International Journal on Applications in Information and Communication Engineering
Volume 5 : Issue 1: May 2019, pp 1 – 4 www.aetsjournal.com ISSN (Online) : 2394 - 6237

PRIVACY PRESERVE DATA SECURITY AGGREGATION AND RESOURCE ALLOCATION IN CLOUD COMPUTING

S.TAMILARASAN, A.MANCHULA

Abstract— Cloud computing is the growing demand in recent years. However, the privacy and security threat on the stored data is major issue. The proposed work studies the security and privacy threat on data, for the applications were data aggregation is necessary. The collected data may reveal sensitive information if no security and privacy technique are applied. Thus the proposed work proved to secure by implementing techniques such as homomorphic encryption. Apart from the data aggregation and providing security and privacy to the collected data, it is important to handle the data collection effectively, for this the proposed system is enhance to provide the resource allocation. The cloud providers may have more than one cloud servers, in which the data is allocated. The problem of resource allocation will further enhance the proposed work to fulfill the needs of Cloud computing.

I. INTRODUCTION

Cloud computing is a term meaning online hosted services. These services are accessible through the Internet, metaphorically called the "cloud". From a business point of view, this computing model is very attractive. Software, hardware, and physical infrastructure expenses are drastically reduced as contracting of computational resources is done in smaller grains and the expansion or reduction of these resources can be done in an automated way, according to the demand. Moreover, the operation of the infrastructure is delegated to a provider that, due to its scale, tends to be much more efficient.

Despite all the advantages cited, the use of cloud computing brings security and privacy concerns. In a poll of the Cloud Industry Forum for the United Kingdom, the two main inhibitors for cloud computing adoption are concerns about data security and privacy, mentioned by 70% and 61% of the respondents, respectively. In most cases, cloud services are provided on a shared infrastructure and, thus, additional attacks – both external and internal – can occur, such as stealing passwords for accessing the cloud service or exploits in the provided application programming interface (API).

In certain use cases – such as smart grids – confidentiality requirements tend to be greater due to its large volume of sensitive data. In this context, sensitive data, such as the fine grained energy consumption of each consumer, should be handled safely, since they can reveal a lot of information about consumers, e.g., excerpts from the day that there are no individuals in the household, arrival and departure times, or rest periods, which reveal their behavior patterns.

II. OBJECTIVES

Objective of study is to propose a software architecture to enable the use of cloud computing in applications with strict security and privacy requirements. This architecture considers how the components of an application can be integrated so that the privacy and security of user data are guaranteed. The sensitive part of the processing is therefore isolated and the architecture considers different strategies for aggregating sensitive data in environments where there are no guarantees of full confidentiality.

III. REVIEW OF LITERATURE SURVEY

1) "Improve Security over Multiple Cloud Service Providers for Resource Allocation"

From the last couple of decades, computations has changed from the client and server side to Cloud. Most of the Data generated today is completely processed in the virtual environment compared to the traditional systems. The physical location of these servers is unknown to many of the users using these services. Customers might not be aware of the storing of their data on backup servers to provide high availability in case of any failures in one of their data centers. Users are losing full control of their data by using Cloud services compared to processing their data on personal

S.Tamilarasan , Department of Computer Science and Engineering , J.K.K. Nattraja college of Engineering and Technology , Komarapalayam.
(Email ID : kingtamilg@gmail.com)
A.Manchula , Department of Computer Science and Engineering , J.K.K. Nattraja college of Engineering and Technology , Komarapalayam.
(Email ID : dr.manchulaphd@gmail.com)

computers. What will happen to customers data once they have stopped using Cloud services? Customers data is completely deleted from all Cloud servers? Even if the data is deleted from all of their servers, can customers will be sure their data will not be reconstructed by cloud service provider (CSP) using forensic applications.

To solve these problems, we have proposed a framework to solve the problem of reconstructing the data from the deleted servers using forensic applications. The use of different strategies for private data aggregation. These strategies include the use of homomorphic encryption or technologies likeIntel SGX.

