International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Efficient Implementation of Big Data Access Control Scheme with Privacy-Preserving Policy

Niranjanamurthy M., Esha Jain, Bhawna Nigam, Sushmitha M.

Abstract: ***In the time of big data, cloud computing, an immense measure of information can be created rapidly from different IT, non-IT related sources. Towards these big data, cloud computing, customary PC frameworks are not up to required skilled to store and process this information. Due to the adaptable and flexible figuring assets, distributed computing is a characteristic fit for putting away and preparing big data. With cloud computing, end-clients store their information into the cloud server and depend on the advanced cloud server to share their information to different clients. To share end-client's information to just approved clients, it is important to configuration access control systems as indicated by the prerequisites of end clients. When re-appropriating information into the cloud, end-clients free the physical control, virtual physical control of their information. In addition, cloud specialist co-ops are not completely trusted by end-clients, which make the entrance control additionally testing. on the off chance that the conventional access control systems (e.g., Access Control Lists) are connected, the cloud server turns into the judge to assess the entrance approach and settle on access choice. Subsequently, end-clients may stress that the cloud server may settle on wrong access choices purposefully or accidentally and uncover their information to some unapproved clients. To empower end-clients to control the entrance of their own information, a proficient and fine-grained huge information access control plot with protection saving strategy is proposed. In particular, the entire trait (as opposed to just its qualities) in the entrance strategies are scrambled. To help information decoding, encoding, a novel Attribute Bloom Filter is utilized [14][16] to assess whether a characteristic is in the entrance arrangement and find the accurate position in the entrance approach on the off chance that it is in the entrance strategy. Just the clients whose traits fulfill the entrance arrangement are qualified to unscramble the information.***

Index Terms: ***Big data, System Architecture, Procedural Design, encryption Module, User Interface Design, MVC Architecture.***

I. INTRODUCTION

Big-data states to a process used when traditional-data mining and management techniques can't expose the understandings and meaning of the fundamental data. Data that is un-structured or time-sensitive or just very huge can't be handled by relational data-base system. In the present time of big data, a tremendous measure of information can be produced rapidly from different IT, non-IT sources. Towards these big data, traditional PC frameworks are not skilled to store and process this information's. server to share their information to different clients [13]. To share end-client's information to just approved clients, it is important to configuration access control systems as indicated by the necessities of end clients. When re-appropriating information into the cloud, end-clients free the physical control of their information. In addition, cloud specialist organizations are not completely trusted by end-clients, which make the entrance control additionally testing. [11]

Objectives:

- The objective of the system is to provide an effective and fine-grained big data Access control conspire with privacy-preserving strategy.
- The system will provide more data access control.
- The system also provides more security by hiding attributes.

Purpose: The main purpose of the structure is to provide more data access control and more security. Before outsourcing data into the cloud whole attribute values are hidden to secure against plain text attacks.

Scope: To know the unauthorized accessibility this scheme gives the chance to end users to select the authorized users, so without the permission of end users the data consumers cannot view any attributes. The registered data consumers can login to the system but to view the attributes they need to get end users permission.

Applicability: The concept is applicable in any organization for outsourcing the data to other persons where the data owner can control the accessibility and the data is secure against plaintext attacks.

II. LITERATURE SURVEY

Trait grounded encryption frameworks where encrypted-specified induction structures (likewise called cipher-text policies) are covered up. An encryptor can encode data/information with a shrouded access structure. A decryptor gets her mystery key related with her traits from a confided in expert ahead of time and if the properties related with the decryptor's mystery key don't delight the entrance structure related with the scrambled information, the decryptor can't unscramble the data or supposition even what access structure was measured by the encryptor. In security thought, the real decryptor can't get the information about the entrance structure related with the scrambled insights more than the way that she can unscramble the records. [1] Data outpouring tendency provided the vision meaning to the buzz word "Big-data". If we associate with old-style data,

Manuscript published on 30 August 2019.
*Correspondence Author(s)
Dr. Niranjanamurthy M., Department of Computer Applications, M S Ramaiah Institute of Technology, Bangalore, India.
Dr. Esha Jain, (Corresponding Author), School of Management, The NorthCap University (Formerly ITM University), Gurugram, India. Email ID: dr.eshajain1985@gmail.com
Dr. Bhawna Nigam, Department of Information Technology, Institute of Engineering & Technology, Devi Ahilya University, Indore, India.
Ms. Sushmitha M., Department of Computer Applications, M S Ramaiah Institute of Technology, Bangalore, India.

Big-data exhibitions some sole physiognomies like it is commonly huge and formless type of data that can't be fingered using outdated databases. Henceforth novel system designs are obligatory for the following processes i.e. data gathering, data broadcast, storage, and large-scale data dispensation mechanisms. The definition of Big data has been presented from many aspects. Here author analyzed Big-data system architecture and various challenges of Bigdata.[2].

