© 2018 IJSRST | Volume 4 | Issue 5 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

A Two Way Encryption for Privacy Preservation of Outsourced Transaction Databases for Association Rule Mining

Priya Kukade[1], Rajani Tale[1], Shweta Thakre[1], Aishwarya Sonwane[1], Prof. Rashmi Jain[2]
[1]BE Students, Department of Computer Science & Engineering, Rajiv Gandhi College of Engineering & Research, Nagpur, Maharashtra, India
[2]Assistant Professor, Department of Computer Science & Engineering, Rajiv Gandhi College of Engineering & Research, Nagpur, Maharashtra, India

ABSTRACT

Data mining-as-a-benefit has been chosen as impressive research issue by specialists. The Data Owner can outsource its data to the server which can be later used for mining the association rules. As both the association rules and the outsourced transaction database are private property of data proprietor. The data owner encrypts its data, send data and mining threshold query to the server, and receives the genuine samples from the encoded designs fetched from the server to secure the privacy. The issue of outsourcing transaction database inside a corporate privacy system is examined in this paper. We propose a plan for privacy preserving outsourced data mining. Our plan guarantees that each changed data is distinctive regarding the aggressor's past data. To counter these attacks we utilize Pallier Encryption on after Rob Frugal encryption implemented with a particular true objective to give protection for outsourced data mining. The exploratory outcomes on genuine transaction database demonstrate that our strategies are adaptable, effective and secure privacy.

Keywords: Cloud Computing, Association rule mining, Privacy-preserving outsourcing, Rob Frugal

I. INTRODUCTION

With the entry of distributed computing and its model for IT administrations upheld the net and expansive learning focuses, the outsourcing of information and figuring administrations is getting a totally one of a kind connation, that is anticipated to soar inside the near future. Business insight and data disclosure administrations, square measure anticipated that would be among the administrations manageable to be externalized on the cloud, on account of their insight serious nature, promote in light of the fact that the many-sided quality of learning mining calculations. In this way, the worldview of mining and administration of learning as administration can hypothetically develop as nature of distributed computing develops [1]. This can be the data mining-as-a-benefit worldview, intended for sanctionative associations with limited process assets as well as data handling background to source their data preparing hosts to a third gathering administration provider [2], [3].

Circulated processing will deal with in which incomprehensible parties of remote servers are planned to permit joined data amassing and online access to PC associations or assets. With the section of passed on enrolling and its model for IT associations in context of the web and tremendous server develops, the outsourcing of data and taking care of associations is getting a novel significance, which is firmly required to take off inside the not so distant future. In business, outsourcing fuses the contracting out of a business framework to another social gathering. Outsourcing courses of action to give an association in a corporate security protecting structure. Assurance affirmation is the basic issue in data mining.

Relationship, by and large, would lean toward not to give their own particular private data to different associations. The examination is that data is dispersed by Client for the advantage of enabling experts to mine encoded diagrams from the blended database. As a depiction, the regard based database from various affiliations can be transported to an untouchable which gives mining associations. The connection association would incline toward not to use an in-house get-together of data mining stars. In like manner, sporadically data is sent to the server or master group who is in charge of keeping up the encoded data and planning mining on it in perspective of asking for from association examiners of the association. The data proprietor is a customer and the server is implied as the expert focus. One of the key issues with this standard is that the server has territory to basic data of the proprietor and may reveal touchy data from the data. For instance, by looking exchange database, the server can derive or reveal which things or things are co-secured and along these lines, the mined blended cases that outline the alliance clients' unnoticeable segments.

We receive a preservationist recurrence based assault show inside which the server knows about the exact arrangement of things inside the proprietor's information and to boot, it conjointly knows about the exact help of everything inside the first learning. In this paper, we will probably design encryption conspire that grants formal privacy assurances to be very much attempted, and to approve this model over substantial scale genuine managing databases (TDB).

