A Novel Precision Bound Sliding Fixed Window Mechanism For Data Streaming Privacy

AchariJanhavi, KulkarniAishwarya ,GadakhMonali, AmbrePrajakta

Prof. G. D. Puri

Computer Engineering Department

Amrutvahini College Of Engineering, Sangamner

Abstract
In Access Control Mechanisms (ACM) and Privacy Protection Mechanisms (PPM) protect sensitive information from unauthorized users. The access control for a data stream allows us to access the database under Role Based Access Control (RBAC) policy that satisfies an authorized predicate sliding-window query. A PPM can use generalization of relational data to anonymize and satisfy privacy requirements such as k-anonymity and l-diversity. Generalization can reduce the delay in publishing of stream data through imprecision bound. Delay in sharing the data stream leads to false negatives i.e., it satisfies the sliding window query at the time instance of query evaluation. Access control policy is defined for the imprecision bound for each query. To optimize the delay in publishing the stream data is the most difficult task for Privacy Protection Mechanism. To overcome this challenge the imprecision bound for maximum number of queries has to be satisfied. The Precision-bounded Access Control for Privacy-Preserving data streams (PACE) problem generate an anonymitydata stream such that the average number of times the query imprecision bound is violated over a given time period.

Index Terms **- -**Arduino Processor, Arm 7 / PIC, Remote Farm Monitoring, GSM, Network communication

1.INTRODUCTION

Traditionally, DATA Stream Controlling Systems (DSMS) have been wished-for to process transactional data, e.g. INTERNET traffic, health checking, and device networks, (21. Access control mechanisms for data streams ensure that only the sanctioned parts of the stream are available to each user or role. Objects endangered under the access control mechanism are the queries or views of the data stream. If the searching evidence in the authorized view of the data stream is not secrecy protected, then the privacy of a person can be compromised even in the presence of access control. For example, for health monitoring and epidemic surveillance applications.Various participants including public health officials, epidemiologists. Doctors, and examines from various agencies and regions, should only access the views of patient streaming data for which they have the authorization. Furthermore, prior to publishing these views to the sanctioned participants, privacy of patients must be protected. The well-known privacy
Preservation techniques of k-anonymity have also been used for privacy protection of data streams. However, to the best of our knowledge, precision bounded access control along with privacy protection has not been investigated before data streams. The focus of this paper is to develop a privacy-preserving mechanism for issuing precision-bounded sanctioned views of streaming data. A precision bound access control framework for privacy-preserving data streams has been proposed by Access Control Mechanism and data are protected under Privacy Protection mechanism. In the PPM, it mainly focus on protecting the user information. Here, ad-min collect the micro data of the patient from various hospital and placed it into the database. After collecting, partitioning the data set in to two sets one is anonymous data another is sensitive data. Anonymization is done by using privacy requirements. In this way, Privacy Protection Mechanism is to protect the sensitive information. Access Control Mechanism gives permission to the user to access the authorized information. Once permission is permitted then imprecision bound has to set the boundary for the query predicate and check whether the user has the rights to access to data with the help of reference monitor. If user is an authorized user then the user can view and access the sensitive information so that Precision gets improved and time complexity is reduced in the system. Syndrome surveillance systems are used to detect and monitor the threads to public health at the state and country level. The department of health in a state collect the emergency symptoms from country hospital in an hourly basis and update the data, classify the data into syndrome categories according to department of health. An access control policy allows the roles to access the tuples under the authorized predicate i.e., Role CE1 can view tuples under permission P1 over the data stream in a 24hour basis and sliding the window for every 4 hours (slide=4hours) in which query can be executed. Permission under an access control policy assures only the authorized view of the data.

