination, and 3) establishing contracts between Clouds and consumers, and among Clouds through negotiation. There are five modules for the Cloud Computing.

A. User Interface Design

This is the first module of the proposed work. The important role for the user is to move login window to user window. This module has created for the security purpose. In this login page we must enter login user id and password. It will check username and password is match or not (valid user id and valid password). If we enter any invalid username or password we can’t enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters the network. In our project we are using JSP for creating design. Here we validate the login user and server authentication.

B. Block Diagram of the Proposed System

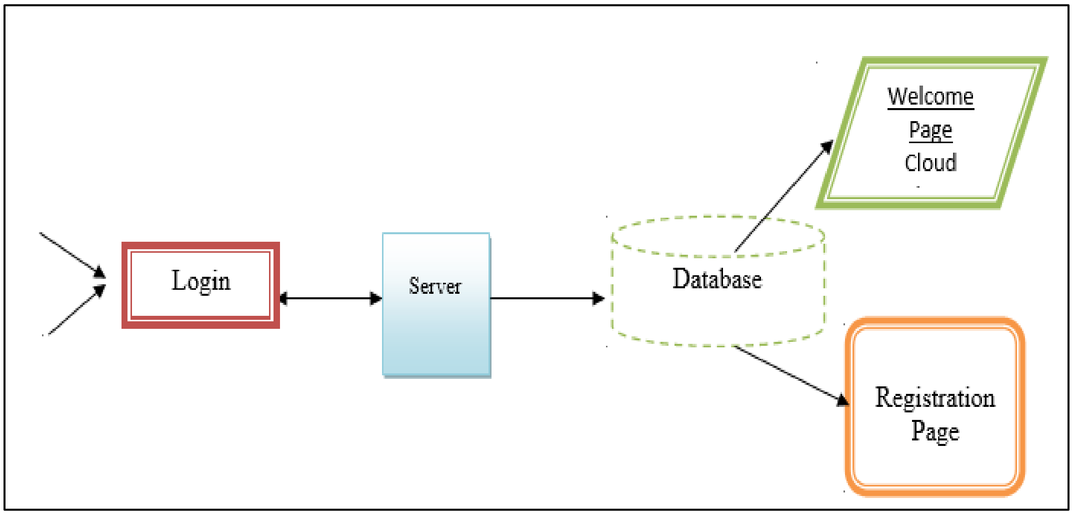
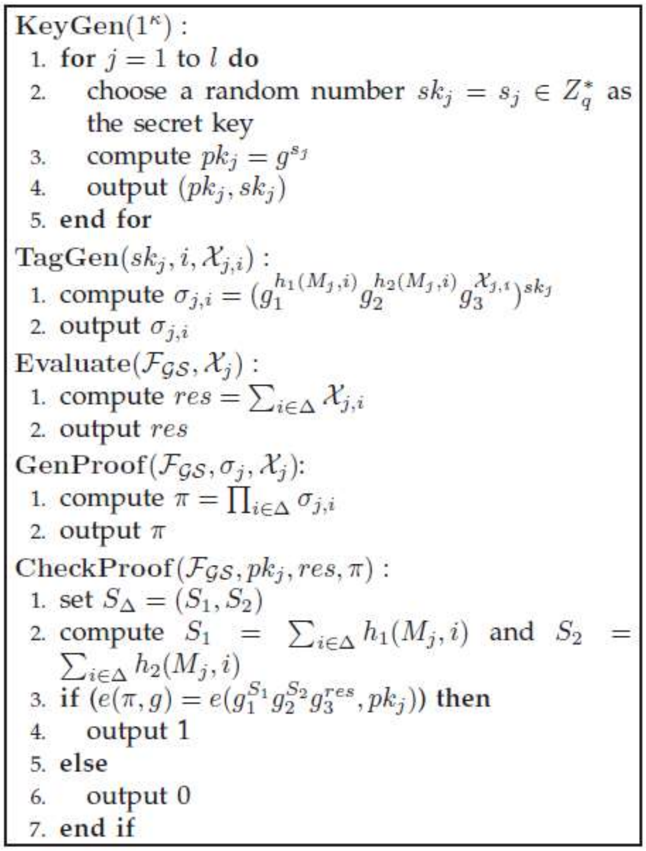


