Efficient Framework For Multi-Screen Social Tv And Privacy Preserving On Cloud User Data

[1]Deivanai.K, [2]R.Viswanathan, [3]Karthika
[1,2] Professor of Galgotias University,[3] Professor Vels University Chennai.
devisports@gmail.com,rvnathan06@gmail.com, karthika.se@velsuniv.ac.in

Abstract: Multi-screen streaming media is being widely used in todays world. Users subscribe to interested channels and and their data is stored on cloud. A miner who have access to this data can analyze users behavioural pattern and attack on them by unnecessary spamming which might lead to harmful sites. In any case, while mining information put away on open cloud, it definitely presents protection worries on sensitive datasets. To empower regular itemset mining, this work requires n supported semi-genuine servers to make scattered decipherment throughout the analysis on encrypted information. Also, the need for this extra n supported semi-fair servers backs off the consecutively time of continuous itemset mining and presents gigantic collaborations and correspondence overheads. In this proposed framework, a protection safeguarding structure for safe regular itemset mining on encoded information, where just a single helped server (alluded to as Evaluator) is required other than the Cloud Service Provider (CSP). A modified paillier homomorphic algorithm is used here for encrypting the user hit count data which is encrypted and can be used for analysis purpose directly.
Key Words: paillier encryption, data security, multi-screen streaming.

1. INTRODUCTION

Distributed computing is the Practice of utility figuring where, assets are professional vided by the specialist organization and the customer will pay as they utilize the assets. Client can get to the cloud through thin customer. Cloud likewise gives memory to substantial measure of information to store and permits calculation. Consequently parcel of client can depend on cloud as it lessens the framework cost that the client needs to contribute.

Frequent itemset mining, that will be that the fundamental activity in association rule mining, is a standout amongst the most broadly utilized information mining strategies on huge datasets today. With the sensational increment on the size of datasets gathered and put away with cloud benefits lately, it is likely to convey this calculation escalated mining process in the cloud. The measure of work additionally exchanged the estimated mining calculation into the correct calculation, where such techniques not just enhance the precision likewise plan to improve the effectiveness. In any case, while mining information put away on open mists, it definitely presents protection worries on sensitive datasets.

There are many applications that are used by customers and their data being stored on cloud. The user is constantly worried about their data being wrongfully used or even being seen by others. In this project, the user can subscribe or buy to various channels that are available and watch videos. Many miners eagerly wait to use their data for recommendation purpose in general. By studying the user behavioral pattern, the miners can even attack on them by unnecessary spamming which the user does not need. Here, in this project, mining is performed on encrypted user data to ensure user privacy and mining results in channel recommendation for users which can be used in multiple screens. Paillier homomorphic encryption is used for this purpose, which is best suited for frequent item set mining that is being used here.

User can shift from system to their mobile phone by scanning the qr code of the video and then logging in. User can add trustworthy device also. We can either set the device for one-time access or trustworthy device. In this way, the video can be shared among devices without interruption and user need not login again and again.

2. RELATED SYSTEM

To empower frequent itemset mining, this work requires n supported semi-genuine servers to perform distributed decipherment throughout the analysis on encrypted information. Also, the need for this extra n supported semi-fair servers backs off the running time of continuous itemset mining and presents gigantic collaborations and correspondence overheads. There are many homomorphic algorithms that can be used, but each with different purposes. RSA is not fully homomorphic as it does not support additive property. RSA supports multiplicative homomorphic property, that is on performing multiplication on encrypted data directly, we get the actual result which is obtained on multiplying original input values.

$$\mathcal{E}(x_1)\cdot\mathcal{E}(x_2) = x_1^e x_2^e \mod m = (x_1 x_2)^e \mod m = \mathcal{E}(x_1\cdot x_2)$$

Also, white box cryptography does some special obfuscation method which is used for obfuscating some very specific type of code.

3. PAILLIER PRIVACY

Paillier cryptosystem is widely used as a homomorphic encryption plan to guarantee security prerequisites in numerous privacy ɸ preserving information mining plans. Homomorphic encryption plot is one of the valuable apparatuses for taking care of encoded delicate data. Be that as it may, a large portion of existing plans has not been broadly utilized as a part of down to applications because of their inefficiency. In this paper, we give an added homomorphic encryption plot which can be utilized for assessing some measurable data, for example, the mean and variance.

Frequently used terms:

ϕn - set of n integers

$\phi n*$ - set of integers coprime to n - this set consists of $\phi(n)$ number of integers

$\phi nn*$ - set of integers coprime to n^2 - this set consists of $n\phi(n)$ number of integers

$\phi(n)$ is Eulers totient function, that is number of positive integers which are less than n and are co-primes to n.

Key group:

n=pq where p and q are large prime numbers that are randomly chosen.

