Data Security in Recommendation System Using Homomorphic Encryption

Kajol Soni and Gaurang Panchal(✉)

U & P U. Patel Department of Computer Engineering,
Chandubhai S Patel Institute of Technology, Changa, India
kajolsoni145@gmail.com, gaurangpanchal.ce@charusat.ac.in

Abstract. Cloud computing is like a daily routine now a day. Even though it has numbers of advantages in technical and business view, still there are some challenges there like data storage security, confidentiality and integrity. Main risk in cloud data is about to trust on cloud owner. Encrypted data is not useful for any computational process, so we cannot store as encrypted data. In recommendation system cloud plays very important role. Using homomorphic encryption, we can perform cloud data analyzation. This paper discusses about different homomorphic encryption technique and solution to recommendation system.

Keywords: Cloud data storage · Homomorphic encryption · Data security · Data confidentiality · Data integrity · Recommendation system · Collaborative filtering

1 Introduction

Cloud computing is a most popular architectural model in the field of Information Technology. It is combination of Distributed Computing, Parallel Computing and Grid Computing Architectures. It provides following kinds of services: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Basic Computing Resources and Storage Network Services can be categorized under IaaS. PaaS provide service to develop and run application without any worry about its complexity and maintenance. SaaS is a service in which we can provide features like subscribe and software licensing. For all these services, there is no need for users to manage or control the cloud infrastructure, including network, server, operating system (OS), storage and even the functions of applications [1, 2]. In other words, we can say cloud computing is a third-party service which can be used for delivery of the applications [3]. Some well-known service providers like Rack space, Microsoft, IBM. The buzz 'cloud computing' word way back in 2006 with the launch of Amazon EC2, gained traction in 2007 [11–29].

The research paper is divided into various sections. Section 2 introduce Recommendation system & literature review followed by Collaborative filtering and Homomorphic encryption in Sect. 3. Section 4 contains the proposed work and in last we will try to conclude the study and its future scope.

S.C. Satapathy and A. Joshi (eds.), *Information and Communication Technology for Intelligent Systems (ICTIS 2017) - Volume 1*, Smart Innovation, Systems and Technologies 83, DOI 10.1007/978-3-319-63673-3_37

2 Recommendation System

Recommendation system (RS) is a one kind of information filtering system that leads to predict some information regarding products, items or preferences [5–9]. RS became very popular in recent years and useful in many areas like movie, music, news, books, social tags, research articles, search queries and products in general. Another popular RS are restaurant, life insurance, online dating, and Twitter pages.

Figure 1 Shows overview of RS. Based on user past history and rating, system will try to match them. After that it will recommend some information. Recommendation system can be divided into two technique: Profile Based and Collaborative Filtering (CF) [4].

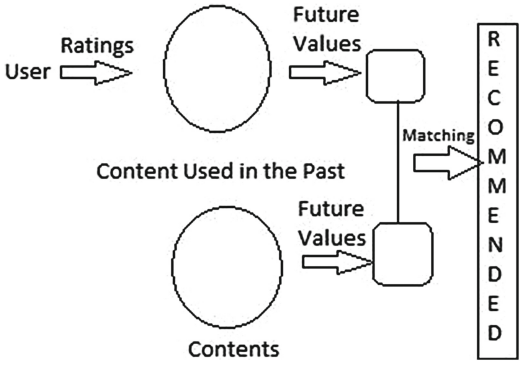

Fig. 1. Recommendation system

CF can further divide into two types: Item based CF and User Based CF. Item based CF will suggest items based on user's previous preferences. In User based CF, system will suggest items based on other user's activity who have similar kind of preferences.

Table 1. Homomorphic encryption & it's application

Algorithm	Nature of algorithm	Cloud storage	Application
Paillier [10]	Partially additive HE	No	E-voting
RSA [10]	Partially multiplicative HE	No	Internet banking
EIgamal [10]	Partially multiplicative HE	No	Hybrid system
EHC [10]	Fully HE	No	MANETS
NEHE [10]	Fully HE	No	E-commerce
AHEE [10]	Fully HE	No	Mobile cipher
BGV [10]	Fully HE	Yes	Security of integer polynomials

Here HE = Homomorphic Encryption, RSA = Rivest, Shamir and Alderman, EHC = Enhanced Homomorphic Encryption, NEHE = Non-interactive Exponential Homomorphic Encryption, AHEE = Algebra Homomorphic Encryption scheme based on updated EIgalmal, BGV = Brakerski, Gentry and Vaikuntanathan

As per research paper study and observation from theory we would like to share some views on homomorphic encryption that there are numbers of homomorphic algorithms are available. Among them we can choose any algorithm as per our requirement. For example, we require lightweight encryption to reduce complexity and power consumption specially in Internet of Things (IOT) application, we can use partially additive HE. For better understanding consider Table 1 which shows comparisons of some homomorphic encryption and its applications.