2) "Security and privacy aware data aggregation on cloud computing"

The use of cloud computing has become common due to advantages such as low cost and sizing of computing resources according to demand. However, it also raises security and privacy concerns, because critical data – for example, in IoT applications – are stored and processed in the cloud. This paper proposes a software architecture that supports multiple approaches to secure data aggregation. For validation purposes, this software architecture was used in the development of applications for smart grids, computing instantaneous consumption of a region and the monthly bill of an individual consumer. The consumption data can be collected by smart meters, enabling consumers to reduce electricity costs through close monitoring. However, such data may reveal sensitive information if no privacy techniques are applied. Therefore, the proposed software architecture proved to be viable from experiments with techniques such as homomorphic encryption and hardware security extensions (Intel SGX). It will increase the cost for the customers, in order to protect the customer's data. Customers need to maintain the cloud services for some more time to replace the data.Basedon rewriting the complete data in the Cloud. If the customers have Big Data in Cloud, it might take a lot of time for writing the complete data.

3) "Reliable Resource Allocation for Optically Interconnected Distributed Clouds"

The Reliable Resource Allocation problem of allocating virtual machines from multiple optically interconnected data centers with the objective of minimizing the total failure probability based on the information obtained from the optical network virtulization. We first describe the framework of resource allocation, formulate the RRA problem, and prove that RRA is NP-complete. We provide an algorithm, named Minimum Failure Cover , to obtain optimal solutions for small scale problems. Then provide a greedy algorithm, named VM-over-Reliability, to solve large scale problems. Numerical results show that VOR achieves results close to optimal solutions gained by MFC for small scale problems.

Numerical results also show that VOR outperforms the resource allocation through random DC selection.A single cloud request with delay and VMs requirement in an aggregation communication pattern. More complicated requests can be achieved through several single requests.Star topology for a given request, and formulated the problem.

4) "Dynamic Resource Allocation Scheme in Cloud Computing"

The data collected from millions of public cameras needs to be retrieved, stored, and analyzed. A system is required which needs to allocate significant amounts of resources to analyse large-scale visual data. Cloud computing provides shared storage, computation, and various services to handle such a tremendous amount of data collected from distributed cameras. In order to reduce the overall cost of analysis, this paper presents a resource allocation algorithm that provides cost-effective resources with the degree of demand; scaling automatically in proportion to demand fluctuation. In the cloud, the users prefer reliable resources at minimum cost whereas service providers prefer efficient resources utilization with maximum profit. Hence, it is necessary to have resource bargaining that assures and satisfies both cloud users and service providers. We propose a bargaining scheme using a game theoretic approach to managing cost and resource utilization in cloud-based distributed cameras. Our experiments show that our approach can lead to 10-15% reduction in cost by dynamically utilizing the resources and switching the service provider when it gets a better deal from other service providers. A cost-effective and dynamic resource allocation method to handle large-scale data streams from distributed cameras.

5) "Dynamic Resource Pricing on Federated Clouds"

Current large distributed systems allow users to share and trade resources. In cloud computing, users purchase different types of resources from one or more resource providers using a fixed pricing scheme. Federated clouds, a topic of recent interest, allows different cloud providers to share resources for increased scalability and reliability.Users and providers of cloud resources are rational and maximize their own interest when consuming and contributing shared resources. In this

paper, we present a dyanmic pricing scheme suitable for rational users requests containing multiple resource types. Using simulations, we compare the efficiency of our proposed strategy-proof dynamic scheme with fixed pricing, and show that user welfare and the percentage.

IV. PROPOSED SYSTEM

The proposed approach differs from the aforementioned research along two principal dimensions. First, it addressed re-identification in longitudinal data publishing. Second, it groups diagnosis codes together, the framework is based on grouping of records, which has been shown to be highly effective in retaining data utility due to the direct identification of records being anonymized.

The proposed system introduces a novel approach to share patient specific longitudinal data that offers robust privacy guarantees, while preserving data utility for many biomedical investigations. The approach aggregates temporal and diagnostic information using heuristics inspired from sequence alignment and clustering methods. It demonstrates that the proposed approach can generate anonymized data that permit effective biomedical analysis using several patient information.