2 LITERATURE SURVEY

2.1

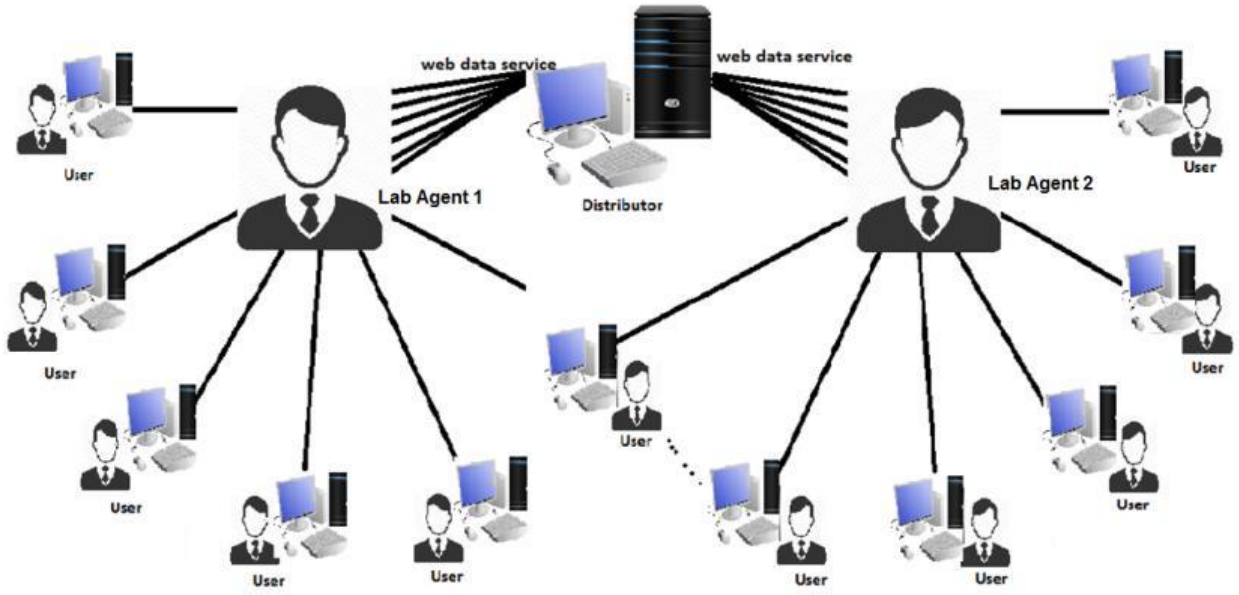
To The existing attitudes for privacy protection of data streams suppress the timestamp attribute. However, claims like access control do require time-print information to evaluate temporal queries over stream data. The attribute values in data stream tuples can be generalized to satisfy given privacy necessities. Generalization of relational data attributes introduces imprecision in the query results for access control mechanism. This imprecision can be reduced it the publishing of stream data is delayed. However, the delay announces false negatives in the query results in case the tuples satisfying the query predicate are not made available to the access controller mechanism, we provide a moving state and explain how haziness in an authorized assessment can he used to assess the effectiveness of the issuing data. Subsequently, author prove how a privacy-preserving mechanism (k-anonymity in our case) can be applied earlier to generating such authorized views. Through these examples we highlight the requirement for defining the imprecision bounds for publishing authorized data stream views.

2.2

In Pattern shadowing arrangements have been developed by public and federal actions to detect and display public condition emergencies. The reserve sector data (age, gender, location, time of arrival, symptoms, etc.) from section hospitals is together and is sent to the department of health at the state level on an hourly basis. The surveillance data stream is classified into syndrome sorts and is anonymised by the state department of health. The data is subsequently public with the department of strength in each county A role based access control policy. Role SE is above roles CEI and CE2 in the role Hierarchy and can execute all the approvals allowed to roles CFI and CF2. This policy allows the users to access the data stream view defined by the authorized queries, e.g., role CFI can view tuples under Permission Pl Liver the data stream in a 24-hour opening with a slide of 4 hours (i.e., updated every four hours).The Temporal Constraint (TC) TI defines a sliding-window (size = 24 hours, slide = 4 hours) of stream data upon which the query can execute. Permissions under an access control policy ensure that only the authorized view of the data stream is available to each user. Anonymization adds false-positives to the authorized view and the precision can be improved by delaying the stream data. However, the delay adds false-negatives for the views (when a tuple satisfying the view is not shared. The imprecision bound for each permission ensures that the authorized view is within the required tolerance at the time of predicate evaluation. The total imprecision for a view is the sum of false-positives and false-negatives and is used to gauge the utility of the authorized view.