Seizing human drive has become obtainable in feature due to the progression of motion sensor technology combined by micro-machine and due to the one of visual footage by high-speed and high resolve image sensors. Subsequently, can without much of a stretch record the human action as the body development Big-Data and dissect it to mission ability to turn into a specialist of an objective body drive. [3]

Big-data analytics as a new significant field of education for both investigators and doctors, representative the important request for explanations to commercial problems in a data-driven knowledge-based economy. Additionally, experiential studies examining the influences of the budding technology on organizational presentation, particularly the effect of organizational ethos on the five Big V s of big data, continue rare. Author suggests a theoretic outline that labels how each type of organizational nation - hierarchy, clan, adhocracy, and marketplace - has influences on each Big V of big data.[4]

Researchers found there were 13 predominant subjects catching 49% of the big data generation in journals during 2011-2016 yet protection and security themes represented just 2% and this pattern as of late dropped to under 1%. Consequently, we contended that we must invigorate all the big data protection security look into. [5].

The data-privacy safety model of big-data for information owners is presented in detail, counting procedure design, logic-design, difficulty analysis and security-analysis. Then, the query privacy defense model of big-data for normal users is introduced in detail, counting query procedure design and query mode-design. Difficulty analysis and safety examination are performed.[6]

The security organization of databases includes multifaceted issues for the businesses. The difficulty of security amount needs to apply surges with the most intricate database. The arithmetical queries related with numerical database uses the collective functions such as min, max, average and count to provide statistical data/ information about entries. The data susceptibilities raise the security issues because of ingenious mixture of statistical queries to get confidential data for the individual entry.[7]

Using distributed computing, individuals can store their data on remote servers and license data access to open customers through the cloud servers [12]. As the re-appropriated information are probably going to contain sensitive privacy data, they are ordinarily encoded before transferred to the cloud. This, in any case, by and large limits the convenience of redistributed information due to the inconvenience of looking over the encoded data. In this paper, they address this issue by structure up the fine-grained multi-catchphrase search plots over encoded cloud data. Their unique commitments are three-overlay. In the first place, they presented the importance scores and inclination factors upon catchphrases which empower the exact watchword search and customized client experience. Second, they build up a useful and extremely proficient multi-watchword search plot. [8]

In cipher text-policy attributed-based encryption (CP-ABE), each cipher content is marked by the encryptor with an entrance structure (additionally called cipher text policy) and every private key is related with a lot of traits [12]. A client ought to have the option to decrypt a cipher text if and just if his private key characteristics fulfill the entrance structure. The conventional security property of CP-ABE is plain content protection, which cipher text uncover no data about the fundamental plain-content. At ACNS'08, Nishide, Yoneyama and Ohta presented the thought of cipher text-policy hiding CP-ABE. Notwithstanding securing the security of plain contents, cipher text-policy concealing CP-ABE likewise ensures the portrayal of the entrance structures related with cipher texts. They saw that cipher text-policy hiding CP-ABE can be developed from attribute-hiding inner-product predicate encryption (PE), and exhibited two developments of cipher text-policy hiding CP-ABE supporting limited access structures, which can be communicated as AND gates on multi-esteemed properties with trump cards. [9] [15]

Acceptance of big data in Healthcare meaningfully surges security and patient privacy anxieties. At the onset, patient info is warehoused in information centers with varying levels of security. Traditional security solutions can't be straight applied to big and integrally varied data sets. With the upsurge in prominence of healthcare cloud arrangements, multifaceted nature in verifying gigantic appropriated Software as a Service (SaaS) solutions surges with varying data sources and formats. Consequently, big data administration is essential before presenting data to analytics. [10]

III. SYSTEM DESIGN AND FLOW

A System Architecture is an applied model that characterizes the structure, conduct and more perspectives on a framework. An architecture description is a formal depiction and portrayal of a framework, composed such that supports thinking about the structure of the framework.

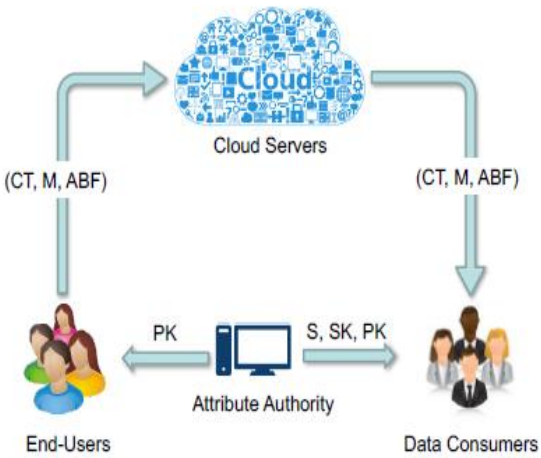

Figure I: System Architecture

Retrieval Number: J93820881019/19©BEIESP
DOI: 10.35940/ijitee.J9382.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

System Flow chart

System flowchart is the graphical portrayal of the progression of information in the framework and represents the work procedure of the framework.