λ=lcm(p-1)(q-1)

Selecting α and β randomly from set of $\phi\ nn*$ then calculate g=(αn+ 1)β^n mod n^2

Public-key: (n, g), Secret key: λ

Encryption

1. Let m be the message to be encrypted where $m\in \phi\ n$
2. Selecting random r where $r\in \phi\ *n$
3. Compute ciphertext as: c=$g^m \cdot r^n$ mod n^2

Decryption

1. Ciphertext $c\in \phi\ *n^2$
2. Compute message: m=(c^λ mod n^2) . μ mod n where function L(u)=$\frac{u-1}{n}$.

The main difference from the original paillier algorithm is the g that is being chosen. The density of this is mostly n. The likelihood that the irregular component from the set picked up is extremely unimportant in bit length of open key n.

Paillier additive homomorphic property:

D(E(m1)*E(m2) mod n^2) = (m1 + m2) mod n

where, E(m1) = encrypted message1; E(m2) = encrypted message2; M1= message1; M2=message2;

D() is the decryption function.

In this scenario, suppose, there are 3 users and 5 channels to which they can subscribe and watch videos. The number of videos they have watched in each channel is recorded and the overview can be seen in Table 1.

Table 1: User hit count on channels

	Movies	Sports	News	Comedy	Discover
User1	5	13	0	10	8
User2	7	0	3	15	2

The number of times the user has visisted that particular channel is noted and this data when used in wrong hands, they can harm user by spamming. So, for transparency, these digits can be encrypted using paillier algorithm. For analysing purpose, performing frequent item set mining, where addition of these encrypted data is possible using the additive homomorphic property of paillier. Overall user data can be obtained and recommended for the users as trending videos from that channel or as most watched and subscribed channel.

4. RESULTS

In this segment, we assess the execution of our conventions, what's more, contrast it and past arrangements. The execution assessments for our protection safeguarding regular itemset mining conventions are tried on four PCs running Windows 10 with Intel Core i5-4570 4.20 GHz CPU on 8 GB RAM. In particular, one is utilized to mimic information clients to scramble every one of the exchanges also, transfer them to CSP; one is utilized as the Miner, and whatever is left of the two are utilized as the CSP and the Evaluator individually. To inflate network latency, we assume that the delay of one round communication is around 10 milliseconds all things considered, and the broadcast rate between two servers is around 10 Mbps.

5. CONCLUSION

Here, a concrete privacy preserving recurrent item-set mining on encoded cloud data is proposed with improved efficiency and security. A multi-screen channel user data is used for this purpose. User can subscribe to the various channels available and channel recommendation will be provided using query processing of encrypted data. In future, further improvement can be done on huge datasets with improved efficiency. Also, many machine learning algorithms are coming up, which can be used for better channel recommendation based on likes and peers watched videos.

REFERENCES

[1] S. Brin, R. Motwani, J. D. Ullman, and S. Tsur. (2016). Dynamic itemset counting and implication rules for market basket data. ACM SIGMOD, vol. 26, no. 2., pp. 255–264.

[2] J. Vaidya and C. Clifton. (2016). Privacy preserving association rule mining in vertically partitioned data. Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining. pp. 639–644.

[3] M. Kantarcioglu and C. Clifton. (2016). Privacy-preserving distributed mining of association rules on horizontally partitioned data. IEEE Transactions on Knowledge & Data Engineering, no. 9, pp. 1026–1037.

[4] J. Vaidya and C. Clifton. (2015). Secure set intersection cardinality with application to association rule mining. Journal of Computer Security, vol. 13, no. 4, pp. 593–622.

[5] T. Tassa. (2014). Secure mining of association rules in horizontally distributed databases. Knowledge and Data Engineering, IEEE Transactions on, vol. 26, no. 4, pp. 970–983.

[6] C. Dong and L. Chen. (2017). A fast secure dot product protocol with application to privacy preserving association rule mining. Advances in Knowledge Discovery and Data Mining, Springer, pp. 606–617.

[7] R. Agrawal, T. Imieli´nski, and A. Swami. (2015). Mining association rules between sets of items in large databases. ACM SIGMOD, vol. 22, no. 2. pp. 207–216.

[8] S. R. Oliveira and O. R. Zaiane. (2016). Privacy preserving frequent itemset mining. Proceedings of the IEEE international conference on Privacy, security and data mining, Australian Computer Society, Inc., pp. 43–54.

[9] Ayeelyan, J., Muthukumarasamy, S., & Rajesh, R.S. (2017). DTNH Indexing Method: Past Present and Future Data Prediction for Spatio-Temporal Data. International Journal of Intelligent Engineering and Systems, 10 (3), pp. 426-434.

[10] Belgacem, F.B.M., & Silambarasan, R. (2017). On Dixon elliptic functions and their Sumudu transforms: Connections to associated continued fractions expansions and Hankel determinants, Nonlinear Studies, 24 (4), pp. 757-773.