3 PROPOSED SYSTEM

The proposed system emphasizes majority on the data privacy for streaming data as the data base can be secured by encrypting it but the streaming data which is in unencrypted format does not have any prevailing security mechanism. The proposed system maintains the hierarchy for the data available in the system and accordingly distributes the data amongst the users who can view the data for a specific time period based on the dynamic window size created for each different data. The threshold of the window size has been purposely kept dynamic as based on the data size available and the data being streamed, the window size i.e. data available for a specific period of time is displayed and the track for the data is also maintained in database for whether the specific user has seen the data or not.



Mechanism of Data Streaming:

- The Data Ad-min or Data Distributer who is none other than the person who is the research lab person who updated the data of the patients and thereby make the data available to the lap agents for making the same data available to the end users like doctors or patients etc so that the data can be streamed over the channel for the requesting user who is authorized to access the data.

- The Lab Agent has the authority to only pipeline the received lab report file in order to make the data visible to the authorized person. Lab Agent has the authority to set the Threshold of data viewing date and the user can view the lab report only for that particular time period or date for which the data is allocated.
- The user when receives the lab report can then view the lap report based on the data available in the file i.e number of bytes of data v/s number of seconds the report will be made available to the user.
- **The data report cannot be downloaded off line as the report being the very private information about the patient.**

Modules of Proposed System :

A precision bound access control framework for privacy-preserving data streams has been proposed by Access Control Mechanism and data are protected under Privacy Protection mechanism. In the PPM, it mainly focus on protecting the user information. Here, ad-min collect the micro data of the patient from various hospital and placed it into the database. After collecting, partitioning the data set in to two sets one is anonymous data another is sensitive data. Anonymization is done by using privacy requirements. In this way, Privacy Protection Mechanism is to protect the sensitive information. Access Control Mechanism gives permission to the user to access the authorized information. Once permission is permitted then imprecision bound has to set the boundary for the query predicate and check whether the user has the rights to access to data with the help of reference monitor. If user is an authorized user then the user can view and access the sensitive information so that Precision gets improved and time complexity is reduced in the system.

- Micro data Creation Module
- Data anatomize Module
- Data Distribution Module
- Data Stream Module
- Data Access Module

Mathematical Model

The proposed system can be mathematically represented as following sets and corresponding set operations:

Set D = {u0, u2, a1, d0, d1, d2, d3, d4, d5, d6}
Where,
d0 = upload data to be distributed
d1 = activate agent service/allocate data
d2= generate agent ID
d3 = generate user ID
d4 = Set resource usage threshold.
d5 = Start Resource Monitor.
d6 = Determine guilty user.

Set A = {a1, a2, a3, a4, u0, d1}
Where,
a1= getting user registered.
a2= supplying the data to user.
a3 = providing service to unauthorized user.
a4 = sending user details to distributor.

Set U = {u0, u1, u2, d1,a4}
Where,
u0= register to agent.
u1= request for data.
u2= get data from agent.
Intersection of the Set modules:

