A Privacy Preserving Framework For Analyzing Auctioning Information In Cloud Computing

[1] Keya V. Patel, [2] Prof .Ujas S. Patel , [3] Prof . Krunal Suthar
[1] M. Tech Student, [2]Assistant Professor, [3]Assistant Professor
[1] Department of Computer Engineering, L.C.I.T ,Bhandu. India.
[2] Department of Computer Engineering, L.C.I.T ,Bhandu. India.
[3] Department of Computer Engineering, SPCE, Visnagar. India

Abstract—Cloud Computing has become a main source for data security, data storage and data privacy .Data stored over the cloud to get useful information and analysis. while performing the data mining techniques on large set of data there are chance to misuse of information ,loss of information and insecurity of stored data. So use the efficient data mining techniques such as K anonymity ,L diversity and T closeness that preserve privacy of sensitive data .In this paper we consider how to perform privacy preserving auctions in cloud that do not leak any information and auction result to anyone. Our main aim of privacy preserving techniques is maximize the efficiency and low computation with minimum information loss.

Keywords — Cloud Computing, informationsecurity,efficiency,privacy preservation ,K anonymity ,L diversity , T closeness.

INTRODUCTION

A enhanced auction mechanisms satisfying various economic properties such as truthfulness, profit maximization, and social efficiency maximization. in this paper we develop a privacy -preserving cloud auction framework that runs without disclosing anything about the bids except what is revealed from the auction results. We focus on a truthful cloud auction mechanism proposed recently , where a cloud provider provides various computing resources to a large number of heterogeneous users.

- For the auctioneer, it can simply adapt its pricing strategy based on the bidders' bids to obtain extra profit.
- For the bidders(cloud user), since VM instances are usually granted for a limited time block, cloud auctions are executed periodically. Through learning the historical bids of others bidder may get to know others' willingness to pay, and choose to bid suntruthfully to get extra profit, thus tampering with the truthfulness of the whole auction.
- For an attacker not participating the auction, once obtaining bid information, it can impair the auction process by submitting a bid that cannot win the auction, but will increase the price paid by the winners.

For privacy preservation some different techniques use such as K anonymity , L diversity ,And Tcloseness.
(1) K anonymity: K anonymity is a classic model. K-anonymity safeguards the data from identity disclosure, but it does not protect the data from background knowledge attack. K-anonymity prevents the disclosure of the patient details that are caused due to linking attacks. K-anonymity prevents linkage attacks but does not prevent attribute disclosure.
(2) L diversity: The technique ℓ-diversity is proposed in order to handle the shortcomings of the k-anonymity, where the technique does not ensure protection against attribute disclosure. l-diversity solves the problem of attribute disclosure by replacing the dataset by ℓ-diversified values for each sensitive attribute. The advantage of l-diversity over k-anonymity is that l-diversity provides higher level of protection to external attacks more than what k-anonymity provides, since k-anonymity does not offer protection against linking attacks .In this model, an equivalence class is said to have l-diversity if there are at least l well-defined values for the sensitive attribute
(3) T closeness: T-closeness was presented as an extension of k-anonymity that also protects against attribute disclosure. It is most efficient technique rather than upper both.

In this paper first provider prepare auctioning related data and that are stored into the cloud .after that user can submit their query onto the database and check for requested details then temporary result can produce against anonymized attribute and display the query result.

RELATED WORKS

In this paper[1] author proposed a secure auctioning model .The goal of auction mechanism is (1)To preserve strategy proof and social efficiency maximization (2) auction mechanism should preserve privacy for bidder. Bid value should be hidden throughout the whole auctioning procedure.[1]

In this paper [2]analyses various privacy preserving data mining techniques for their pros and cons and give a proposed concept with minimum information loss. The proposed hybrid technique can successfully achieve the goal of privacy preservation without any information loss[2]

In this paper [3] study about the problem of preserving location privacy in mobile crowd sensing. we can easily determine the location of a Smartphone user only with the price of the task in user's bid. This block the platform in selecting the winning users who offers the lowest price for a given sensing task. [3]

Author proposed [4] privacy preserving framework for truthful cloud auction that runs without closing anything about the bid. No bidder can learn anything about the bids of other bidder. any user not participating the auction can not learn anything about all bidders , accept auction result of the current run.[4]

author [5] focuses on auction mechanism to achieve both privacy preservation and verifiability. most relevant work for this paper is online auction mechanism for ad exchanges was proposed. This work ,only guarantee about privacy of bid , but not consider the problem of the verification.[5]

In this paper we show different anonymization technique comparison [6] While *k*-anonymity protects against identity disclosure ,it does not provide sufficient protection against attribute disclosure .The notion of `*L*-diversity attempts to solve this problem by requiring that each equivalence class has at least well-represented values for each sensitive attribute.
In this paper We have shown that `*L*-diversity has a number of limitations and have proposed a novel privacy notion called *t*-closeness.[6].