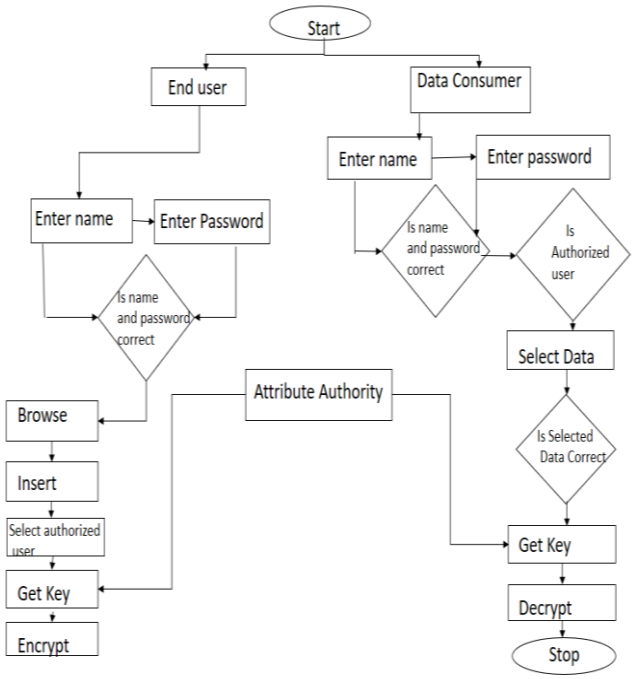

Figure II: System Flow chart

IV. MODULES AND IMPLEMENTATION

A module is a different unit of programming or equipment. Regular qualities of measured segments incorporate compactness, which enables them to be utilized in an assortment of frameworks, and interoperability, which enables them to work with the parts of different frameworks.

• End User Application
• End User Encryption
• Cloud Service Provider
• Data Consumer Request
• Retrieve Data

End user application Module

- End user have to register into the cloud server.
- Then login to the system and select the data they need to share.
- The authority for the data is very important. So that user will give authorization permission to some of the consumers.

End user encryption Module

- End user send the request to attribute authority.
- Attribute authority receives the request from end user.
- And generates the key for the encryption purpose.
- Advanced encryption standard algorithm is used for the encryption purpose.
- End user will encrypt the data by using the received key from attribute authority.

Cloud server provider Module

- Cloud service provider receives the request from the consumer and provides the relevant data to them.
- Cloud service provider acts as the storage place.

Data Consumer Request Module

- Data consumer need to register into the service provider and then login to the service provider.
- Then service provider send request to the cloud service provider.
- It consists of book related request. Because the data set contain the book relevant data.
- This request is processed in the cloud service provider.

Retrieve data Module

- Cloud service provider receives the request from the cloud consumer.
- And searches for the relevant data to the query from the consumer.
- This data is transferred to the cloud consumer.
- And the consumer sends the request to the attribute authority for key.
- Then receives the key from the attribute authority and uses it to decryption.

Procedural Design

Procedural plan is best used to demonstrate programs that have an undeniable progression of information from contribution to yield. It represents the architecture of a program as a lot of connecting forms that pass information starting with one then onto the next.

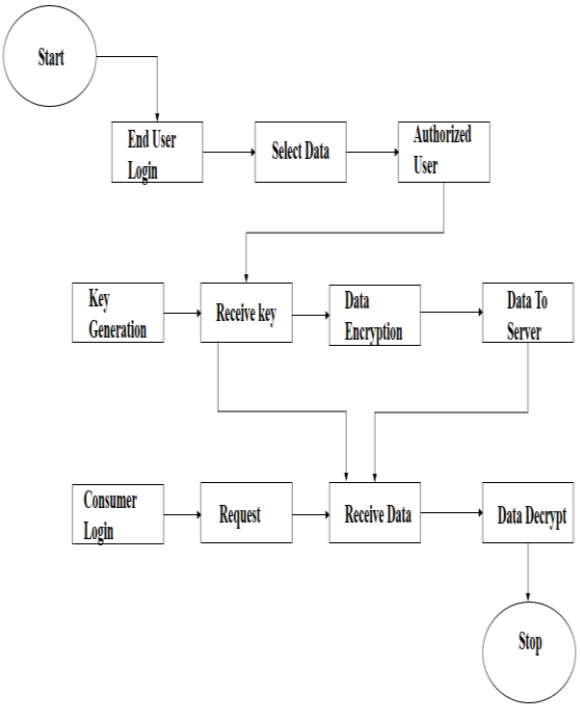

Figure III: Procedural Design

Algorithm Design: Algorithm configuration is a particular technique to make a numerical procedure in critical thinking forms.

AES encryption calculation:

Stage 1: Start

Stage 2: Derive the arrangement of round keys from the cipher key.

Stage 3: Initialize the state exhibit with the square information (plain text).

Stage 4: Add the underlying round key to the beginning state exhibit.

Stage 5: Perform nine rounds of state control.

Stage 6: Perform the tenth and last round of state control.