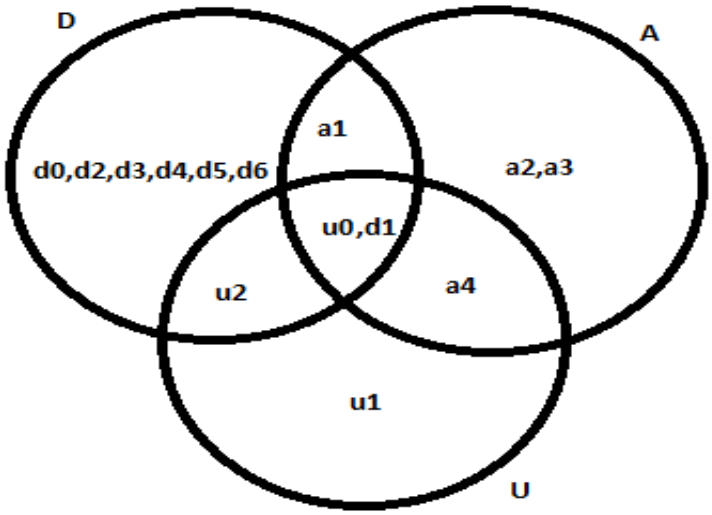


Fig 3.2 Intersection of Modules for data streaming and privacy preservation

4. IMPLEMENTATION RESULTS

4.1 Data Distributor Screen

Fig 4.1 Data Distribution from research lab Login

4.2 Lab Agent Activation Screen

Fig 4.2 Lab Agent Activation Panel

4.3 Report File Upload Panel

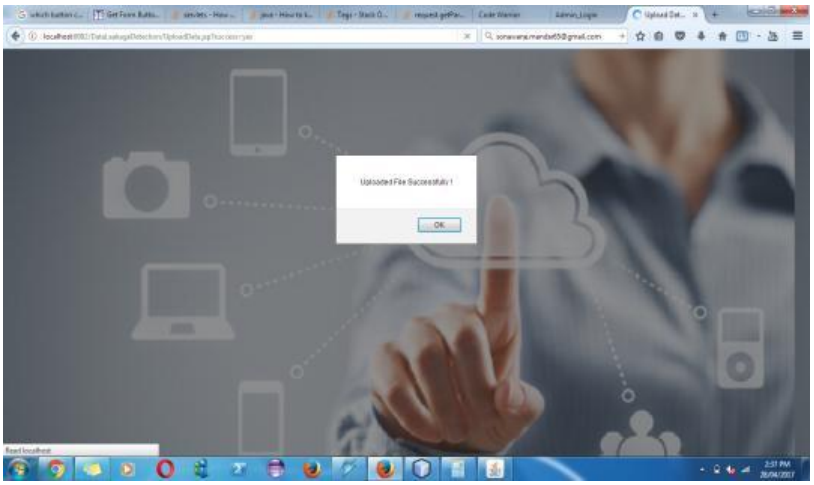


Fig 4.3 Research Lab Report File Upload

4.4 Data Allocation to User By Agent

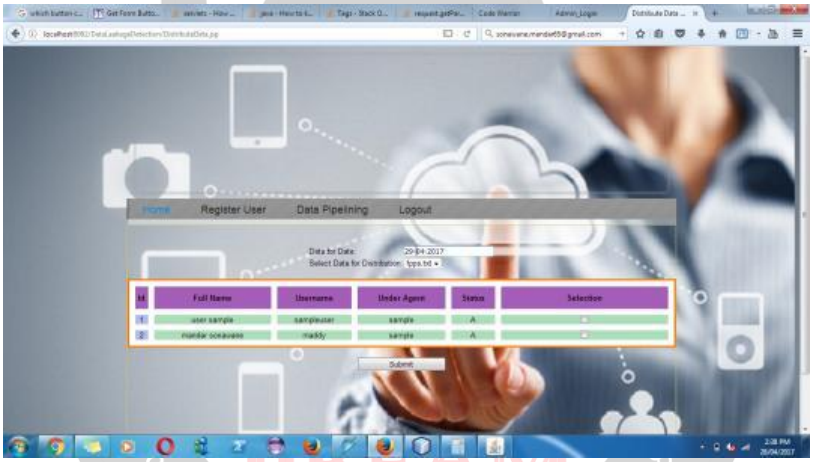


Fig 4.4 Data Allocation to User By Agent

4.5 Data Access by End User

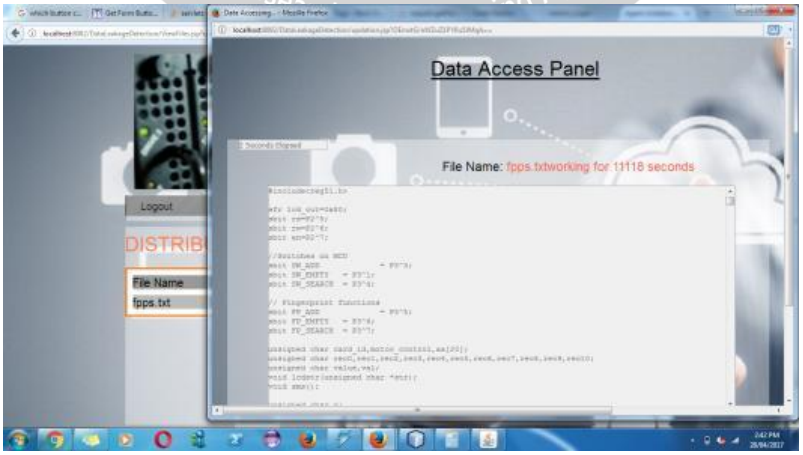


Fig 4.5 Data Access By End User

4.6 Data Leak Detected for Same Data Viewed

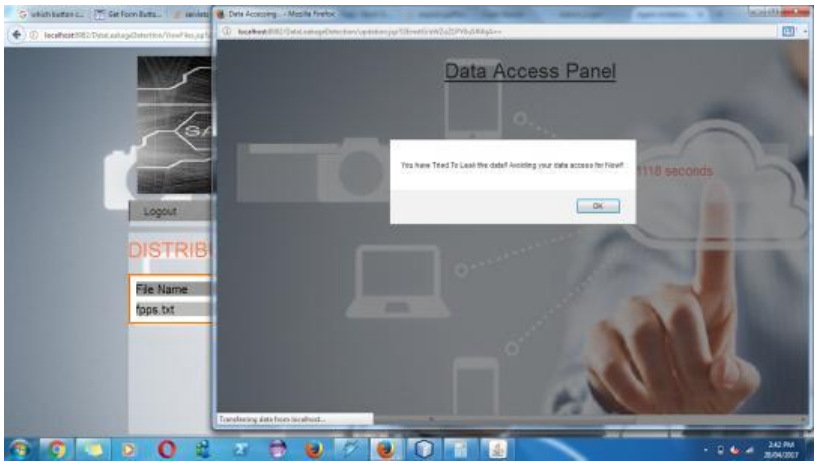


Fig 4.6 Data Leak Detected for Same Data Viewed

5. CONCLUSIONS

The human effort can be reduced with the proposed system. The provision of automatic control of fans providing cooling environment inside the playhouse makes the farmers work easy and it can be achieved by using the proposed system with less hardware and using simple operations. Combined wireless RF (IEEE 806.15.4) communication technology with data acquisition system is used; we build wireless data acquisition system based on Eduino processor and the wireless sensor network. Eduino is used to maintain high accuracy. At regular interval PC Master will send the request for data to wireless sensor node through sub masters. The request will be sent in the form of frames. The frame transmitted by PC master will contain the sub master id as well as the wireless sensor node id from where the data is to be retrieved.

6. ACKNOWLEDGEMENT