Fig. 1: User Interface Diagram

C. System Methodology



```
KeyGen($1^\kappa$) :
for $j = 1$ to $l$ do
    choose a random number $sk_j = s_j \in Z_q^*$ as the secret key
    compute $pk_j = g^{s_j}$
    output $(pk_j, sk_j)$
end for
TagGen($sk_j, i, \mathcal{X}_{j,i}$) :
compute $\sigma_{j,i} = (g_1^{h_1(M_j,i)} g_2^{h_2(M_j,i)} g_3^{\mathcal{X}_{j,i}})^{sk_j}$
output $\sigma_{j,i}$
Evaluate($\mathcal{F}_{\mathcal{GS}}, \mathcal{X}_j$) :
compute $res = \sum_{i\in\Delta} \mathcal{X}_{j,i}$
output $res$
GenProof($\mathcal{F}_{\mathcal{GS}}, \sigma_j, \mathcal{X}_j$):
compute $\pi = \prod_{i\in\Delta} \sigma_{j,i}$
output $\pi$
CheckProof($\mathcal{F}_{\mathcal{GS}}, pk_j, res, \pi$) :
set $S_\Delta = (S_1, S_2)$
compute $S_1 = \sum_{i\in\Delta} h_1(M_j, i)$ and $S_2 = \sum_{i\in\Delta} h_2(M_j, i)$
if $(e(\pi, g) = e(g_1^{S_1} g_2^{S_2} g_3^{res}, pk_j))$ then
    output 1
else
    output 0
end if
```

Fig. 2: Proposed System Methodology

D. Owner Login and File upload

This is the second module of our project. The important role for the Product owners is to move login window to Product owner window. Owner upload file, on that time file will splitter in to four different part and store in four different path with different keys.

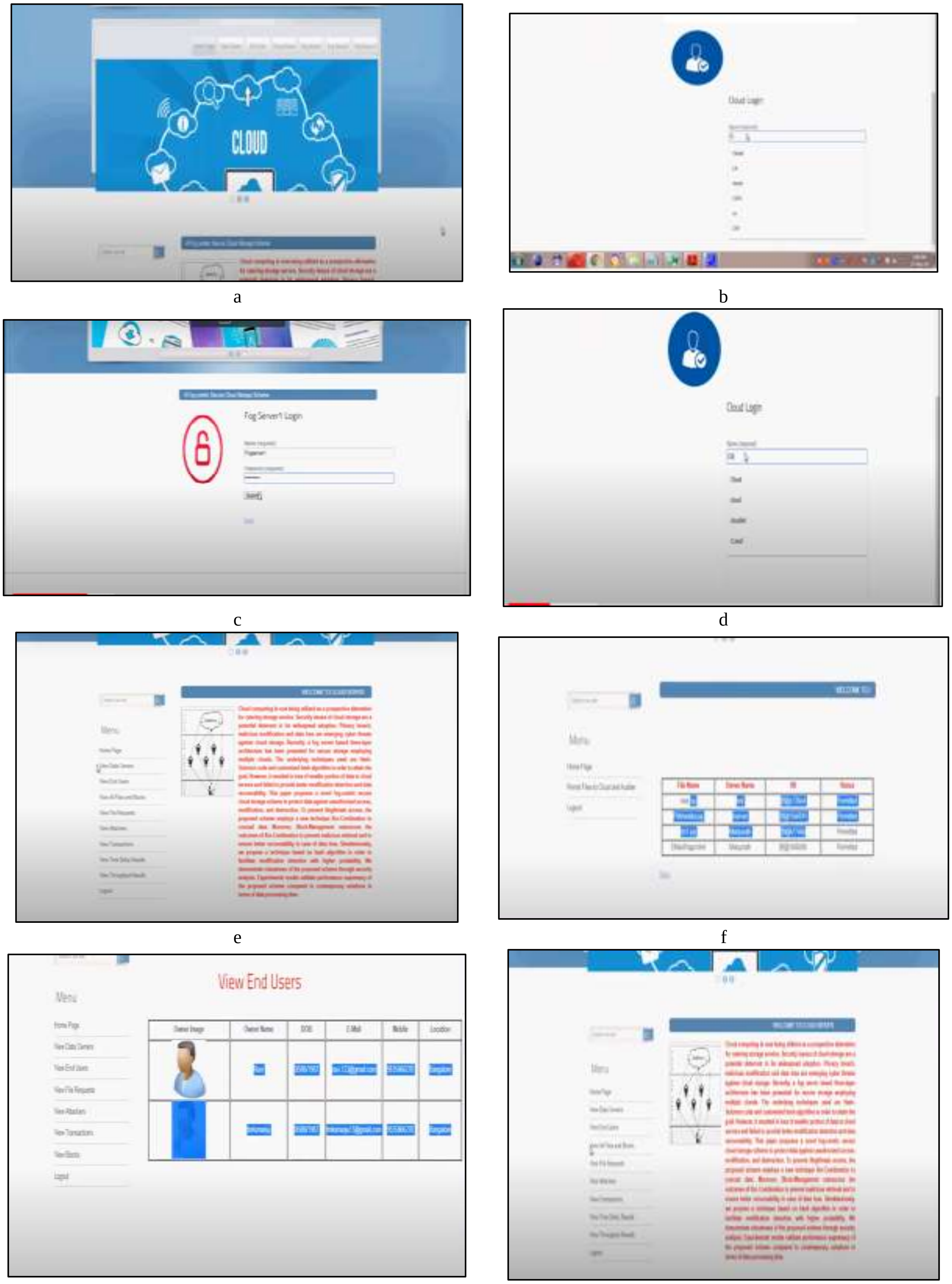
V. IMPLEMENTATION AND OUTPUT

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design. It shows what the system does and not how it should be implemented.