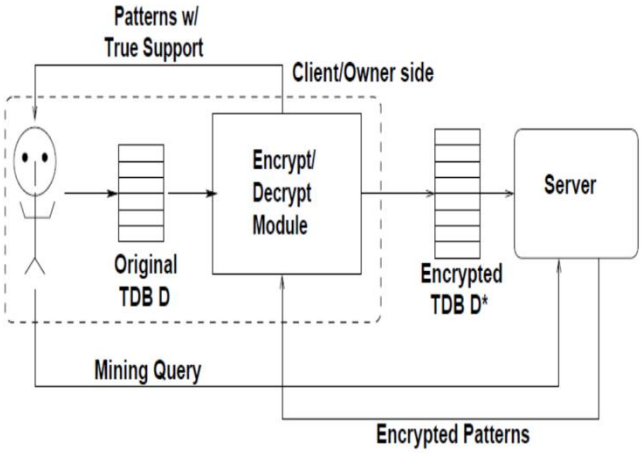

Figure 1. Architecture of Mining-as-Service Paradigm

The plan behind our model is delineated in Fig.1.The customer/proprietor encodes its data exploitation relate degree scramble/unscramble (E/D) module. Though the fundamental purposes of this module will be clarified in Encryption/Decryption Section. The server conducts data preparing and sends the (encoded) examples to the proprietor. Our coding subject has the property that came bolsters aren't genuine backings. The E/D module recoups truth character of the came designs moreover their actual backings.

We have built up an encryption plot, known as RobFrugal. The E/D module will use to redesign purchaser data before it's transported to the server. At that point, to allow the E/D module to recoup verity designs and their right help, we tend to suggest that it makes and keeps a conservative structure, alluded to as outline. We tend to also offer the E/D module with a conservative technique for incrementally keeping up the unique against refreshes inside the kind of adds. Related work is spoken to inside the following segment. The example mining undertaking is assessed at that point. Our privacy show is given in next segment. At that point next area builds up the encryption/decoding subject we tend to utilize. At long last, we finish up this paper and talk about bearings for future examination in last Section.

II. RELATED WORK

This section portrays the idea of Database as a Service and advantages, engineering of database outsourcing model, difficulties, and security administrations related with the same.

A. Database as a Service

Database as a Service (DBaaS) is a structural and operational approach empowering IT suppliers to convey database usefulness as an administration to at least one customers. DBaaS bears associations a chance to institutionalize and upgrade on a stage that takes out the need to send, oversee and bolster committed database equipment and programming for each project‟s various advancement, testing, generation, and failover conditions [3]. The DBaaS improves the need to buy and introduce the data administration equipment and programming at the data owner's site. The data proprietor and customers utilize the readymade database benefit profited to them by specialist co-op. The Organizations pay for the database benefit they are getting from the specialist co-op. For the organizations with less measure of assets constrained equipment and time-bound activities, DBaaS best suits the situation. Because of its innate versatile property, DBaaS can scale up well in the event of expanding client requests and furthermore downsize when the request dies down. The sending of foundation for ventures gets less demanding with the assistance of DBaaS. It offers adaptable and on-request benefits, improves execution tuning of the framework, brings down the working expense and many-sided quality, quickens the provisioning i.e. permits to clone the old database with another diagram, abbreviates the business cycle, gives failover condition to extend execution, empowers the concentrated organization and administration of a wide range of databases[4]. Considering the appropriation of DBaaS in ventures [5], the exploration expresses that in 2016, the income created by DBaaS suppliers will be $1.8 billion which is twice of the income produced in 2012 which is $150 million as appeared in figure 2.

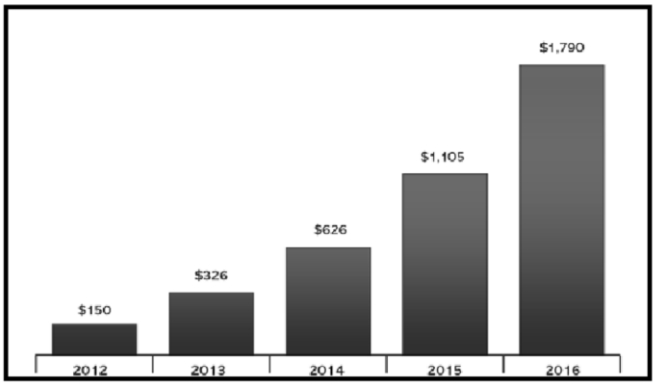

Figure 2. DBaaS Market Revenue and Forecast ($ Million)