COMPARISON OF VARIOUS RESEARCH SCHEMES

The table below shows a short comparison about the various schemes proposed by a researcher by taking different parameters. The table gives the description about the basic technique used with the benefits that researcher gets the limitations found in scheme shown in table. 1

	A Privacy Preserving Framework for Analyzing Auctioning Oriented Data in Cloud Computing							Oth ers	
Individual Criteria → Papers ↓	Cloud Computing	Privacy Preservation	Data Mining	Data Security	Efficiency	Encryption	Verification	Quasi Identifier	T Closeness
[1]	✓	✓	✓	✓	✓	X	X	X	X
[2]	✓	✓	✓	✓	✓	✓	X	X	X
[3]	✓	✓	X	✓	X	✓	X	X	X
[4]	✓	✓	✓	✓	✓	✓	X	X	X
[5]	✓	✓	X	✓	✓	✓	✓	X	X
[6]	✓	✓	X	✓	✓	X	X	X	✓

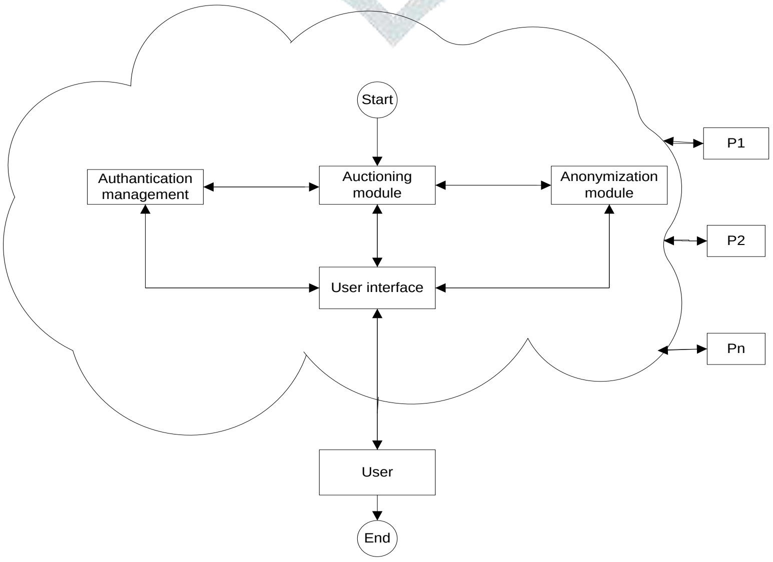
Table 1: Comparison study

Proposed Methodology

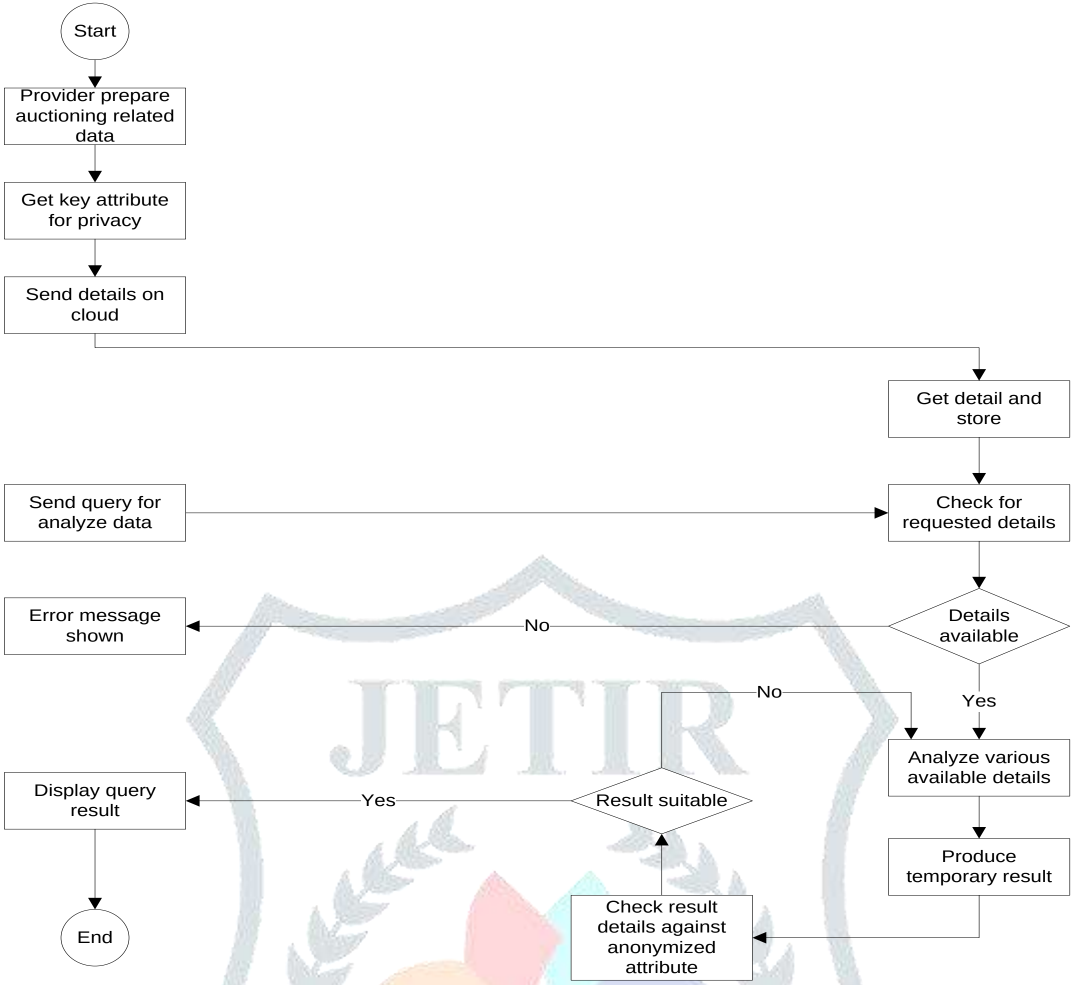
The system will work on various types of information related to auctioning like personal, payment Etc. Customer have ability to choose the sensitive attributes. User send query to the stored details into database and check for related information and analyze various available details. User can interact with Authentication management , Auctioning module and Anonymization module into the cloud environment. Method will mine all the data and give proper result with least information loss. System consider both the fundamental that's sensitive attribute of different type of information and efficient anonymization method to hide users sensitive details.