- Processor : Duall Core 2 Duos.
- Ram : 2gb dd Ram
- Hard Disk : 250 Gb

The software requirements document is the specification of the system. It should include both a definition and a specification of requirements. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks and tracking the team's and tracking the team's progress throughout the development activity.

- Front End : J2ee (Jsp, Servlet), Struts
- Back End : My Sql 5.5
- Operating System : Windows 7
- Ide : Eclipse



a

b

c

d

e

f

g

h

Fig. 3: (a-h) Output Screenshots of the Proposed System

VI. CONCLUSION

In this paper, we focused on the problem of supporting k-NN query over encrypted cloud data while the data owner cannot share his key with query users. For this a new solution is proposed with multiple keys to solve the key sharing problems thoroughly. At the core of our scheme, a series of novel secure protocols based on Twin-Cloud structure and DT-PKC cryptosystem is presented. We showed a theoretical analysis that our scheme can protect the data confidentiality and query privacy. Finally, extensive experimental evaluations demonstrate the efficiency and the scalability of the proposed scheme. As a future work, we will extend our work to support other data mining tasks, such as classification and similarity computation.

REFERENCES

[1] S. Yu, S. Guo, and I. Stojmenovic, “Can we beat legitimate cyber behavior mimicking ‘['attacks from botnets?” in 2012 Proceedings IEEE INFOCOM, March 2012, pp. 2851–2855.

[2] M. Li, S. Yu, W. Lou, and Y. T. Hou, “Toward privacy-assured cloud data services with flexible search functionalities,” in 2012 32nd International Conference on Distributed Computing Systems Workshops. IEEE, 2012, pp. 466–470.

[3] H. Cui, X. Yuan, and C. Wang, “Harnessing encrypted data in cloud for secure and efficient image sharing from mobile devices,” in 2015 IEEE Conference on Computer Communications (INFOCOM). IEEE, 2015, pp. 2659–2667.

[4] N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, “Privacy preserving query over encrypted graph-structured data in cloud computing,” in Distributed Computing Systems (ICDCS), 2011 31st International Conference on. IEEE, 2011, pp. 393–402.

[5] E. Kabir, A. Mahmood, H. Wang, and A. Mustafa, “Micro aggregation sorting framework for k-anonymity statistical disclosure control in cloud computing,” IEEE Transactions on Cloud Computing, vol. PP, no. 99, pp. 1–1, 2015.

[6] A Ramathilagam and K Vijayalakshmi, “A Survey of scheduling algorithms in cloud computing environment”, International Journal of Control Theory and Application Vol. 36, No. 9, pp.137-145.

[7] Z. Yan,W. Ding, X. Yu, H. Zhu, and R. H. Deng, “Deduplication on encrypted big data in cloud,” IEEE Transactions on Big Data, vol. 2, no. 2, pp. 138–150, 2016.

[8] S. Yu, Y. Tian, S. Guo, and D. O. Wu, “Can we beat ddos attacks in clouds?” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 9, pp. 2245–2254, Sept 2014.

[9] A. Priyalatha and A. Ramathilagam, “A New Task Scheduling LCGA Algorithm in Cloud Computing Environment”, International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences, 2019, Vol. 7, No. 3, pp. 32-37.

[10] A Ramathilagam and K Vijayalakshmi, “Meeting Deadlines Using Artificial Bee Colony (ABC) Based Resource Mechanism in Public Clouds with Task Replication in Large-Scale Biomedical Data”, Journal of Computational and Theoretical Nanoscience, 2018, Vol. 15 (3), 866-875

[11] B. Yao, F. Li, and X. Xiao, “Secure nearest neighbor revisited,” in Data Engineering (ICDE), 2013 IEEE 29th International Conference on. IEEE, 2013, pp. 733–744.

[12] Y. Elmehdwi, B. K. Samanthula, and W. Jiang, “Secure k-nearest neighbor query over encrypted data in outsourced environments,” in 2014 IEEE 30th International Conference on Data Engineering. IEEE, 2014, pp. 664–675.