B. Architecture of Outsourced Transaction Database Model

There are chiefly three elements associated with the Outsourced Transaction Database Model. Three substances are:

- Data Owner
- Service Provider
- Clients

The engineering is look like given underneath of Outsourced Transaction Database Model:- Generally, data proprietor and customers are considered as trustful substance while specialist co-op is doubtful in setting of uncovering data in an unapproved way. The Data-proprietor is in charge of refresh, embed, erase, change, and get to databases. The data proprietor has the specialist to allow or deny the customers for getting to the database. The Service supplier plays out every one of the data upkeep errands. Data administration equipment and programming apparatuses are conveyed and kept up at the provider's site. The obligations of Service-supplier are given beneath:-

- ✓ Provide Database as a Service
- ✓ Maintenance & administration of database
- ✓ Transaction Management
- ✓ Backup/Recovery System
- ✓ Fault Tolerance
- ✓ Scalability

- ✓ Database Availability
- ✓ Disaster Protection
- ✓ Efficient Query Processing

The query is prepared effectively and results are sent back to the questioned. The Clients are offered authorization to get to the data as indicated by their benefit level. There are three kinds of outsourced database display which are sorted based on number of data proprietors and customers included.

1. Unified Client Model
2. Multiple Client Model
3. Multiple Data Owner Model

The main model is "brought together customer show" in which the database is utilized by single element i.e. here usefulness of customer and data proprietor is same. The data proprietor does every one of the operations on the database. The correspondence interface between data proprietor and customer has high transmission capacity. This model is received in [8], [9], and [10].

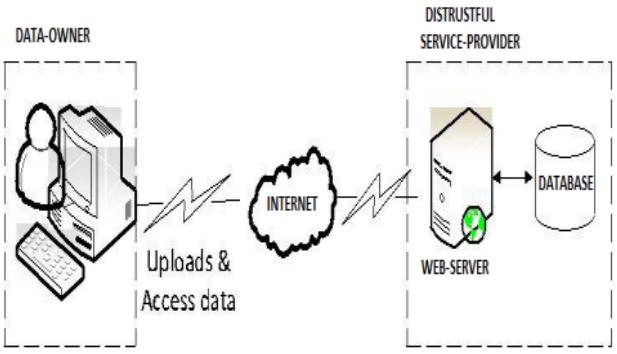

Figure 3. Single Data-owner and Service-Provider

The second sort of outsourced database display is "different customer show" where various customers are given the expert of read just access. Here, the database can be gotten to through cell phones, PCs, PCs with constrained transfer speed correspondence interface.

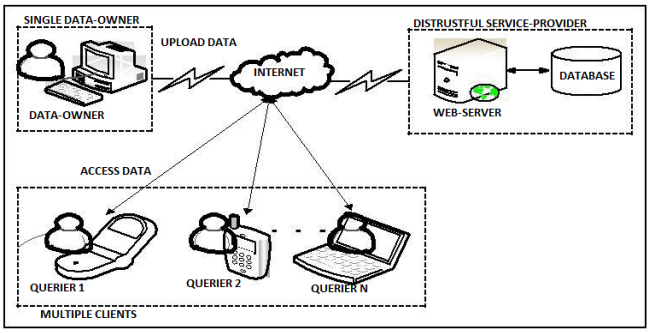

Figure 4. Single Data-Owner Multiple Clients and Service-Provider

This model is received by [8], [9], [11]. "Numerous data proprietor show" is the third sort of model which is received in [12]. In this model, every datum proprietor transfers data at benefit provider's site. In this way, for each gathering of data proprietor and customer, the different access control and security arrangements are should have been connected. This model can likewise be called as multi-expert outsourced database show.

