IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 1, January 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 10, Issue 1, January 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1001013 |

Secure the k-nn Request on the Encrypted Data within KIDS

Monika Rokade, Dhanshri Chavan

Associate Professor, Department of Computer Engineering , Sharadchandra Pawar College of Engineering, Dumbarwadi, Post-Khamundi , Tal-Junnar, Dist-Pune (MS), India

P.G. Student, Department of Computer Engineering, Sharadchandra Pawar College of Engineering, Dumbarwadi, Post-Khamundi, Tal-Junnar, Dist.-Pune (MS), India

ABSTRACT: - Cloud computing age has drawn the notice of scholars and corporations because of its computing power, computing efficiency and edibility. Using the cloud computing era to evaluate outsourced data has proven to be a completely new information utilization strategy. However, due of the high security risks associated with cloud computing, most businesses increasingly encrypt data before outsourcing it. As a result, several new works on the k-Nearest Neighbor set of rules for encrypted information have appeared in recent years. However, basic concerns are currently being addressed within contemporary research: this system is no longer reliable, adequate, or efficient. To keep the congeniality of encrypted outsourced statistics, statistics get admission to patterns, and the question record, our proposed scheme uses current encryption schemes: Order Preserving Encryption and the Paillier cryptosystem, and uses the encrypted the k-dimensional tree to optimize the conventional scheme.

KEYWORDS: Outsourced data, privacy preservation-nearest neighbors, k-dimensional tree.

I. INTRODUCTION

Many computer security problems can be essentially reduced to separating malicious from non-malicious activities. This is, for example, the case of spam filtering intrusion detection, or the identification of fraudulent behavior. But, in general, defining in a precise and com putationally useful way what is harmless or what is offensive is often too complex. To overcome these difficulties, most solutions to such problems have traditionally adopted a machine-learning approach, notably through the use of classifiers to automatically derive models of (good and/or bad) behavior that are later used to recognize the occurrence of potentially dangerous events. A few detection schemes proposed over the last few years have attempted to incorporate defenses against evasion attacks. One such system is keyed intrusion detection system (KIDS), introduced by Mrdovic and Drazenovicat DIMVA10. A KIDS is an application-layer network anomaly detection system that extracts a number of features (words) from each payload [1]. The system then builds a model of normality based both on the frequency of observed features and their relative positions in the payload. KIDScore idea to impede evasion attacks is to incorporate the notion of a key, this being a secret element used to determine how classification features are extracted from the payload. The security argument here is simple: even though the learning and testing algorithms are public, an adversary who is not in possession of the key will not know exactly how a request will be processed and, consequently, will not be able to design attacks that thwart detection.

II. RELATED WORK

The k-NN search is one of the most familiar solutions in many applications, such as ranked key-words search, classification, recommender system,, intrusion detection, location privacy protection. In these works, many new schemes are designed to implement the privacy-preserving k-NN algorithm, some of which utilize data encryption techniques and some of which utilize Secure Multiparty. Computation. In recent years, many studies on the security of the k-NN search over the encrypted outsourced data in the cloud have been carried out and deepened. An efficient Asymmetric Scalar-Product-Preserving Encryption (ASPE) scheme is proposed, which can be used in the k-NN query processing because it can achieve the distance comparison between the encrypted data. However, there is still room for improvement in the security of this scheme. It is not secure under the chosen-plaintext attacks, and it cannot preserve the data access pattern from being leaked to the cloud. Zheng et al. utilized kd-tree, AES, and a homomorphism encryption technique to design a k-NN scheme for privacy preservation for outsourced healthcare data. This scheme can preserve the confidentiality of all data in high efficiency. To ensure the security of all data, this scheme requires that the user must

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 10, Issue 1, January 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1001013 |

be a trusted authorized user. But how to solve the k-NN query request of untrusted users is also a challenge, and this scheme still needs to be verified on the real healthcare data set. For this reason, in this literature, a k-NN query scheme for untrusted users was proposed. To solve the security problem, the data owner is required to be online for a long time, which will bring frequent interactions between the data owner and the cloud, so this scheme still has room for improvement in terms of efficiency.

