

# Customized Privacy Preservation Model for Cloud Environment

JyotiNagwanshi<sup>1</sup>, Mrs. Sarika Jain<sup>2</sup>

<sup>1,2</sup>M. Tech, Department of CSE, Assistant professor, Department of CSE, 12 SAIT College  
Indore (M.P.), India

**Abstract-** Sensor nodes are one of the major utility to control the complete home appliance and can be known as smart home controller. Data Analytics may used to explore pattern and explore more relevant a useful use cases. Privacy preservation also plays crucial factor during the whole phenomena. The complete solution generates a need to improve the capability of access control model. The project will develop solution to maintain the privacy during the analytics process on smart home data. Subsequently, access control model will help to categorize and priorities the database attributes and data according to access. It will help to maintain data privacy during web mining.

**Keywords-** Access Control, Privacy Protection, Sensitive Data, K-mean algorithm.

## I. INTRODUCTION

Such as price, product positioning, or staff Data mining is primarily used today by companies with a strong consumer focus - retail, financial, communication, and marketing organizations. It enables these companies to determine relationships among "internal" factors skills, and "external" factors such as economic indicators, competition, and customer demographics. And, it enables them to determine the impact on sales, customer satisfaction, and corporate profits. Finally, it enables them to "drill down" into summary information to view detail transactional data.

With data mining, a retailer could use point-of-sale records of customer purchases to send targeted promotions based on an individual's purchase history. By mining demographic data from comment or warranty cards, the retailer could develop products and promotions to appeal to specific customer segments.

For example, Blockbuster Entertainment mines its video rental history database to recommend rentals to individual customers. American Express can suggest products to its cardholders based on analysis of their monthly expenditures. "Privacy is a state in which one is not observed or disturbed by other people" Privacy protection policy is an approach to isolate the sensitive information from unauthorized access. The complete work concludes that Map Reduce Framework does not consist proposed security policy and suffering with data leakage problem. Subsequently, Security threat attack is

also possible and malicious framework may give open system access to unauthorized user.

## II. RELATED WORK

Veenal et al. In[1] proposed that data warehousing represents an ideal vision of maintaining a central repository of all organizational data. Centralization of data is needed to maximize user access and analysis. Dramatic technological advances are making this vision a reality for many companies. And, equally dramatic advances in data analysis software are allowing users to access this data freely. The data analysis software is what supports data mining.

Quang Tran et al. In[2] described about data structure that holds the list of users that the operating system as a whole recognizes, along with a flag which indicates whether each user may read, write, execute, delete, or modify the file (or some combination of these). Whenever a user tries to perform any of these actions on the file, the operating system checks the file's ACL and determines whether the requested action for that user, the data is appended; if not, the append operation fails.

Travis Mayberry et al. In[3]The attributes do not necessarily need to be related to appending data to the file, for example is allowed. If the action is allowed each other, and in fact, the attributes that go into making a decision can come from disparate, unrelated sources. They can be as diverse as the date an employee was hired, to the projects on which the employee works, to the location where the employee is stationed, or some combination of the above. One should also note that an employee's role in the organization can serve as one attribute that can be (and often is) used in making an access control decision.

Tien Tuan et al. In[4] Privacy is a state in which one is not observed or disturbed by other people" Privacy protection policy is an approach to isolate the sensitive information from unauthorized access. The complete work concludes that MapReduce Framework does not consist proposed security policy and suffering with data leakage problem.

## III. PROBLEM STATEMENT

One of the challenges of bringing security to cloud computing is that users and developers want to spend as little mental effort and system resources on security as possible.

Completely novel APIs, even if secure, are unlikely to gain wide acceptance. Therefore, a key research question is how to design a practical system that (1) enables efficient distributed computations, (2) supports a familiar programming model, and (3) provides precise, rigorous privacy and security guarantees to data owners, even when the code performing the computation is untrusted.

The problem in the web mining arises when confidential information is derived from released data by unauthorized users. This problem is commonly known as the “database inference” problem. Recent advances in web mining field have lead to increased concerns about privacy. There are mainly three issues which arise in data mining process are as follows:

- A. Privacy issue: Because of privacy issues, people are afraid of their personal information is collected and used in unethical way that potentially causing them a lot of troubles.
- B. Security issue: There have been a lot of cases that hackers accessed and stole big data of customers from big corporation such as Ford Motor Credit Company with so much personal and financial information available, the credit card stolen and identity theft become a big problem.
- C. Misuse of information/inaccurate information: Information is collected through data mining intended for the ethical purposes can be misused. This information may be exploited by unethical people or businesses to take benefits of vulnerable people or discriminate against a group of people.

