A New Scheme for Privacy Preservation with Optimization for Data in Cloud Computing

Ritu Prajapati[1], Nirav Shah[2]
[1]M.E. Department of Computer Engineering, Silver Oak College of Engineering and Technology
[2]Asst. Professor, Department of Information Technology, Silver Oak College of Engineering and Technology

***Abstract* - To fulfill people's requirements for low latency and strong computing power in mobile devices, edge computing emerges as a paradigm for realizing service provisioning in the edge of mobile cloud near the activity area of the mobile subscribers. Among the numerous researches on location privacy preservation, cloud-based location privacy preservation has become a hot topic, but it undoubtedly brings new problems such as data confidentiality and user privacy disclosure. Design for wearable devices with identity authentication and data access control considerations in the space-aware and time-aware contexts. In the time-aware cloud computing mode, ciphertext policy attribute-based encryption is applied for fine-grained access control, and bloom filter is used to achieve efficient data structure without privacy exposure. In these paper works on privacy preservation with trust mechanism.**

***Index Terms* - Privacy-Preservation, Edge computing, Data anonymization.**

I.INTRODUCTION

Cloud computing is dramatically changing the way that organizations manage their data, owing to its attractive features such as robustness, low cost, and ubiquitous nature. However, privacy concerns arise whenever sensitive data is outsourced to the cloud where the data is processed and stored. The fact that users no longer have physical possession of the outsourced data makes it a formidable task to achieve the data confidentiality and integrity. As the data, in most cases encrypted, have to be not stored, but also processed in clouds, the cryptography-based data confidentiality and integrity protection approaches are not adequate to satisfy the security requirements. Privacy preserving in cloud environments includes two aspects: data processing security and data storage security. Data processing security covers the issues of how to protect user privacy at runtime in a virtualized cloud platform. Data storage security covers the issues of guaranteeing user data privacy when the data is stored in data center.[1]

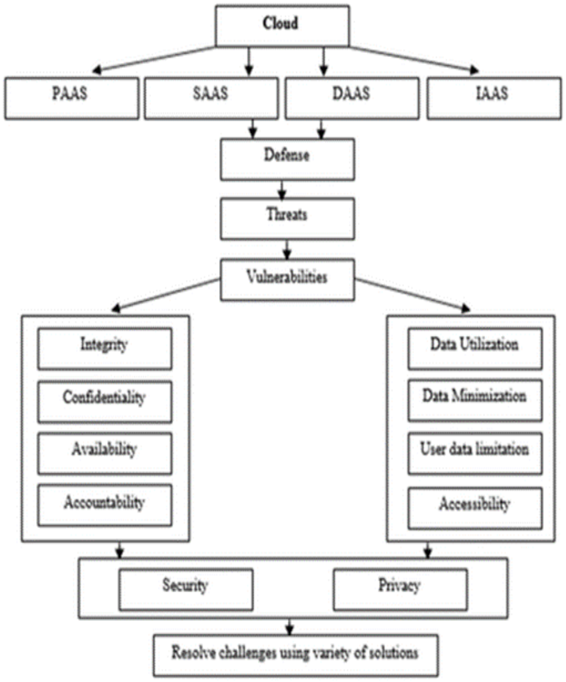

Fig: Privacy Protection in Cloud

II.PROBLEM DEFINITION

- Requirement for low latency and strong computing power in mobile devices, edge computing emerges as a paradigm for realizing service provisioning in the edge of mobile cloud. Among the numerous researches on location privacy preservation, cloud based location privacy preservation required, but it undoubtedly brings new problems such as data confidentiality and user privacy disclosure.

- This cloud privacy preservation task works on privacy preservation with data anonymization and trust mechanism.

III.BACKGROUND THEORY

Data anonymization:

- Data anonymization is the process of protecting private or sensitive information by erasing or encrypting identifiers that connect an individual to stored data. For example, you can run Personally Identifiable Information (PII) such as names, social security numbers, and addresses through a data anonymization process that retains the data but keeps the source anonymous.[2]
- Data anonymization is the process of changing data that will be used or published in a way that prevents the identification of key information. Anonymized data can be stored in a cloud and processed without concern that other individuals may capture the data.[3]

Disadvantages of Data Anonymization

- The GDPR stipulates that website must obtain consent from users to collect personal information such as IP addresses, device ID, and cookies. Collecting anonymous data and deleting identifiers from the database limit your ability to derive value and insight from your data. For example, anonymized data cannot be used for marketing efforts, or to personalize the user experience.

Trust Mechanism:

- Trust is a critical factor in cloud computing; in present practice it depends largely on perception of reputation, and self-assessment by providers of cloud services.[4]
- A reputation-based trust mechanism reflects the overall view of a community towards a cloud service provider. It can help with cloud service selection; but is insufficient for other important purposes. After establishing an initial trust on a cloud service, a cloud user needs to verify and re-evaluate that trust.

Trust is a mental state comprising:

1. expectancy - the trustor expects a specific behavior from the trustee (such as providing valid information or effectively performing cooperative actions).
2. belief - the trustor believes that the expected behavior occurs, based on the evidence of the trustee’s competence, integrity, and goodwill.
3. willingness to take risk - the trustor is willing to take risk for that belief.