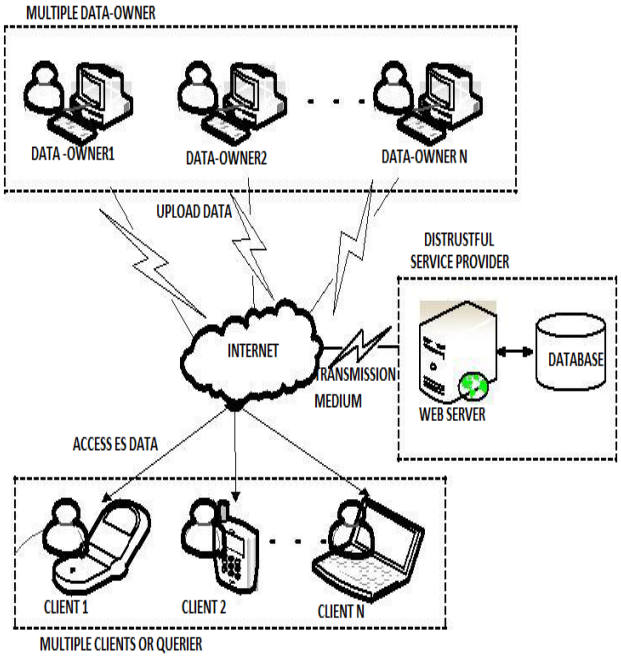

Figure 5. Multiple Data-owner Multiple Clients and Service Provider

C. Security Requirements

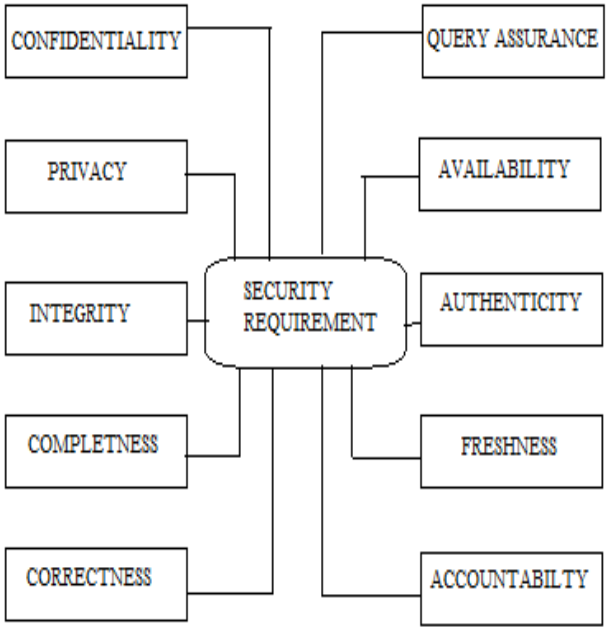

Figure 6. General Security Requirements for achieving Security in Database Outsourcing

The figure 6 portrays the general security prerequisites for actualizing them in database outsourcing.

1. The secrecy is one of the vital angles in security. Making the data garbled when it is in the travel state or put away in data lope is alluded to as preserving the data secrecy.
2. Privacy is likewise considered while keeping up the classification. For the most part, the privacy includes client privacy and access privacy. For concealing the character of the client, the client privacy is considered. Access privacy hides the database get to design for a specific client.
3. Uprightness guarantees that the data being put away in the database or being transmitted in the system is sealed or unaltered. Uprightness can be considered as the blend of two measurements as fulfilment and rightness.
4. The fulfilment ensures that the inquiry comes about are recovered by executing the question over all the database records which contain the predicate (tuple) communicated in the inquiry.
5. Accuracy guarantees that the outcomes picked up by executing the inquiry against the database are unaltered, amend and are created by the certified database servers or bona fide forms getting to the database.
6. Question affirmation gives the customer a chance to trust that inquiry is executed over the veritable database server as it were.
7. Accessibility is critical viewpoint in the security group of three of CIA (Confidentiality, Integrity, and Availability). Accessibility is characterized as how much the database framework is up and working in an operable state. It is especially urgent for the specialist organization to influence the database to benefit accessible constantly.
8. Validness alludes to the reliability and validity of databases, correspondence by means of transmission joins, transactions, customers, data proprietors and the specialist co-op. Every one of the substances must be approved for guaranteeing the credibility. Advanced mark gives the better method to accomplish the legitimacy.
9. Freshness is the new viewpoint considered in database outsourcing. Freshness of database is guaranteed just when the inquiry is executed on the latest release (adaptation) of the database transferred by the data proprietor. Keeping up the Freshness has an awesome importance when the database is constantly or intermittently refreshed and overhauled by the data proprietor. By sending the timestamp to the customers demonstrating the legitimacy of database is a decent approach for guaranteeing the Freshness of the database.
10. The assignments performed by every element are responsible for that substance as it were. This is called as responsibility. Access control is alluded to as permitting just the approved clients to get to the secured data they are allowed to. Access control can be acknowledged by following the three stages viz. Distinguishing proof, Authentication and Authorization.