IV. PROPOSED SOLUTION

The need is to develop efficient systems that can exploit this potential to the maximum, keeping in mind the current challenges associated with its analysis, structure, scale, timeliness and privacy. There has been a shift in the architecture of data-processing systems today, from the centralized architecture to the distributed architecture.

Access Control is primary principle of information security and specifies “Who Can Access What”. Implementation of Control mechanism will filter out complete user access to framework data and avoid data leakage. It will also help to classify the request and response according to user rights.

To implement the access control, a list of services and users are expected. Access Control Matrix will give relation between users and services. It will classify the all user into categories and also services as same. The complete phenomena will help develop structured security plan to implement privacy protection mechanism using Access Control.

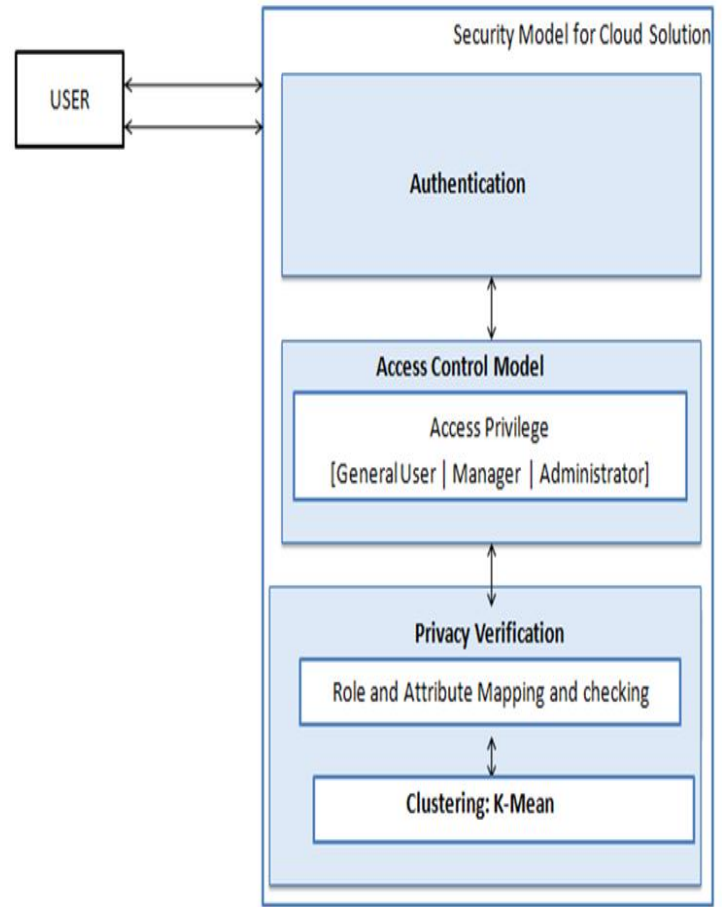


Fig.1: Proposed Architecture

The complete solution will implement into current framework to avoid security attack. Following salient features will be achieved by implementing the proposed solution.

- A. Proposed solution will consider a large Super Market dataset as input to retrieve important information.
- B. AK-mean algorithm will be implemented in application for clustering the data and efficiently retrieve credential information.
- C. Attribute Based Access Control Model with Access Matrix will be implements for proper access and rights classification to define “Who can Access What”
- D. Security Model with Service Component will be configured to process and execute the complete application in efficient manner.
- E. Performance will be measured after searching and information retrieval operation in term of computation & execution time, memory overhead and privacy management.

V. IMPLEMENTATION RESULT

Screenshots to demonstrate the complete implementation is cited below:

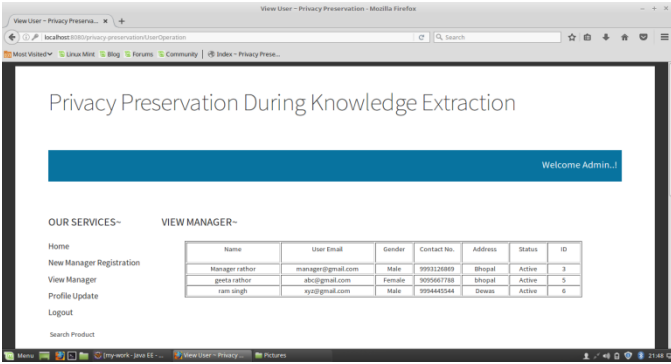


Fig.2: Service Page

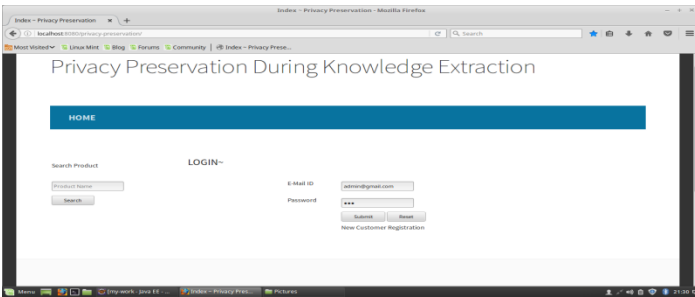


Fig.3: Login Page

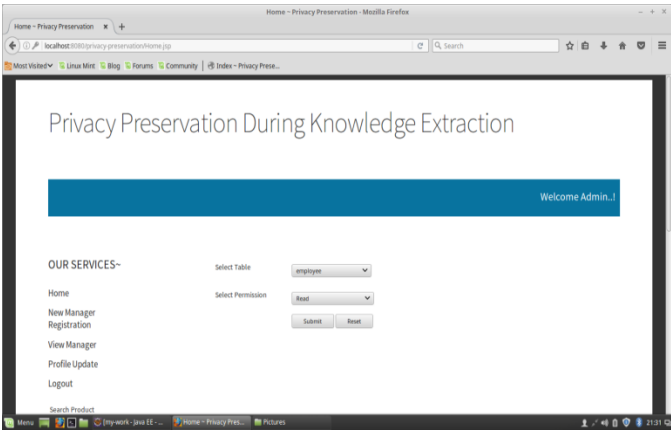


Fig.4: Home Page

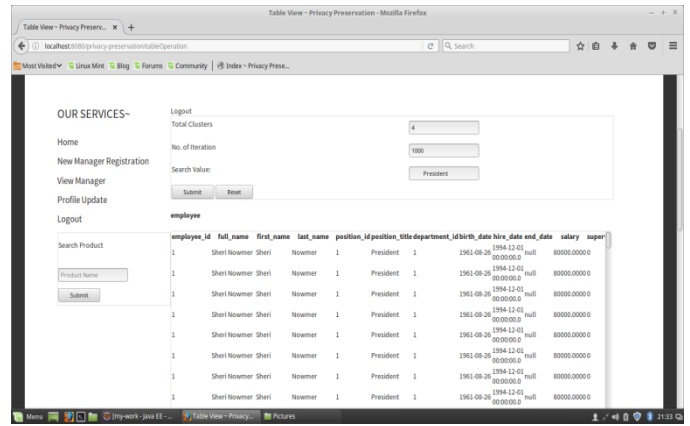


Fig.5: Searched Product

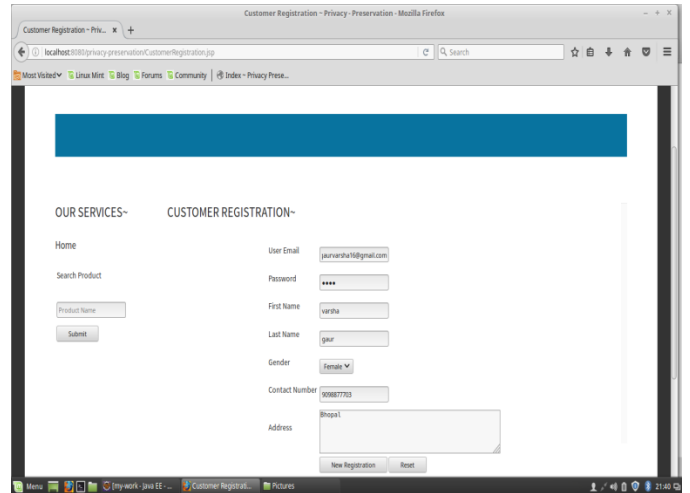


Fig.6: Registration Page

VI. RESULT

The complete solution has been evaluated on basis of number of occurrence found by in permitted tables along with search text. A snap view of complete result analysis is shown in below tables;