Data Pre-Processing

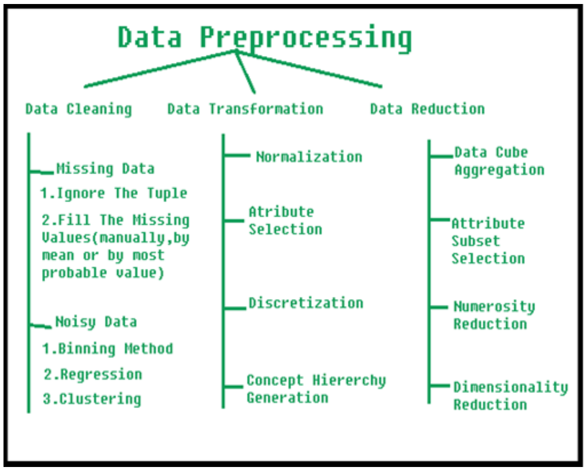

Fig: Data Pre-Processing

- Data preprocessing is a data mining technique that involves transforming raw data into an understandable format. Real-world data is often incomplete, inconsistent, lacking in certain behaviors or trends, and is likely to contain many errors.[5]
- Data preprocessing is a proven method of resolving such issues. Data preprocessing prepares raw data for further processing.

In addition, the system used for data preservation must be capable of enhancing the efficiency level of the database record services. In general, data are utilized for the purpose of recording a summarized personal information history that can be shared and retrieved by various users with the help of different online methods.[6]

Edge computing nodes near the mobile devices are deployed for task performing in the edge of the activity area of the mobile subscribers. Besides, the private user data be transmitted from mobile devices to edge computing nodes are classified into several parts, and these different data is transmitted to the edge computing nodes to calculate. In this way, edge computing enhances the real-time transmission rate and improves execution efficiency of tasks requiring great computing. Considering that humans are more sensitive to the delay of the interaction path, the users interaction experience is improved because edge computing performs cognitive tasks fairly accurately and quickly [7]. Not only that, but industrial production also becomes smarter and more efficient due to strong computing power of edge computing [8]. Whats more, edge computing has various advantages such as low latency and location awareness, better widespread geographical distribution than cloud computing, support streaming and real time applications [9].

IV.FLOW OF SYSTEM

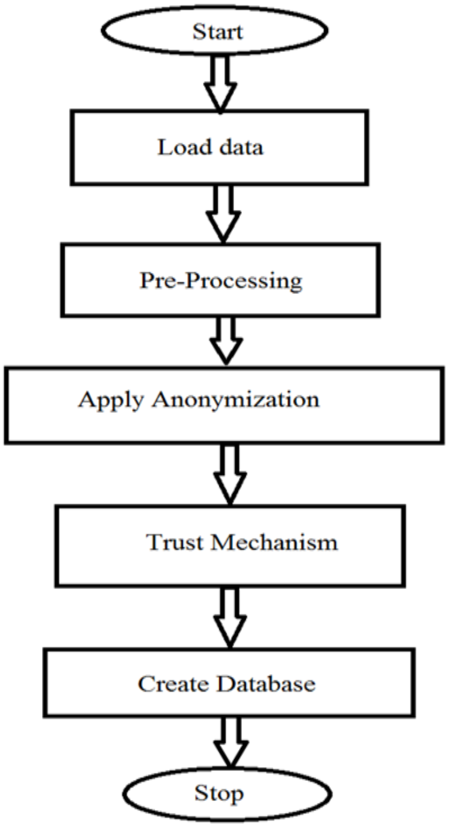

Fig: Flow of System

V.STEPS OF THE PROPOSED SYSTEM

Step 1: Data available on the different servers.
Step 2: For privacy-preservation anonymization can be apply.
Step 3: Trust mechanism enhances the privacy-preservation.
Step 4: Merge Trust mechanism and data anonymization.
Step 5: Create database.

VI.CONCLUSION

To fulfil people's requirements for low latency and strong computing power in mobile devices, edge computing emerges as a paradigm for realizing service provisioning in the edge of mobile cloud near the activity area of the mobile subscribers. Among the numerous researches on location privacy preservation, cloud-based location privacy preservation has become a hot topic, but it undoubtedly brings new problems such as data confidentiality and user privacy disclosure.

REFERENCES

[1] Niharika Singh, Ashutosh Kumar Singh" Data Privacy Protection Mechanisms in Cloud" Springer 2017

[2] https://www.imperva.com/learn/data-security/anonymization/

[3] Reenu Sara George, S Sabita" Data anonymization and integrity checking in cloud computing" IEEE 2013.

[4] Jingwei Huang, David M Nicol" Trust mechanisms for cloud computing" Springer 2013

[5] https://www.techopedia.com/definition/14650/data-preprocessing#:~:text=Data%20preprocessing%20is%20a%20data,likely%20to%20contain%20many%20errors.

[6] SHUKOR ABD RAZAK, NUR HAFIZAH MOHD NAZARI AND ARAFAT AL-DHAQM" Data Anonymization Using Pseudonym System to Preserve Data Privacy" IEEE 2020

[7] Kiryong Ha, Zhuo Chen, Wenlu Hu, Wolfgang Richter, Padmanabhan Pillai and Mahadev Satyanarayanan," Towards Wearable Cognitive Assistance," Proceedings of the 12th annual international conference on Mobile systems, applica- tions, and services, pp.6881, 2014.

[8] Lei Ren, Xuejun Cheng, Xiaokang Wang, Jin Cui and Lin Zhang," Multi-Scale Dense Gate Recurrent Unit Networks for Bearing Remaining Useful Life Prediction," Future Generation Computer Systems, vol.94, pp.601-609, 2018.

[9] Xiaolong Xu, Yuancheng Li, Tao Huang, Yuan Xue, Kai Peng, Lianyong Qi and Wanchun Dou," An Energy-Aware Computation Offloading Method for Smart Edge Computing in Wireless Metropolitan Area Networks," Journal of Network and Computer Applications, vol.133, pp.75-85, 2019.