ID is the demonstration of discovering which element is questioning the framework. Once the distinguishing proof is finished, validation comes into picture. It alludes to check the claim of an element to be bona fide. For actualizing the hearty security, the multifaceted validation component can be executed. The multi-factor validation can be the blend of username, passwords, biometric verification and the remarkable resources like swipe cards. Once the particular substance is recognized and validated, which data is allowed to access and which sorts of operations on data (Read, Write, Execute, and Update) are permitted to be performed is discovered. This is called as approval.

III. IMPLEMENTATION METHODOLOGY

We indicated Homomorphic Paillier encryption and FP-Growth association run creation techniques for assurance driving forward mining of organization together measures from outsourced exchange database. The execution reasons for energy of proposed structure are appeared in Figure 1.

We get a handle on an immediate rehash based assault appear in which the server knows the correct game-plan of things in the proprietor's data and what's more, it in like way knows the correct help of consistently thing in the essential data. It was one of the early wears out guaranteeing against the rehash based strike in the data mining outsourcing condition. It has been displayed utilizing counterfeit things to shield against the repeat based hit it was insufficient concerning a formal hypothetical examination of security insistences and has been appeared, all in all, to be defective beginning late in, the system for breaking the proposed encryption is given. Therefore, in our past and preparatory work, we proposed to deal with this issue by utilizing k-affirmation, i.e. in that everything in the outsourced dataset ought to be unclear from at any rate k – 1 things concerning their help. The working behind our model is addressed in Figure 1.

The customer scrambles its data utilizing an encode/unscramble module in protection saving, this module can be in a general sense saw as a "black box" from its viewpoint. The server conducts data mining and sends the (encoded) cases to the proprietor. The propose encryption plot has the property that the returned bolster are not genuine sponsorships. In the propose structure the E/D module recoups the true blue personality of the returned designs too their bona fide bolster. The (E/D) module unimportant to demonstrate that if the data is blended utilizing 1-1 substitution figures, In the figure content many figures and in this way the exchanges and cases can be broken by the server with a high likelihood by driving the rehash based assault. In the propose framework devise encryption orchestrates with a definitive target that formal protection confirmations can be appeared against strikes drove by the server utilizing foundation data. At to begin with, we formally depict a snare appear for the adversary and make amend the foundation taking in the foe may have. Our idea of security requires that for each figure message thing, there are in any event k–1 unmistakable figure things that are misty from the thing concerning their sponsorships Second, we influence an encryption to plot, called RobFrugal that the E/D module can use to change customer data before it is sent to the server. Third, to permit the E/D module to recuperate the true blue cases and their right help of data thing, we prescribe that it makes and keeps a smaller structure, called diagram. We additionally give the E/D module with a suitable structure for incrementally keeping up the outline against refreshes as affixes.

The Algorithms used in the methodology are as follows:

A. Rob Frugal Encryption

1) 1 to 1 substitution cipher :

The method which transformed original transaction database D into its encrypted version D^*. To improve

the security fake transaction are added with encrypted database. Table 1(a) shows original transaction while Table 1(b) shows transaction after one to one substitution (encrypted)

Table 1 (a). TDB

TDB
Soda Nuts
Soda Milk
Milk Soda
Nuts Milk
Soda Dates
Nuts Soda
Soda Egg
Nuts Cake
Cake

Table1 (b). TDB*

TDB*
e6 e5
e6 e4
e4 e6
e5 e4
e6 e2
e5 e6
e6 e3
e5 e1
e1

2) Support Calculation :

This approach was started with calculation of support of the items. Support count is the number of time the items occurred in the original transaction database.

3) Frugal Grouping :

Table 2. Descending order of items based on their item support

Item	Support
e6	6
e5	4
e4	3
e1	2
e3	1
e2	1

4) Robust k-Grouping method (Rob Frugal Grouping) Where k be the group size (i.e 2 or 3), Here we consider the group size as 2.