In this system , provider prepare the auctioning related data and send it onto the cloud environment and they are stored into the database. User send query for analyzed data .it is check into database and analyze various available details and produce temporary result. After that check result details against anonymized attribute and display query result.

Flow 1 : User Interaction With Cloud Environment



Flow 2: Running Process Flow


Start
Provider prepare auctioning related data
Get key attribute for privacy
Send details on cloud
Get detail and store
Send query for analyze data
Check for requested details
Error message shown
No
Details available
Yes
No
Analyze various available details
Display query result
Yes
Result suitable
Produce temporary result
Check result details against anonymized attribute
End

Algorithm Steps:

Step 1: Start.
Step 2: Provider purchase Auctioning related data.
Step 3: Get key attribute for privacy.
Step 4: Send details on cloud.
Step 5: Get details and store in database.
Step 6: Then user send query for analyze data.
Step 7: Check for requested details into database.
Step 8: If details available in database Then analyze various available details.
Step 9: Else error message shown.
Step 10: Produce temporary result from step8.
Step 11: Then ckeck result details against anonymized attribute.
Step 12: If result suitable Then display query result.
Step 13: Else go to step8.
Step 14: End.

CONCLUSION

we study how to preserve privacy for auctioning data with efficient anonymization techniques with minimum information loss and low computation. We provide No any disclosure about customer’s key attribute(sensitive) details and Least loss of information in result due to proper anonymization method. T -closeness technique is best for novel privacy preservation notion.

The proposed system concluded as , Mines the auctioning details efficiently , No any discloser about customer’s key attribute(sensitive) details , Users have option to provide quasi attribute which ensure the user about security of this details , Provide least loss of information in result due to proper anonymization method.

REFERENCES

1. Yu-E Sun, He Huang, Xiang-Yang Li, Yang Du, Miaomiao Tian, Hongli Xu, and Mingjun Xiao, “Privacy-Preserving Strategy proof Auction Mechanisms for Resource Allocation” In Tsinghua Science And Technology, IEEE-2017.
2. Anu Rinny Sunny , “ Preserving Privacy of Data Using K Anonymization and T-Closeness”In IET Software IEEE 2017.
3. Arshveer Kaur, Sanjeev Sofat ,“A proposed hybrid approach for Privacy Preserving Data Mining” In International Conference on Inventive Computation Technologies (ICICT) ,IEEE-2016.
4. Ting Wen, Yanmin Zhu, Tong Liu,“*P*2: A Location Privacy-Preserving Auction Mechanism for Mobile Crowd Sensing”, In Global Communications Conference (GLOBECOM) ,IEEE-2016.
5. Zhili Chen, Lin Chen, Liusheng Huang, Hong Zhong,“On Privacy-preserving Cloud Auction ”, In 35th Symposium on Reliable Distributed Systems (SRDS) , IEEE-2016.

6. Minping Zhou, Chaoyue Niu, Zhenzhe Zheng, Fan Wu, and Guihai Chen,"An Efficient, Privacy-Preserving, and Verifiable Online Auction Mechanism for Ad Exchanges", In Global Communications Conference (GLOBECOM) ,IEEE-2015.

7. Jordi Soria-Comas , Josep Domingo-Ferrer , "Differential Privacy via t-Closeness in Data Publishing", In Eleventh Annual International Conference on Privacy, Security and Trust (PST), IEEE 2013.

8. Ninghui Li , Tiancheng Li, Suresh Venkatasubramanian *"t*-Closeness: Privacy

9. Beyond *k*- Anonymity and `-Diversity" In 23rd International Conference on Data Engineering IEEE 2007.

10. [9] Ashwin Machanavajjhala , Johannes Gehrke , Daniel Kifer " ℓ-Diversity:

11. Privacy Beyond k-Anonymity" In 22nd International Conference on Data

12. Engineering ,IEEE 2006.

13. [10] Josep Domingo-Ferrer, Jordi Soria-Comas **,"**From t-Closeness to Di_erential Privacy and Vice Versa in Data Anonymization" In IEEE 2006.