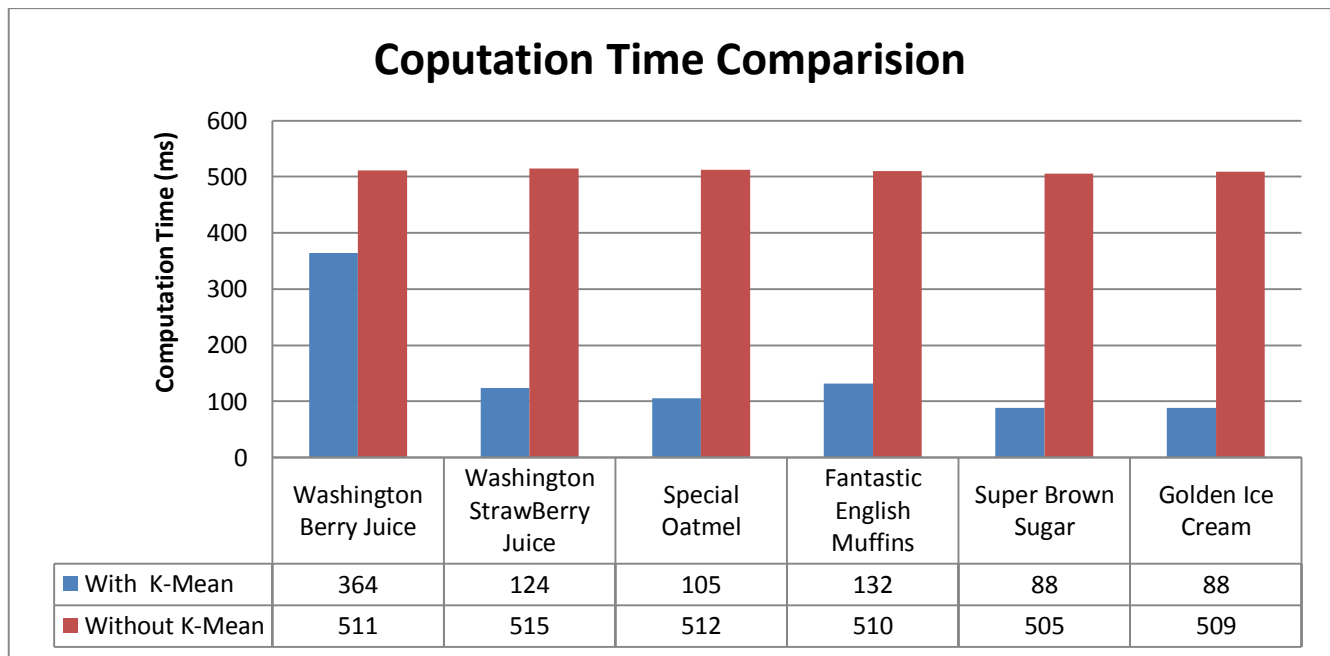
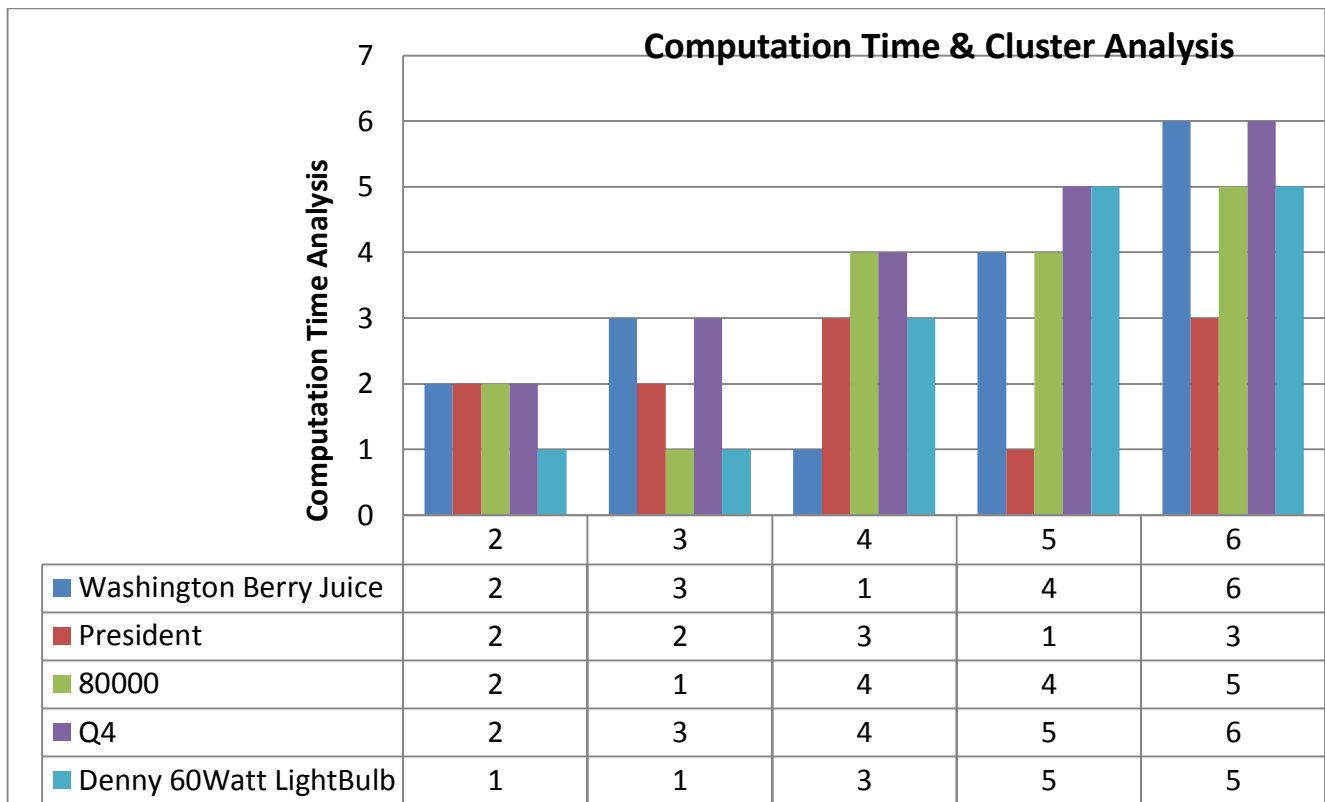