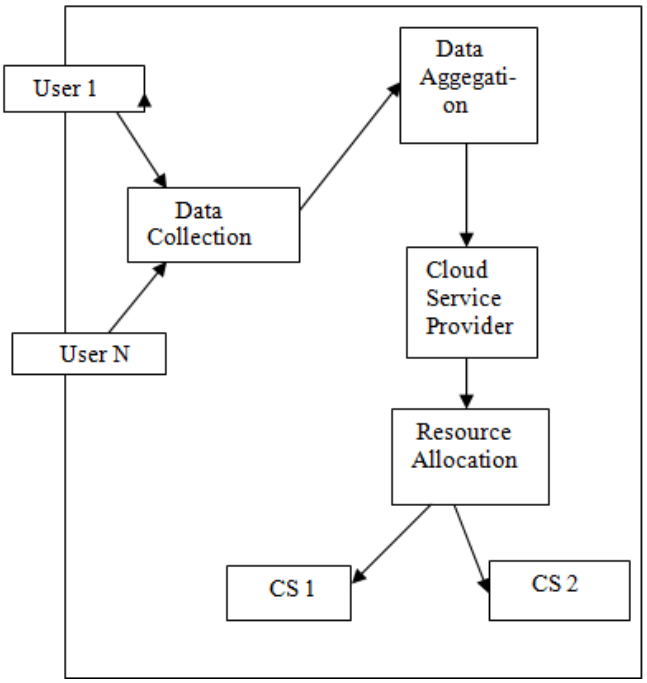
All protocols the thesis propose to solve problems rely on the fact that the anonymity of DB is not affected by inserting t if the information contained in t, properly anonymized, is already contained in DB. Then, Problem 1 is equivalent to privately checking whether there is a match between t and (at least) one tuple contained in DB.

The first protocol is aimed at suppression-based anonymous databases, and it allows the owner of DB to properly anonymize the tuple t, without gaining any useful knowledge on its contents and without having to send to t's owner newly generated data. To achieve such goal, the parties secure their messages by encrypting them.

ADVANTAGES

- Introduced the first approach to sharing patient data while providing computational privacy guarantees.
- The approach uses sequence alignment and clustering-based heuristics to anonymize longitudinal patient records.
- The investigations suggest that it can generate longitudinal data with a low level of information loss and remain useful for biomedical analysis.
- The approach is not guided by specific utility (e.g., satisfaction of GWAS validation), but it can be extended to support with confident.
- The new system checks whether the database inserted with the tuple is still k-anonymous, without letting two different users know the contents of the tuple and the database, respectively.
- The two protocols solve this problem on suppression-based and generalization-based k-anonymous and confidential databases.
- The protocols rely on well-known cryptographic assumptions.
- The new system provides theoretical analyses to proof their soundness and experimental results to illustrate their efficiency.

V. BLOCK DIAGRAM



VI. SYSTEM ARCHITECTURE

The system architecture of the proposed system, in which we aim to solve the security and privacy issue in data collection and aggregation. Also resource allocation problem is studied for efficient allocation of cloud resources.

A.Data publisher/ Producers

Data publishers/ Producers are responsible for generating data, which will be published in topics on the message bus. When necessary, these data will be processed by aggregators and eventually will be received by consumers – applications, for example. Sensitive data produced can not be used to threaten the security and

privacy of their owners, so each type of producer must provide strategies to ensure this.

B. Data aggregator

After consuming the producer's data of message topics on the message bus, it is often necessary to perform operations on them. These operations, such as sum, multiplication or grouping are performed by aggregators. The purpose of this component is to transform sensitive data in order to prevent critical information from being discovered while ensuring that it is still relevant to consumers. Any aggregation must be safe, so these components work in tandem with the producers because the data sent must be computable by the respective aggregator.

C. Secure storage

Secure storage is achieved by ElGamal cryptosystem. The data from producer is encrypted and re-encrypted and stored in cloud storage. When user/consumer wants to retrieve data, he will request the ID to aggregator. Aggregator verifies request and give key to the consumer. With the key consumer can decrypt and re-decrypt retrieve data from server.