Given the items support table, from a group of size k such that no two items from any original transaction comes adjacent to each other i.e. we can't group e6,e5 or e6,e2 as they occurs adjacent in original transaction. After K-grouping method we get output as:

Item	Support	Noise (Difference)
e6	6	0
e1	2	4
e5	4	0
e3	1	3
e4	3	0
e2	1	2

Table 3: Rob Frugal with K-robust grouping

5) Fake Transaction Construction :

We can construct Fake transaction by adding Noise in to original transaction i.e. we can add e1 4 times, similarly e3 3times and e2 2 times in original transaction, so we generate transaction from given noise as {e1, e3, e2}, {e1, e3}, {e1}

B. Paillier Encryption

1) Key generation :

a) Select two large prime numbers a and b arbitrary and independent of each other such that gcd(n, Φ (n)) = 1, where Φ (n) is Euler Function and n=ab.

b) Calculate RSA modulus n = ab and Carmichael's function is given by λ = LCM (a-1, b-1).

c) Select g called generator where $g \in \mathbb{Z}^*_{n2}$ Select α and β randomly from a set $\mathbb{Z}_n^*$ then calculate $g = (\alpha n + 1)\ \beta^n \bmod n^2$.

d) Compute the following modular multiplicative inverse $\mu = (L\ (g^\lambda \bmod n^2)^{-1} \bmod n$. Where the function L is defined as $L(u) = (u-1)/n$.

The public (encryption) key is (n and g).

The private (decryption) key is (λ and μ).

2) Encryption:

a. Let mess be a message to be encrypted where mess ∈ $\mathbb{Z}_n$.

b. Select random r where $r \in \mathbb{Z}^*_{n2}$.

c. The cipher text can be calculated as:

Cipher = $g^{mess} \cdot r^n .\text{mod } n^2$.

3) Decryption:

a. Cipher text $c \in \mathbb{Z}^*_{n^2}$

Original message: mess = L (cipher$^{\lambda}$ mod n^2).μ mod n.

C. Association Rule Generation (FP-Growth)

Input: Built FP-tree

Output: complete set of frequent patterns

Method: Call FP-growth (FP-tree, null).

Procedure FP-growth (Tree, α)

{

1) If the event that Tree contains a single path P then

2) For each β = comb. of nodes in P do

3) pattern = β ∪ α

sup= min (sup of the nodes in β)

4) else

for each aiin the header of Tree do {

5) generate pattern = β ∪ α

sup= ai.support

6) Construct β's conditional pattern base

FPTree = construct β's conditional FP-tree

7) If Tree β = null

Then call FP-growth (Tree β, β)}

}

IV. MATHEMATICAL EXPLANATION

Let I = {i1, i2... in} be a set of n binary attributes called items.

Let D = {t1, t2... tm} be a set of transactions called the database.

Each transaction in D has a unique transaction ID and contains a subset of the items in I.

TRA1 = {bread}

TRA2= {milk, bread}

TRA3= {bread, milk}

TRA4 = {water, milk}

TRA5 = {bread, meat}

TRA6 = {bread, egg}

TRA7 = {water}

Where, I = {milk, bread, butter, meat}

The support supp(X) of an itemset X is defined as the proportion of transactions in the data set which contain the itemset.

For ex, the itemset milk, water has a support of 1/7= 0.1

The confidence of a rule is defined conf(X=> Y) = supp(X U Y) / supp(X)

V. RESULT ANALYSIS

Following are the results obtained during the implementation phase:

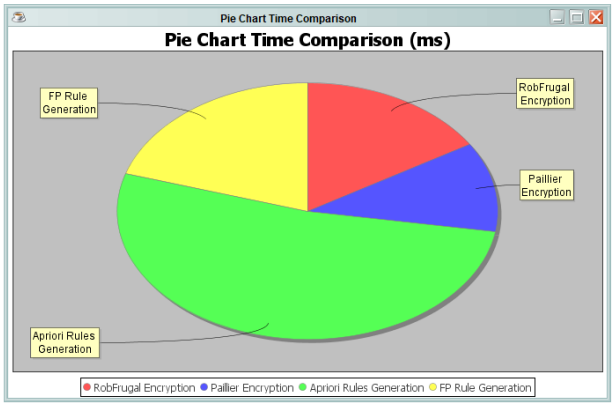

Figure 7. Time Comparison of the Algorithms

Figure 7 & Figure 8 shows the analytical comparison of resource utilization by the system. Fig. 7 Shows that among the two ARM, Apriori & FP-Growth the Time required by the Apriori is almost double then that of FP-Growth. Whereas Pallier Encryption will take a bit lesser time as compared to Rob-frugal.