Stage 7: Copy the last state exhibit out as the encoded information (cipher text).

Stage 8: Stop

User Interface Design:

Use case outlines are normally alluded to as conduct graphs used to depict a lot of activities (use cases) that frameworks (subject) ought to or can perform in a joint effort with at least one outside clients of the framework. The primary motivation behind utilization case chart is to indicate who collaborates with the framework, and the principle objectives they accomplish with cooperation.

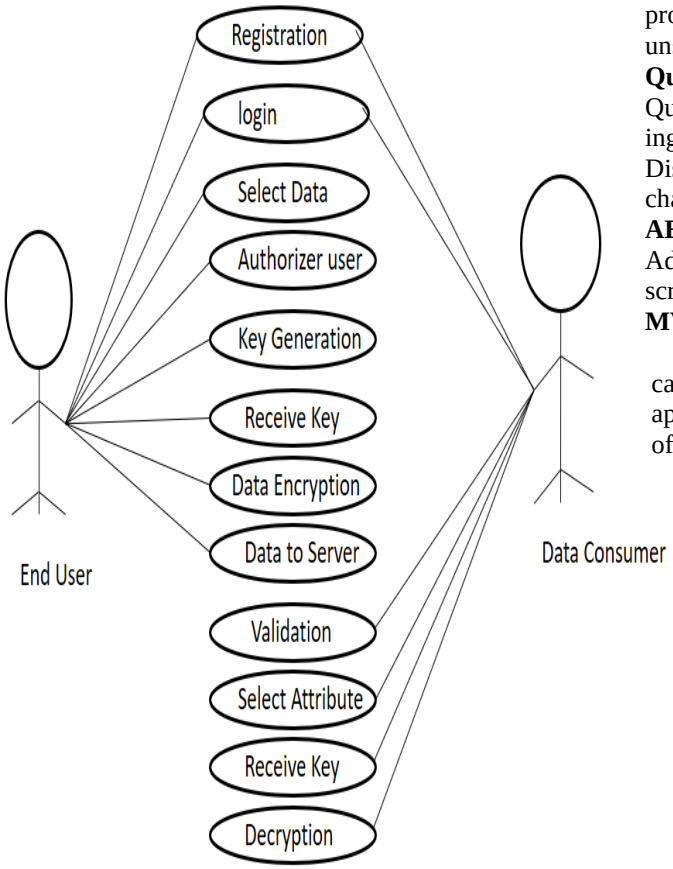

Figure IV: User Interface Design

Security Issues

• Authorized accessibility:

The End-user must register to the cloud, by providing username and password. End-user is responsible for giving accessible permission only for authorized user. Without the permission the Data-consumer can login but cannot perform any other actions. The End-user can give access permission only to the users who are already registered to the cloud.

• Validation process:

The registered Data-Consumer can login to the system but in order to perform any other activities, validation process will be done. The Data-consumer name should be present in the End-user's selected authorized user list.

• Attributes checking process:

The data consumers should select all the attribute correctly. If the data consumers fail to select all the attributes correctly, then they cannot decrypt the data. In order to decrypt the data, again they should select all correct attributes.

Execution approaches

Execution is the phase of the task when the hypothetical structure is transformed out into a working framework. In this way it tends to be viewed as the most basic stage in the accomplishing a Successful new framework.

The entire quality (as contrasting to just its qualities) in the ingress provisions are scrambled. To help data decoding, encoding, a novel Attribute Bloom Filter is utilized to measure whether a trait is in the ingress method and discover the accurate position in the ingress strategy on the off chance that it is in the entrance arrangement. Just the clients whose properties fulfill the entrance arrangement are qualified to unscramble the information.

Quality Bloom Filter

Quality Bloom Filter is to assess whether a property is in the ingress arrangement and

Discover the careful position in the access policy on the off chance that it is in the access policy.

AES encryption

Advance Encryption Standard calculation is utilized to scramble the information and decode the information.

MVC Architecture

Model **V**iew **C**ontroller or MVC as it is prominently called, is a product configuration design for creating web applications. A Model View Controller pattern is comprised of the accompanying three sections:

- **Model** - The most minimal dimension of the example which oversees looking after information.
- **View** - This oversees showing all or a segment of the information to the client.
- **Controller** - Software Code that controls the communications between the Model and View.

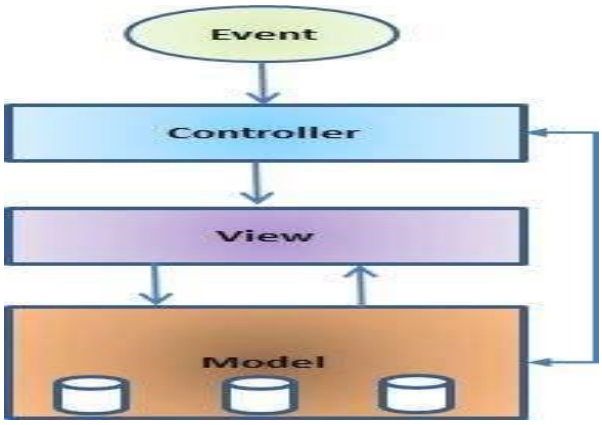

Figure V: MVC Architecture

Retrieval Number: J93820881019/19©BEIESP
DOI: 10.35940/ijitee.J9382.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

MVC is mainstream as it segregates the application rationale from the UI layer and supports detachment of concerns. Here the Controller gets questions from the buyers and gives openness. The View at that point utilizes the information arranged by the Controller to produce a last respectable list.