D. Resource allocation

Resource allocation is done between two cloud server. The data from producer, after encryption and re-encryption reaches aggregator. Aggregator uploads the aggregate the data from different producers and consolidate data is uploaded to cloud server. Resource allocation is done randomly between two cloud server to upload data from aggregator.

VII. CONCLUSION

Software requirements like security and privacy should not be ignored by applications that handle sensitive data and use cloud computing. In this paper, we describe a software architecture to address such requirements. This architecture allows the use of different strategies for private data aggregation. These strategies include the use of homomorphic encryption or technologies like Intel SGX.

For our evaluation identified two use cases involving concerns with the mentioned requirements.

Given the use cases, proof of concept applications were developed in order to identify the advantages and disadvantages of each aggregation method. For homomorphic encryption, the main advantage identified was the viability to implement in any environment, although it is much less efficient. Intel SGX, on the other hand, used for the first time in a cloud computing orchestrator, much lower response times and allows performing various forms of computation on the sensitive data, but it demands a specific infrastructure from the service provider. Because of the compromises that need to be made, natural future work include how to guide developers into the selection of the best approach for their application. Another direction is to combine different technologies could work together to strengthen privacy and security.

One approach would be to combine different strategies with secure multi-party computation to avoid that a compromised technology would not impact on the overall application.

References

[1] Markovic DS, Zivkovic D, Branovic I, Popovic R, Cvetkovic D. Smart power grid and cloud computing. Renew Sust Energ Rev. 2013;24:566–77.

[2] Cloud Industry Forum. UK cloud adoption snapshot & trends for 2016: The business case for cloud. 2015. https://www.outsourcery.co.uk/media/1180/cloud-industry-forum-paper-15.pdf. Accessed 17 Aug 2017.

[3] Pasupuleti SK, Ramalingam S, Buyya R. An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing. J Netw Comput Appl. 2016;64:12–22.

[4] Younis YA, Merabti M, Kifayat K. Secure Cloud Computing for Critical Infrastructure : A Survey. In: The 14th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting. United Kingdom: Liverpool John Moores University; 2013.

[5] McKeen F, Alexandrovich I, Berenzon A, Rozas CV, Shafi H, Shanbhogue V, Savagaonkar UR. Innovative instructions and software model for isolated execution. In: HASP '13 The Second Workshop on Hardware and Architectural Support for Security and Privacy. New York: ACM; 2013. p. 10.

[6] Herbert Schildt, "C# 2.0, The Complete Reference", Osborne Complete Reference Series.

[7] Y. Chen, S. Tang, L. Zhou, C. Wang, J. Du, T. Wang, and S. Pei, "Decentralized clustering by finding loose and distributed density cores," Information Sciences, 2016.

[8] X. Xing, D. Xie, and G. Wang, Energy-balanced data gathering and aggregating in WSNs: a compressed sensing scheme. Taylor & Francis, Inc., 2015.

[9] D. C. Harrison, W. K. G. Seah, and R. Rayudu, "Rare event detection and propagation in wireless sensor networks," Acm Computing Surveys, vol. 48, no. 4, pp. 1–22, 2016.

[10] F. T. Jaigirdar and M. M. Islam, "A new cost-effective approach for battlefield surveillance in wireless sensor networks," in International Conference on NETWORKING Systems and Security, 2016, pp. 1–6.

[11] M. Z. A. Bhuiyan, G. Wang, J. Wu, J. Cao, X. Liu, and T. Wang, "Dependable structural health monitoring using wireless sensor networks," IEEE Transactions on Dependable & Secure Computing, vol. 14, no. 4, pp. 363–376, 2017.

[12] Alistair Mc Monnies, "Object-oriented programming in Visual C#. NET", Pearson Education, and ISBN: 81-297-0649-0, First Indian Reprint 2004.

[13] Robert D.Schneider, Jetty R.Garbus, "Optimizing SQL Server", Second Edition, Pearson Education Asia, ISBN: 981-4035-20-3