Similarly, Figure 8 shows that Memory utilized by Apriori is again a bit of higher side as compared to FP-Growth, while the difference between the memory utilization of Encryption Algorithms is very less. As we said that there will be a double encryption to ensure the privacy of the data, we need to remember that this will lead to the resource utilization overhead. From the results we can conclude that if we use FP-Growth instead of Apriori, the utilization of the resource can be reduce while maintaining the security or privacy of the data with double encryption.

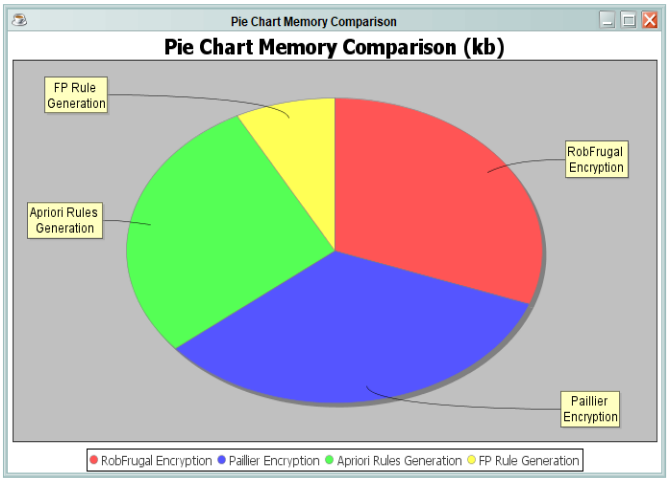

Figure 8. Comparison of Memory Utilization of the Algorithms

VI. CONCLUSIONS

Proposed Mechanism addresses a plan of encryption strategies for encryption techniques for Transactional databases that are appropriate for outsourcing association regulate mining. Beginning from an unmistakable balanced substitution figure, which is feeble to assaults, we use Paillier Homomorphic encryption tally which gives perfect security over existing loot thrifty estimation. In like way for association supervise time FP-Growth estimation is utilized which has ideal execution over Apriori. Addresses about demonstrate that our encryption system is incredibly excited to assaults as opposed to fundamental encouraged figure, which can be effectively broken with the assistance of foundation data. Besides man in within strike and conjecturing assault are dicey as structure utilizes Paillier encryption frameworks. At long last, through experimentation the proposed framework has better execution regarding time and security and lead time.

VII. REFERENCES

[1]. Fosca Giannotti, Laks V. S. Lakshmanan, Anna Monreale, Dino Pedreschi, and Hui (Wendy) Wang,-Privacy-Preserving Mining of Association Rules From Outsourced Transaction Databases, in IEEE SYSTEMS JOURNAL, VOL. 7, NO. 3, SEPTEMBER 2016.

[2]. W. K. Wong, D. W. Cheung, E. Hung, B. Kao, and N. Mamoulis,-Security in outsourcing of association rule mining, in Proc. Int. Conf. Very Large Data Bases, 2007, pp. 111-122.

[3]. L. Qiu, Y. Li, and X. Wu,-Protecting business intelligence and customer privacy while outsourcing data mining tasks, Knowledge Inform. Syst., vol. 17, no. 1, pp. 99-120, 2008.

[4]. C. Clifton, M. Kantarcioglu, and J. Vaidya,-Defining privacy for data mining, in Proc. Nat. Sci. Found. Workshop Next Generation Data Mining, 2002, pp. 126-133.

[5]. https://451research.com/reportshort?entityId=78105&referrer=marketing

[6]. Yung-Wang Lin, Li-Cheng Yang, Luon-Chang Lin, and Yeong-Chin Chen, Preserving Privacy in Outsourced Database, International Journal of Computer and Communication Engineering, Vol. 3, No. 5, September 2014.