V. RESULTS AND DISCUSSION

Test Reports:

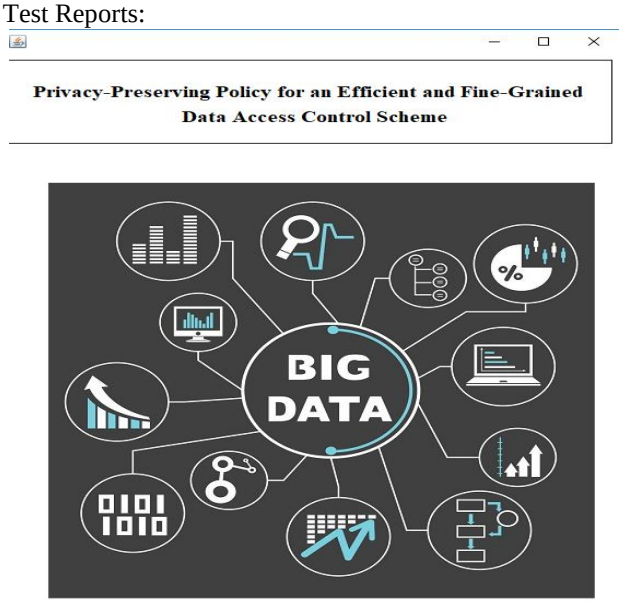

Figure VI: Home Page

As soon as the application runs this is the home page that appears for all next functionalities to be used.

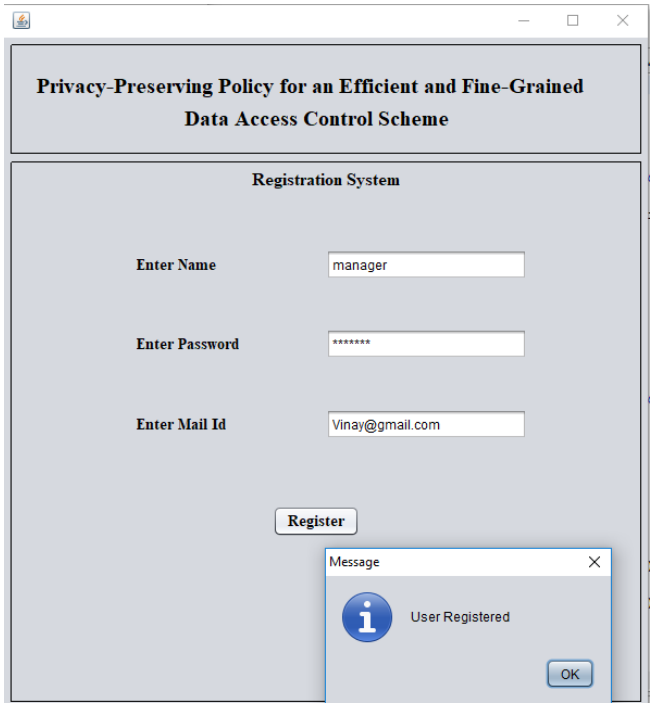

Figure VII: User Registration Page –
Here user has to register by entering his name and mail id for login credentials.

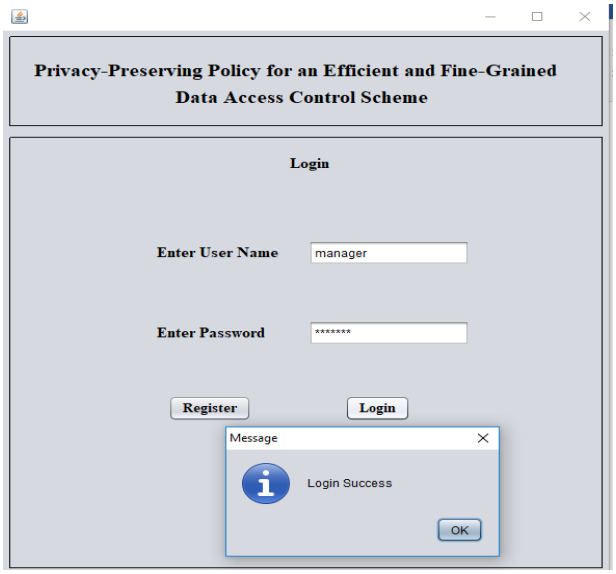

Figure VIII: End User login page –
Here the user has to give his login credentials to login into the application and do the necessary actions.