As Shown in Table 1, many algorithms are available but only BGV can be implemented on Cloud storage. As per our recommendation point of view we will choose BGV algorithm.

3 Homomorphic Encryption

Homomorphic Encryption (HE) is a one kind of encryption that allow to process on encrypted data. In HE we first need to encrypt data using secret encryption key. After processing on data we need to use decryption key to get original data. Advantage of HE is that after processing on encrypted data we can get the same result as it was applied on plain text or original data.

Advantage of homomorphic encryption over simple encryption is we do not need to worry about data integrity and privacy. In Fig. 2 we had shown simple mechanism of homomorphic encryption. Homomorphic encryption has major two operations: addition and multiplication. According to operation performed on the data it can be classified into mainly two sub categories. One is fully homomorphic encryption and another is partially homomorphic encryption. In fully homomorphic encryption both addition and multiplication is performed, while in partially homomorphic encryption any of them is used.

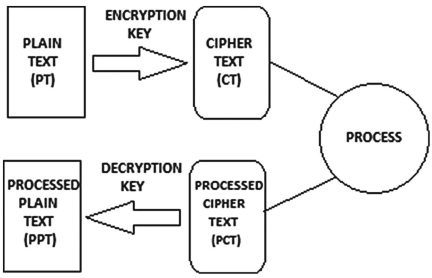

Fig. 2. Homomorphic encryption

4 Proposed Work

To Ensure data privacy we need to encrypt data. For that we proposed a better encryption scheme over simple encryption and it is HE. As we know that recommendation system will recommend items from stored data in cloud. So before putting data on cloud encrypt

them using BGV algorithm. If we are supposed to share that information with third party's recommendation system, there will be no issue of data privacy and data integrity.

Figure 3 shows basic diagram of proposed system. From the figure it's clear that it will solve issue of data privacy, data confidentiality and data integrity.

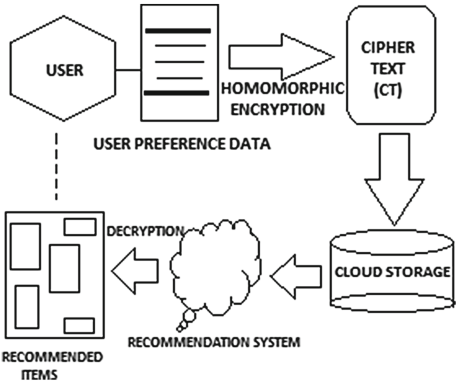

Fig. 3. Proposed homomorphic encryption for recommendation system

5 Conclusion

Providing security in cloud storage is a biggest challenge. Here in we presented our views and a way to provide data privacy and security to cloud data and it can be used for further process like recommender system. In this paper, we proposed a demo level of mechanism of homeomorphism encryption on recommender system, but in real time it require high computational power as cloud has big data storage. In future work, we will try to provide a solution with better efficiency so that it can deal with big amount of data.

References

1. Schafer, J.B., Konstan, J., Riedi, J.: Recommender systems in e-commerce. In: Proceedings of the 1st ACM conference on Electronic Commerce, pp. 158–166. ACM Press, New York (1999)
2. Kargupta, H., Datta, S., Wang, Q., Sivakumar, K.: On the privacy preserving properties of random data perturbation techniques. In: Proceedings of the 3rd IEEE International Conference on Data Mining (ICDM 2003), Melbourne, Florida, USA, pp. 99–106. IEEE, November 2003
3. Lemire, D., Maclachlan, A.: Slope one predictors for online rating-based collaborative filtering. Society for Industrial Mathematics (2005)
4. Lemire, D., Maclachlan, A.: Slope one predictors for online rating-based collaborative filtering. In Proceedings of the SIAM Data Mining (SDM 2005), Newport Beach, California, USA, April 2005