Fig.8: Comparison of computation time

Similar to this cluster based result observations certain test cases are also performed on developed solution and record the observation. A list of respective observations is cited below;

A. Login validation and credential check has been applied and found appropriate answer for valid credentials and reject reply for invalid.

B. Session management verification has been performed after logout using back event.

Invalid update credential check is also performed.

#### VII. CONCLUSION

The complete work concludes that proposed work will not only suggest a solution to implement access control mechanism with proposed security model but will help to achieve better performance in large data set. Here a hybrid security model has been proposed based on ABAC and RBAC to manage table permissions and access. A super market dataset has been considered as the source of information and data schema to implement the proposed solution and evaluate the performance.

The complete solution implements the four different user roles and classifies their responsibility and security according to attributes. Complete solution is evaluated on basis of number of occurrence found with provided security facility. The complete work ends with satisfactory results.

Future Work the complete solution is implemented for cloud computing environment. It can be extended for large dataset and perform analysis using Hadoop server.

#### VIII. REFERENCES

- [1]. Veena1, Devidas, "Data Anonymization Approaches for Data Sets Using Map Reduce on Cloud: A Survey" NMAM Institute of Technology, Nitte, Karnataka, India.
- [2]. Quang Tran, Hiroyuki Sato, "A Solution for Privacy Protection In MapReduce". Graduate School of Engineering, The University of Tokyo.
- [3]. Travis Mayberry, Erik-Oliver Blass, Agnes Hui Chan, "PIRMAP: Efficient Private Information Retrieval for MapReduce", Proceedings of Financial Cryptography and Data Security (FC'13), pp. 371—385, Okinawa, Japan,
- [4]. Tien Tuan Anh Dinh, Prateek Saxena, Ee-Chien Chang, Beng Chin Ooi, Chunwang Zhang, "M 2R: Enabling Stronger Privacy in MapReduce" Computation School of Computing, National University of Singapore.
- [5]. Indrajit Roy Srinath T.V. Setty Ann Kilzer Vitaly Shmatikov Emmett Witchel, "Airavat: Security and Privacy for MapReduce". The University of Texas at Austin.
- [6]. [https://hadoop.apache.org/docs/r1.2.1/mapred\\_tutorial.html#Overview](https://hadoop.apache.org/docs/r1.2.1/mapred_tutorial.html#Overview).



Jyoti Nagwanshi received the B.E. degree from Shri Govind Ram Seksariya Institute of Technology and Science (S.G.S.I.T.S) Indore in May 2012 in field Information Technology currently pursuing M.Tech from Shri Aurobindo Institute of technology, her interest in cloud computing, networking, security.