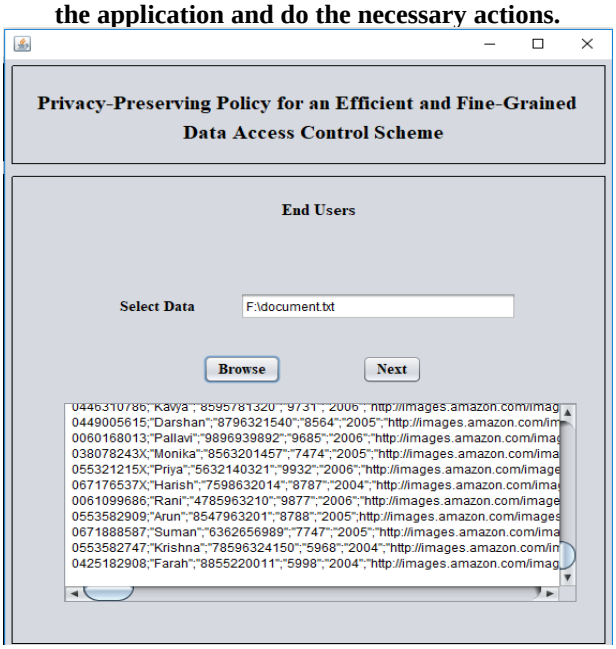

Figure IX: End User Page To Browse Data –
Here The User Can Browse The Document Based On The Name And The Do The Necessary Actions For That Particular Document.

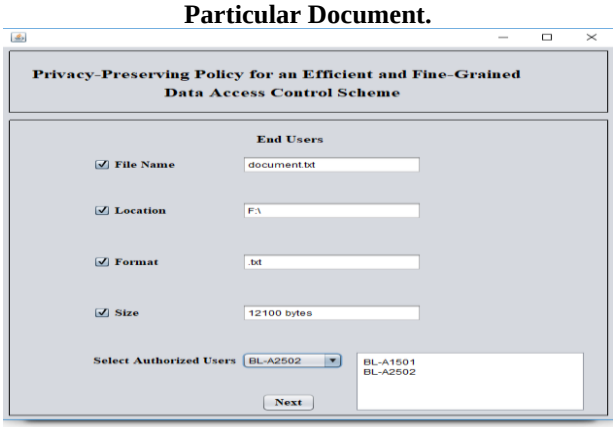

Figure X: End user page to select authorized users –
Here end user can to give authorization to the users.

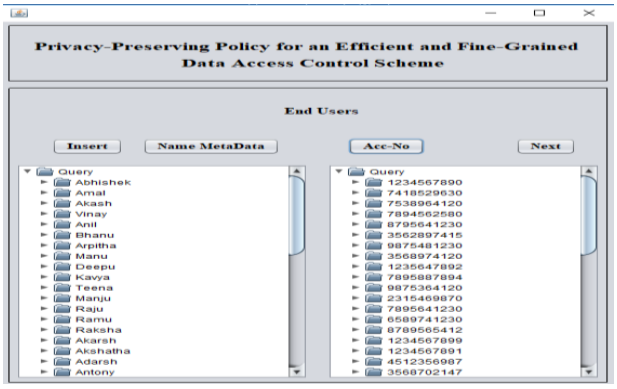

**Figure X1: End Users Page To Insert Data –
Here End Users Can Insert The Data Based On The Document Name Or The Account Number.**