5. Aggarwal, C.C., Yu, P.S.: A General Survey of Privacy-Preserving Data Mining Models and Algorithms, Chapter 2, pp. 11–52. Springer, New York (2008)
6. Han, S., Ng, W.K., Yu, P.S.: Privacy-preserving singular value decomposition. In: Proceedings of the 25th IEEE International Conference on Data Engineering (ICDE 2009), Shanghai, China, IEEE, March–April 2009
7. Basu, A., Kikuchi, H., Vaidya, J.: Privacy-preserving weighted slope one predictor for item-based collaborative filtering. In: Proceedings of the International Workshop on Trust and Privacy in Distributed Information Processing (TP-DIS 2011), Copenhagen, Denmark, July 2011
8. Zhang, X., Hong tao D.: Ensure data securiy in cloud stoarge. In: NCIS 2011, pp. 284–287
9. Vaidya, J., Yakut, I., Basu, A.: Efficient integrity verification for outsourced collaborative filtering. In: Data Mining (ICDM), IEEE (2014)
10. Kangavalli, R., Vagdevi, S.: A mixed homomorphic encryption scheme for secure data storage in cloud, IEEE (2015)
11. Ganatra, G., Kosta, Y.P., Panchal, G., Gajjar, C.: Initial classification through back propagation in a neural network following optimization through GA to evaluate the fitness of an algorithm. Int. J. Comput. Sci. Inf. Technol. **3**(1), 98–116 (2011)
12. Panchal, G., Ganatra, A., Kosta, Y., Panchal, D.: Forecasting employee retention probability using back propagation neural network algorithm. In: IEEE 2010 Second International Conference on Machine Learning and Computing (ICMLC), pp. 248–251. Bangalore, India (2010)
13. Panchal, G., Ganatra, A., Shah, P., Panchal, D.: Determination of over-learning and over-fitting problem in back propagation neural network. Int. J. Soft Comput. **2**(2), 40–51 (2011)
14. Panchal, G., Ganatra, A., Kosta, Y., Panchal, D.: Behaviour analysis of mul-tilayer perceptrons with multiple hidden neurons and hidden layers. Int. J. Comput. Theory Eng. **3**(2), 332–337 (2011)
15. Panchal, G., Panchal, D.: Solving np hard problems using genetic algorithm. Int. J. Comput. Sci. Inf. Technol **6**(2), 1824–1827 (2015)
16. Panchal, G., Panchal, D.: Efficient attribute evaluation, extraction and selection techniques for data classification. Int. J. Comput. Sci. Inf. Technol **6**(2), 1828–1831 (2015)
17. Panchal, G., Panchal, D.: Forecasting electrical load for home appliances using genetic algorithm based back propagation neural network. Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) **4**(4), 1503–1506 (2015)
18. Panchal, G., Panchal, D.: Hybridization of genetic algorithm and neural network for optimization problem. Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) **4**(4), 1507–1511 (2015)
19. Panchal, G., Samanta, D.: Comparable features and same cryptography key generation using biometric fingerprint image. In: 2nd IEEE International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics, pp. 1–6. AEEICB (2016)
20. Panchal, G., Samanta, D.: Directional area based minutiae selection and cryptographic key generation using biometric fingerprint. In: 1st International Conference on Computational Intelligence and Informatics, pp. 1–8. Springer, New York (2016)
21. Panchal, G., Samanta, D., Barman, S.: Biometric-based cryptography for digital content protection without any key storage, pp. 1–18. Springer (Multimedia Tools and Application), New York (2017)
22. Panchal, G., Kosta, Y., Ganatra, A., Panchal, D.: Electrical load forecasting using genetic algorithm based back propagation network. In: 1st International Conference on Data Management, IMT Ghaziabad. MacMillan Publication (2009)

23. Patel, G., Panchal, G.: A chaff-point based approach for cancelable template generation of fingerprint data. In: International Conference on ICT for Intelligent Systems (ICTIS 2017), p. 6 (2017)
24. Patel, J., Panchal, G.: An IOT based portable smart meeting space with real-time room occupancy. In: International Conference on ICT for Intelligent Systems (ICTIS 2017), pp. 1–6 (2017)
25. Soni, K., Panchal, G.: Data security in recommendation system using homo-morphic encryption. In: International Conference on ICT for Intelligent Systems (ICTIS 2017), pp. 1–6 (2017)
26. Patel, N., Panchal, G.: An approach to analyze data corruption and identify misbehaving server. In: International Conference on ICT for Intelligent Systems (ICTIS 2017), pp. 1–6 (2017)
27. Bhimani, P., Panchal, G.: Message delivery guarantee and status update of clients based on IOT-AMQP. In: International Conference on Internet of Things for Technological Development (IoT4TD-2017), pp. 1–6 (2017)
28. Mehta, S., Panchal, G.: File distribution preparation with file retrieval and error recovery in cloud environment. In: International Conference on ICT for Intelligent Systems (ICTIS 2017), p. 6 (2017)
29. Kosta, Y., Panchal, D., Panchal, G., Ganatra, A.: Searching most efficient neural network architecture using Akaikes information criterion (AIC). Int. J. Comput. Appl. **1**(5), 41–44 (2010)