Enhanced Privacy-Preserving on Outsourced Association Rule Mining on Vertically Partitioned

Ms.P.N.V.Lakshmi[1], Ms. K. Naga Prasanthi[2], Dr.D.Veeraiah[3]
[1]M.Tech CSE Student, [2]Sr.Asst.Professor, [3]Associate Professor,
Dept of CSE, LBRCE, LB Reddy Nagar, Mylavaram, AndhraPradesh, India.

Abstract- In data mining, Association rule mining (ARM) and frequent item set mining (FIM) are two standard and usually studied data analysis techniques for a range of applications. Numerous research processes have been proposed for privacy-preserving mining on vertically partitioned databases. In the current work enhanced Caesar cipher algorithm for privacy preserving is proposed. The proposed system in this paper developed the cloud-based FIM solution, which is used to develop the better association rule mining system. This is purely developed for the outsourced databases which accept the number of data owners to share the data securely with data privacy.The proposed system reduces the time computation and increase the accuracy of the association rules and provides security for the association rules.

Keywords- Proposed Encryption, privacy preserving, Data mining.

I. INTRODUCTION

Association rule mining and frequent item set mining are two genuinemeasures and loosely examined data examination systems. These 2 methodologies are utilized in applications, let's say, market basket analysis, healthful services, web use mining, bioinformatics, and expectation. Exchange information is an appointment of exchanges, and each exchange is an appointment of data things with a 1 of a form TID (Transaction ID).This theme focus on security protective mining on vertically separated out databases. To ensure data security the framework can define a good planned cryptography plot. At that time the framework propose a FIM arrangement that is employed to manufacture anARM arrangement. The system defines some answers to the third party databases that alter totally different data administrators to efficiently give access to the data without compromising on data privacy.

II. LITERATURE SURVEY

The primary effort [1] to note and introduce the assurance matters in vertically separated out documents, a secure with in factor understanding is given and adjusted to build a security provided mining. Relationship precepts can then be uncovered in given trendy factor gatherings and their chains. They presented scalar product oriented protocol to provide security for the values which are present in the data. Since the generation of this important work, collection of securitypreservative association rule mining or persistent factor set mining arrangements are disclosed with in the structure ([2]-[3])

B. Rozenberg and E. Gudes [2] has presented some work that one of the data holder should take responsibility to compute mining results from other data holders. To protect their data, other data administrators include fake data into the genuine data.

Two methodologies (FIM & ARM) are applied with a substitution cipher before outsourcing. Later works demonstrated that it is not secure.

J. Zhan, S. Matwin, and L. Chang[3] has presented another work in which the data holders encrypt their data with awry encoding techniques. They do not use the other servers to compute the mining result. This data is still vulnerable to attacks. Regardless of this, a later work had identified that it is not secure.

S. Zhong, [4], has planned the following system: There are two methodologiesto get privacy preserving answers for FIM solutions. The first method reveals that there is no use of the original supports, and the second method does not reveal the genuine supports.Therefore it is difficult to calculate ARM results without frequent item sets. It achieves more security. Our current work also achieves similar security levels. Here, onlythe data holder's data is outsourced.

Giannottiet al. introduced a solution supported by k-anonymity frequency approach [6]. To avoid counter frequency analysis attack, the data holdersinsert some fake TIDS (transactions) into genuine data bases. These data bases are encrypted with asymmetric encryption algorithms. Then, ARM results computed by the third party servers or the mining task should be out sourced. Our proposed system utilizes this approach to provide the security for the genuine data.

J. Lai, Y. Li, R. H. Deng, J. Weng, C. Guan, and Q. Yan[7]:Another work presented in this paper is a protection preserved outsourced ARM computed in the arrangement of predicate encoding. This arrangement is flexible to pick plaintext assaults on disorganized things, but it's flooded against repetition examination assaults. Applying this we declare vertically separated-out databases and we can similarly originate the release of the proper supports to data administrators. We have a tendency to expect that the cloud is aware of the factor frequencies instead of picked plaintext-cipher text sets, and our answers of the two methodologies are flexible to study of Repetition assaults.

Apriori, Eclat and FP-growth

Frequent item set mining and association rule mining calculations, for example, Apriori, Eclat and FP-development for the protection point of view were not considered in this setting. Vaidya, Clifton and Kantarcioglu are the first to decide and report protection concerns in a level plane/vertically separated databases.

III. PROPOSED SYSTEM

The proposed system provides security to both genuine data and frequent item sets in vertically separated databases. This indirectly provides security to association rules mined from above data.