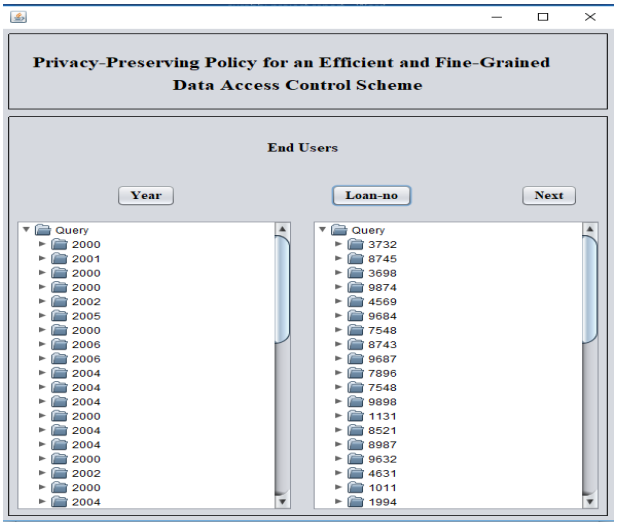

**Figure XII: End users page to insert data –
Here end users can insert the data based on the year or the loan no.**

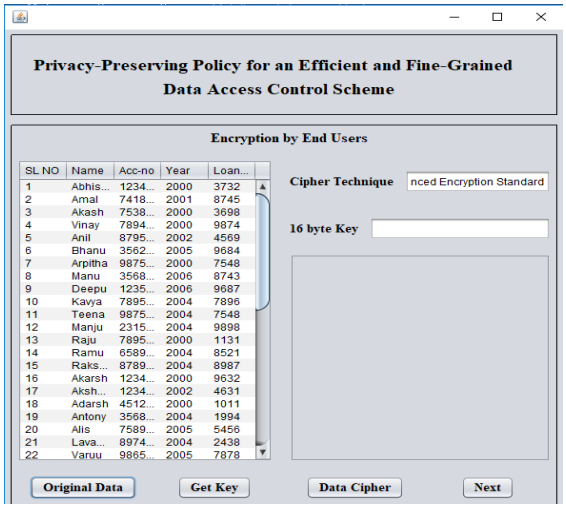

**Figure XIII: End Users Page To Encrypt Original Data –
The Data Which Are Visible To All The End Users Can Be Encrypted Here.**

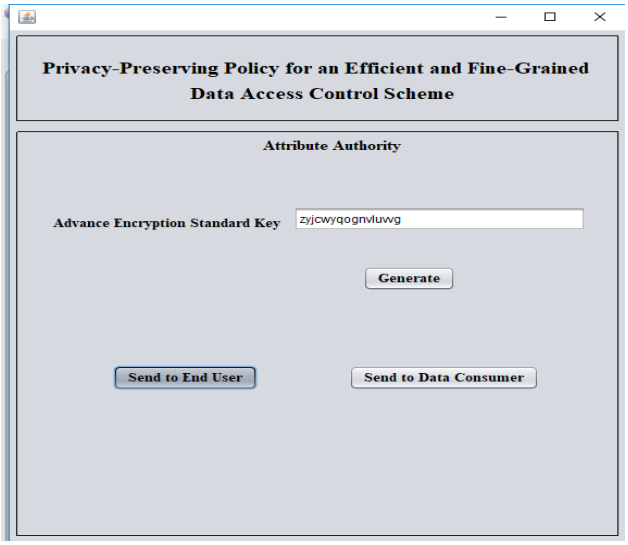

**Figure XIV: Attribute Authority
Here The Attribute Authority Can Be Generated And Sent To End User Or Data Consumer.**

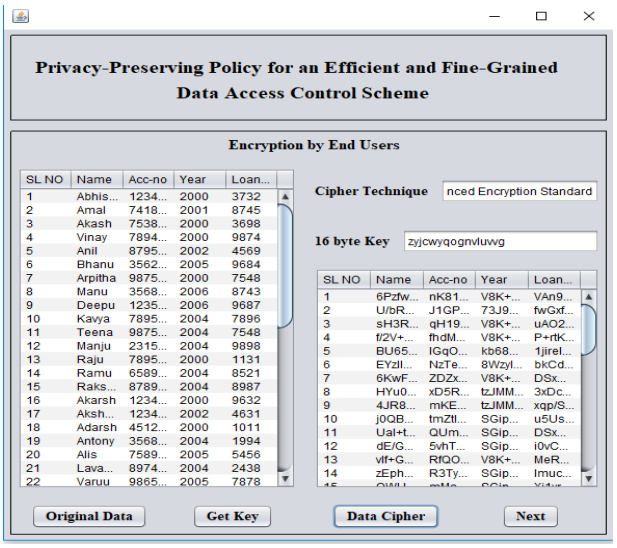

**Figure XV: Encryption by End users –
Here the encrypted data can be viewed by the end users.**

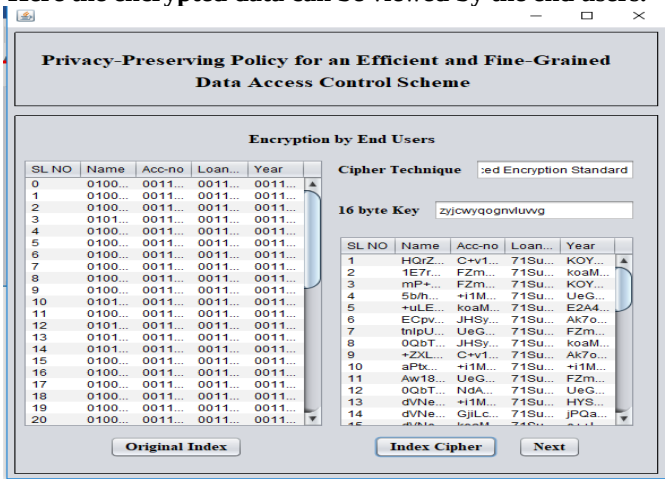

**Figure XVI: Encrypting The Index –
The Index Can Be Encrypted From The Original Index.**

Retrieval Number: J93820881019/19©BEIESP
DOI: 10.35940/ijitee.J9382.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Figure XVII: Data consumer login here by giving the credentials.