[7]. H. Hacigumus, B. Iyer and S. Mehrotra, Providing database as a service, in Proc. of IEEE 18th ICDE, 2002, pp. 29-38.

[8]. E. Mykletun, M. Narasimha, and G. Tsudik,Authentication and integrity in outsourced databases, In Proc. of ACM Trans. On Storage, vol. 2, 2006, pp. 107-138.

[9]. M. Xie, H. Wang, J. Yin, and X. Meng, Integrity auditing of outsourced data,"VLDB 2007, pp. 782-793.

[10]. Zheng-Fei Wang, Ai-Guo Tang,Implementation of Encrypted Data for Outsourced Database, In Proc. of Second International Conference on Computational Intelligence and Natural Computing (CINC), IEEE, 2010, pp. 150-153.

[11]. Li Feifei, Marios H, George K, Dynamic Authenticated Index Structures for Outsourced Database, In Proc. of ACM SIGMOD‟06. Chicago, Illinois, 2006, pp. 121-132.

[12]. SomchartFugkeaw, Achieving Privacy and Security in Multi- Owner Data Outsourcing, In Proc. of IEEE Transactions 2012, pp.239-244.

[13]. Weichao Wang, ZhiweiLi,Rodney Owens, Bharat Bhargava,Secure and Efficient Access to Outsourced Data, CCSW'09, November 13, 2009, Chicago, Illinois, USA ACM 978-1-60558-784-4/09/11.

[14]. Shucheng Yu, Cong Wang, KuiRen, and WenjingLou,Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, IEEE INFOCOM 2010.

[15]. M. Xie, H. Wang, J. Yin, and X. Meng, Integrity auditing of outsourced data, VLDB 2007, pp. 782-793

[16]. W. K. Wong, D. W. Cheung, E. Hung, B. Kao, and N. Mamoulis, "Security in outsourcing of association rule mining," in Proc. Int. Conf. Very Large Data Bases, 2007, pp. 111-122.

[17]. G. I. Davida, D. L. Wells, and J. B. Kam. "A database encryption system with sub keys." ACM TODS, 6(2):312-328, 1981.

[18]. J. He and M. Wang. Cryptography and relational database management systems. In IDEAS, 2001.

[19]. B. Iyer, S. Mehrotra, E. Mykletun, G. Tsudik, and Y. Wu. A framework for efficient storage security in RDBMS. In EDBT, 2004.

[20]. C. Tai, P. S. Yu, and M. Chen, "K-support anonymity based on pseudo taxonomy for outsourcing of frequent item set mining," in Proc. Int. Knowledge Discovery Data Mining, 2010, pp. 473-482.

[21]. F. Giannotti, L. V. Lakshmanan, A. Monreale, D. Pedreschi, and H.Wang, "Privacy preserving data mining from outsourced databases," in Proc. SPCC2010 Conjunction with CPDP, 2010, pp. 411-426.

[22]. M. Kantarcioglu and C. Clifton, "Privacy-preserving distributed mining of association rules on horizontally partitioned data," IEEE Trans. Knowledge Data Eng., vol. 16, no. 9, pp. 1026-1037, Sep. 2004.

[23]. S. J. Rizvi and J. R. Haritsa, "Maintaining data privacy in association rule mining", in Proc. Int. Conf. Very Large Data Bases, 2002.

[24]. A. Evfimievski, R. Srikant, R. Agrawal, J. Gehrke, "Privacy Preserving Mining of Association Rules", Information System, 2004.

[25]. H. Kargupta, S. Datta, Q. Wang, K. Sivakumar, "On the Privacy Preserving Properties of Random Data Perturbation Techniques", In Proceedings of the 3rd International Conference on Data Mining, 2003.

[26]. Z. Huang, W. Du, B. Chen, "Deriving Private Information from Randomized Data", In Proceedings of the ACM SIGMOD Conference on Management of Data, 2005.

[27]. S. L. Warner, "Randomized Response: A Survey Technique for Eliminating Evasive Answer Bias", J. Am. Stat. Assoc., 1965.

[28]. A. Evfimievski, R. Srikant, R. Agrawal, J. Gehrk, "Privacy Preserving Mining of Association Rules", In Proceedings the 8th ACM SIGKDD International Conference on Knowledge Discovery in Databases and Data Mining, 2002.