We would like to take this opportunity to express our profound gratitude and deep regard to our guide Prof. Guide Name for his/her exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. His / Her valuable suggestions were of huge help throughout our project work. His / Her perceptive criticism kept our working to make this project in a much better way. Working under his/her is an extremely knowledgeable experience for us.

7. REFERENCES

[1] S.Chaudhuri, T. Dutta, and S. Sudarshan, ”Fine Grained Authorization through Predicated Grants,” Proc. IEEE 23rd Intl Conf. Data Eng.,pp.2007.
[2] D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn, and R, Chandramouli, ”Proposed NIST standard for role based access control,” ACMTrans.Inf.Syst. Security, vol. 4, no. 3, pp. 224274,2001.
[3] G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis, ”A framework for efficient data Anonymization under privacy and accuracy constraints”, ACMTrans. Database Syst., vol. 34, no. 2, p. 2009.
[4]K. LeFevre, R. Agrawa, V. Ercegovac, R. Ramakrishnan, Y. Xu, and D. De-Witt, ”Limiting Disclosure in Hippocratic Databases,” Proc. 30th Intl Conf.Very Large Data Bases, pp. 108-119.2004.
[5] K. LeFevre, D. DeWitt, and R. Ramakrishnan, ”Mondrian multidimensional k-anonymity,” in Proc. 22nd Int. Conf. Data Eng., p. 25.2006.
[6] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, ”ldiversity: Privacy beyond kanonymity,” ACM Trans. Knowl. Discov.Data, vol. 1, no. 1, p. 3.2007.
[7] R. Nehme, E. Rundensteiner, and E. Bertino, ”A security punctuation framework for enforcing access control on streaming data,” in Proc.IEEE 24th Int. Conf.Data Eng., pp. 406415,2008.
[8] Z. Pervaiz, W.G. Aref, A. Ghafoor, and N. Prabhu, ”Accuracy constrained privacy-preserving access control mechanism for relational data,” IEEETrans. Knowl. Data Eng., vol. 26, no. 4, pp. Apr.2014