The two arrangements are meant for applications wherever data administrators have association with abnormal state of security necessity. The arrangements are in addition applicable for data administratorshoping to source data reposition – i.e. data owners will source their data into cloud in a more secured protective approach. This can be the principal effect in outsourced ARM and FIM for vertically separated databases. The hidden key procedures in our answers are productive planned encoding and protected outsourced comparison methodology.

Proposed Encryption Algorithm:

The Proposed encryption algorithm generates tons of plain text tasks. Set of computations have been done on the plain texts to protect the data and retrieval of accurate results. It takes time for computations. Therefore, there can be chance to reveal the sensitive information to the out-siders.

In this paper, we propose a symmetrical planned encoding system. It focuseson hiding the uneven supports. This topic supports one or two of planned encoding augmentations and strained extent of Proposed Encryption duplications [20].

Algorithm Proposed Encryption:

ENK () be the function of encrypting with the public key,
ENK (m1), ENK (m2) and the public key used in the encryption,
ENK (m1+m2) by performing
A modular multiplication of ENK (m1) and ENK (m2). Similarly given ENK (m1), m2 and the public key, one can compute
ENK (m1 × m2) by performing
Modular exponentiation ENK (m1) m2.
ENK (m1 + m2) = ENK (m1) × ENK (m2)
ENK (m1 × m2) = ENK (m1) × ENK (m1) × ENK (m1)
= ENK (m1) m2

IV. RESULTS

The Proposed association rule mining and frequent Patterns is implemented on java with IDE net beans 8.1 and database is MySQL. Implementation is done on various domains like supermarket for analysis of current trends in shopping.

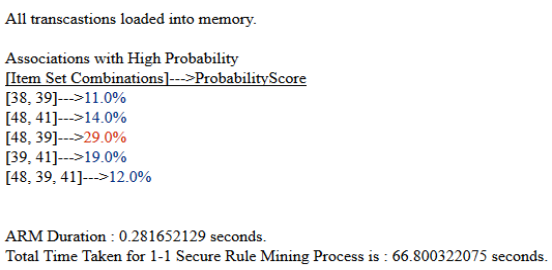

Fig.1: Existing System

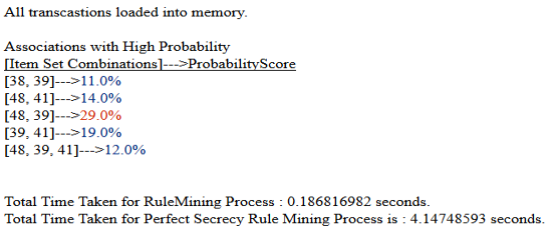

Fig.2: Proposed System

Compare with existing system the proposed system performance is more based on the computation time and accuracy of the association rules.

V. CONCLUSION

In this paper, the new proposed encryption technique is used to get the privacy and security for the frequent item sets. Caesar cipher is used to encrypt the data for securing messages. The proposed system adopts the enhanced encryption technique with Caesar and symmetric modular multiplication security scheme for the generated results. The time taken for computation are reduced compared to existing ones. Thus it is known that the proposed system performs better.

VI. REFERENCES

[1]. J. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," in Proc. SIGKDD, 2002, pp. 639–644.

[2]. B. Rosenberg and E. Gudes, "Association rules mining in vertically partitioned databases," Data Knowl. Eng., vol. 59, no. 2, pp. 378–396, 2006.

[3]. J. Zhan, S. Matwin, and L. Chang, "Privacy-preserving collaborative association rule mining," in Proc. DBSEC, 2005, pp. 153–165.

[4]. S. Zhong, "Privacy-preserving algorithms for distributed mining offrequent itemsets," *Information Sciences*, vol. 177, no. 2, pp. 490–503, 2007.

[5]. F. Giannotti, L. V. S. Lakshmanan, A. Monreale, D. Pedreschi, and H. Wang, "Privacy-preserving mining of association rules from outsourced transaction databases," IEEE Syst. J., vol. 7, no. 3, pp. 385–395, Sep. 2013.

[6]. M Sedighimanesh, a Sedighimanesh, J Baqeri. "Collect, Study and Preparation of Standards for Security and Stability in Desktop Applications." International Journal of Computer Networks and Communications Security 4, no. 11 (2016): 303-308.

[7]. Molloy, N. Li, and T. Li, "On the security and practicality of outsourcing precise association rule mining," in Proc. ICDM, Dec. 2009, pp. 872–877.