[11] Bellini, Emanuele, & Nadir Murru. (2015). An Efficient and Secure RSA--like Cryptosystem Exploiting R'edei Rational Functions over Conics. Finite Fields and Their Applications pp. 1–18.

[12] Chandrasegar Thirumalai. (2016). Review on the memory efficient RSA variants. International Journal of Pharmacy and Technology, Vol. 8 Issue 4, pp. 4907-4916.

[13] Chandrasegar Thirumalai, & Srivastav Budugutta. (2018) Public Key Encryption for SAFE Transfer of One Time Password. International Journal of Pure and Applied Mathematics, Vol. 118, No. 8, pp. 283-288.

[14] Chandrasegar Thirumalai, Senthilkumar M, Silambarasan R, & Carlos Becker Westphall. (2016). Analyzing the strength of Pell's RSA. IJPT, Vol. 8 Issue 4, pp. 21869-21874.

[15] C. Thirumalai & S. Shanmugam. (2017). Multi key distribution scheme by diophantine form for secure IoT communications. Innovations in Power and Advanced Computing Technologies (i-PACT), pp. 1-5.

[16] C. Thirumalai, M. Senthilkumar & B. Vaishnavi. (2016). Physicians medicament using linear public key crypto system. International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 1936-1939.

[17] C. Thirumalai & H. Kar. (2017) Memory efficient multi key (MEMK) generation scheme for secure transportation of sensitive data over cloud and IoT devices. Innovations in Power and Advanced Computing Technologies (i-PACT), pp. 1-6.

[18] C. Thirumalai, M. Senthilkumar & B. Vaishnavi. (2016). Physicians medicament using linear public key crypto system. International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 1936-1939.

[19] Firdhous, M., Ghazali, O., & Hassan, S. (2014). Statistically controlled robust trust computing mechanism for cloud computing. Journal of Information and Communication Technology, 13 (1), pp. 21-36.

[20] Hemanidhi, A., & Chimmanee, S. (2017). Military-based cyber risk assessment framework for supporting cyber warfare in Thailand. Journal of Information and Communication Technology, 16 (2), pp. 192-222.

[21] Jose, L., Malathy, C., & Poovammal. E. (2016). A survey on privacy preservation of healthcare data using cryptographic techniques. IJPT, 8 (4), pp. 22322-22329.

[22] Mahanta, Hridoy Jyoti, Sibbir Ahmed, & Ajoy Kumar Khan. A randomization based computation of RSA to resist power analysis attacks. Intelligent Systems and Control (ISCO), 2017 11th International Conference on. IEEE.

[23] Memon, Q.A. (2017). Neural network-based double encryption for JPEG2000 images. Journal of Information and Communication Technology, 16 (1), pp. 137-155.

[24] P Viswanathan. (2011). Fusion of cryptographic watermarking medical image system with reversible property. Computer Networks and Intelligent Computing, pp. 533-540.

[25] Pasupuleti, S.K. (2018). Effective and secure data storage in multi-cloud storage architectures. International Journal of Information and Communication Technology, 12 (1-2), pp. 74-97.

[26] Q. Kong, R. Lu, M. Ma, & H. Bao. (2017). A privacy-preserving sensory data sharing scheme in internet of vehicles. Future Generation Computer Systems (2017).

[27] Rivest RL, Shamir A, & Adleman LA. (1978). Method for obtaining digital signatures and public-key cryptosystems. Commun ACM.

[28] Sasikala, I., Ganesan, M., & John, A. (2014). Uncertain data prediction on dynamic road network. ICICES 2014, art. no. 7033972.

[29] Thangavel, M., P. Varalakshmi, Mukund Murrali, & K. Nithya. (2015). An Enhanced and Secured RSA Key Generation Scheme (ESRKGS). Journal of information Security and application, Vol. 20, 2015, pp. 3-10.

[30] T Chandra Segar, & R Vijayaragavan. (2013). Pell's RSA key generation and its security analysis. Computing, Communications and Networking Technologies (ICCCNT), pp. 1-5.

[31] V. Shanthi, P. Jeevana, G. K. Chaithanya & C. Thirumalai. (2017) Evaluation of McCabe's cyclomatic complexity metrics for secured medical image. ICEI, Tirunelveli, India, 2017, pp. 1122-1126.

[32] Xiao, P., Chen, R., & Qu, X. (2017). Improving security and energy-efficiency for cloud-based storage platforms in mobile computing environments. International Journal of Information and Communication Technology, 10 (4), pp. 468-481.

[33] Zirra, P., Wajiga, & G.M. (2011). Cryptographic algorithm using matrix inversion as data protection. Journal of Information and Communication Technology, 10, pp. 67-83.