III. PROPOSED ALGORITHM

A. *Encrypted kd-search:*

INPUT: $E(Q)$, $E(KD\text{-}TREE)$, K(IN K-NN SEARCH),
OUTPUT: $E(CAND)$// AN ARRAY CONTAINS ALL DATA TIINSIDE NODES RELATED TO A QUERY
1. L 0// L IS THE $E(CAND)$, A LIST OF K VACANCIES TO STORE THE NEAREST POINT(S) WHICH WILL BE FOUND.
2. Z 0//(Z IS THE NUMBER OF NEAREST NEIGHBOR(S))
3. KNN_INDEX IS READY FOR THE INDEXES OF THE K NEAREST POINTS
4. GETDIS( ){
5. **FOR** J 1 TO M DO
6. DIS K ($E(TI)$-$E(Q)$K //GET THE DISTANCE
7. END FOR
8. }
10. **IF** $E(Q1) \leq E(TROOT1)$== COMPARE THE VALUES OF THE ONE DIMENSION BETWEEN TWO POINTS.
11. **THEN** ENTER THE LEFT TREE
12. **ELSE** ENTER THE RIGHT TREE
13. $E(TLEAF)$ RECURVE (10)-(12)//$E(TLEAF)$ IS THE LEAF NODE OF THE CURRENT TREE
14. **IF** $Z < K$
15. **THEN** PUT THE $TLEAF$ INTO L, Z ZC 1, SAVE THE INDEX AND CALCULATE DIS (THE DISTANCE BETWEEN THE NODE AND Q)
16. **ELSE IF** DIS < MAXDIS //MAXDIS IS THE BIGGEST DISTANCE IN L
17. **THEN** REPLACE THE FARTHEST POINT.
18. TRAVERSE UPWARD, AND FOR EACH NODE:
19. CALCULATE THE DISTANCE DIS' BETWEEN $E(Q)$ AND ANOTHER
CHILD NODE OF THE PARENT NODE THE CURRENT
NODE BELONGS TO.
22. **IF** DIS' < MAXDIS JJ $Z < K$ 23. **THEN** EXECUTE (10)
24. EXECUTE (18)-(21)
25. COMPUTE THE INDEXES (INDEX[1]; : : : ; INDEX[K]) OF THE K SMALLEST DISTANCES AMONG (D1; : : : ; DN)
26. CLASSQ XINDEX[I]
27. **FOR** J 2 TO K D
28. CLASSQ -XINDEX[I]
29. END FOR
30. RETURN $CLASSQ$ TO THE QUERY USER BOB.

B. *Description of the Proposed Algorithm:*

Aim of the proposed algorithm is to provide the high security to the data over the cloud .

This is the first work that studies secure k-NN query on encrypted data with multiple keys. Propose scheme not only preserves the data confidentiality and query privacy but also supports the offline data owner.Based on the property of multiple keys, system can thoroughly solve the problems induced by key sharing with query user.

System present a set of novel protocols of secure two party computation based on distributed two trapdoors public-key cryptosystem, which become a cornerstone of secure k-NN scheme.

Based on the original protocols that system proposed, construct a secure k-NN scheme with multiple keys. And system show that the proposed scheme is secure under the standard semi honest model. Also, it demonstrate the practical applicability of solution.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 10, Issue 1, January 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1001013 |

IV. CONCLUSION AND FUTURE WORK

System concentrated the issue of secondary k-NN question over encoded cloud in- formation proprietor cant impart his key to question clients. System define another arrangement with mul-tiple keys illuminate the key distribution issues altogether. At the center of plan, system ex-hibited a progression of novel secure agreements based on Twin-Cloud structure and DT-PKC cryptosystem. System demonstrated a hypothetical investigation that system plan can secure the information secrecy and question protection. At long last, broad trial assessments exhibit the effectiveness and the adaptability of the propose plan. System will stretch out work to help other information mining undertakings, such as order and comparability calculation. Framework dissected the quality of KIDS against key-recovery assaults. The concentration in this work has been on recouping the key through productive techniques, showing that the order procedure spills data about it that can be utilized by an attacker. In any case, a definitive objective is to dodge the framework, and framework recently accepted that significant the key is basic to make an assault that sidesteps discovery or, at any rate, that essentially encourages the procedure. It stays to be seen whether a keyed classifier, for example, KIDS can be simply sidestepped without unequivo-cally recouping the key. On the off chance that the appropriate response is in the positive, at that point the key does not guarantee protection against avoidance. In research attempt, system will extend proposed work to support other data mining tasks, such as classification and similarity computation.

REFERENCES

[1] L. Ou, H. Yin, Z. Qin, S. Xiao, G. Yang, and Y. Hu, “An effcient and privacy-preserving multiuser cloudbased LBS Query scheme,” Secur. Commun. Netw., vol.2018, Mar. 2018, Art. no. 4724815.
[2] Juan E. Tapiador, Agustin Orfila, Arturo Ribagorda, and Benjamin Ramos, Key-Recovery Attacks on KIDS, a Keyed Anomaly Detection System, IEEE Transactions On Dependable And Secure Computing, Vol. 12, No. 3, May/June 2015.
[3] Y. Zhu, Z. Wang, and Y. Zhang, Secure k-nn query on encrypted cloud data with limited key-disclosure and offline data owner, in Pacific-Asia Conference on Knowledge Discov- ery and Data Mining. Springer, 2016, pp. 401414.
[4] Rosenberg, Ishai, and Ehud Gudes. ”Evading System-Calls Based Intrusion Detection Systems.” In International Conference on Network and System Security, pp.200-216. Springer International Publishing, 2016.
[5] Npoles, Gonzalo, IselGrau, Rafael Falcon, Rafael Bello, and Koen Vanhoof. ”A Granular Intrusion Detection System Using Rough Cognitive Networks.” In Recent Advances in Computational Intelligence in Defense and Security, pp. 169-191. Springer International Publishing, 2016.
[6] Shah, Bhavin, and Bhushan H. Trivedi, ”Improving Performance of Mobile Agent Based Intrusion Detection System.” In Advanced Computing Communication Technologies (ACCT), 2015 Fifth International Conference on, pp. 425-430. IEEE, 2015.
[7] 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 Communica- tions (INFOCOM). IEEE 2015.
[8] S. Liu, Q. Qu, L. Chen, and L. M. Ni, Smc: A practical schema for privacy-preserved data sharing over distributed data streams, IEEE Transactions on Big Data, vol. 1,no. 2, pp. 6881, 2015.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details