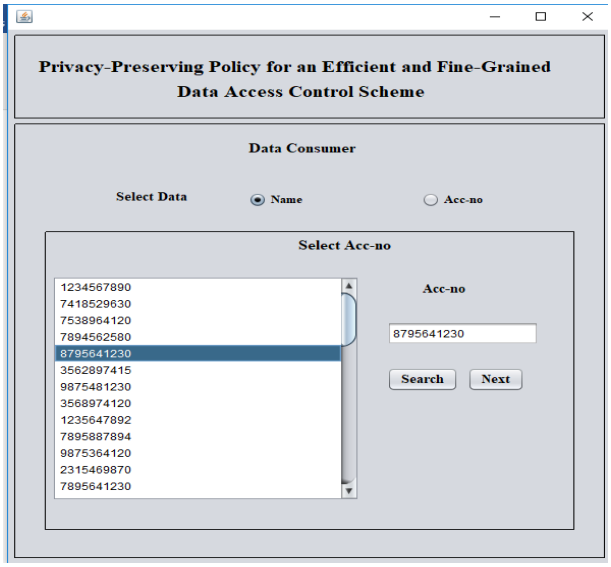

Figure XX: Data consumer page to select data and search according to it.

Figure XVIII: Data consumer validation can be done after giving credentials.

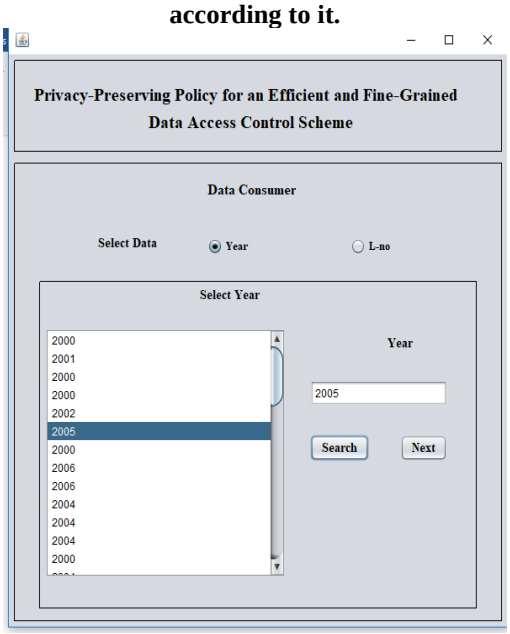

Figure XX1: Data consumer page to select data year wise and then search the data.

Figure XIX: Data consumer page to select data

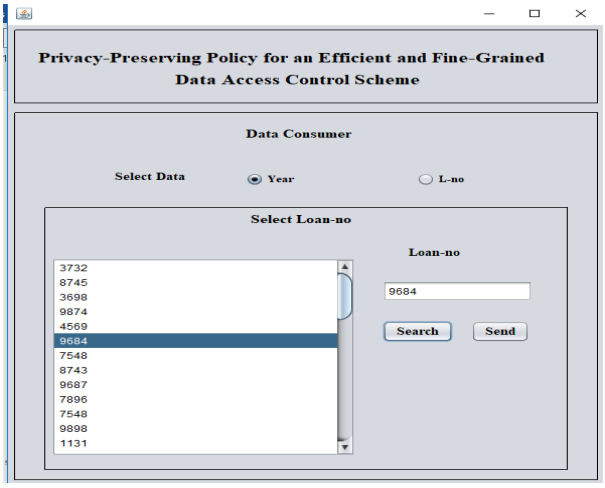

Figure XXII: Data consumer page to select data according to loan no and search.

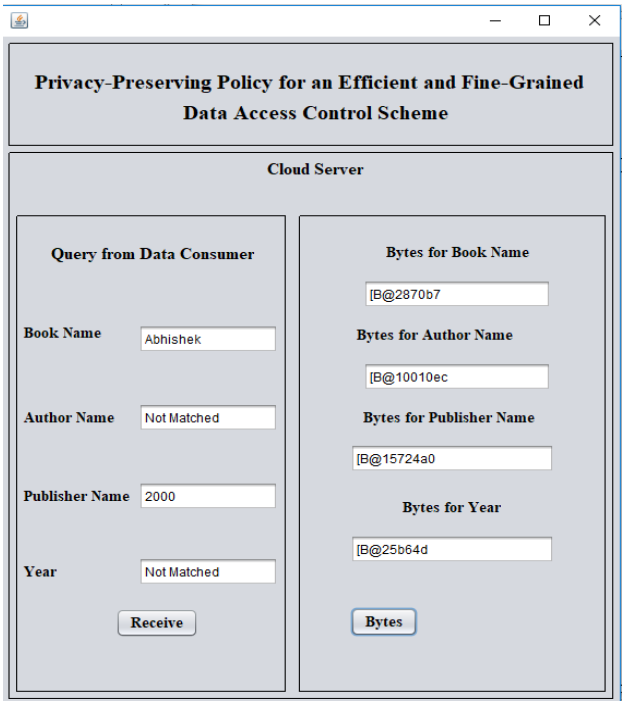

Figure XXIII: Receiving query from data consumer (not matched condition)

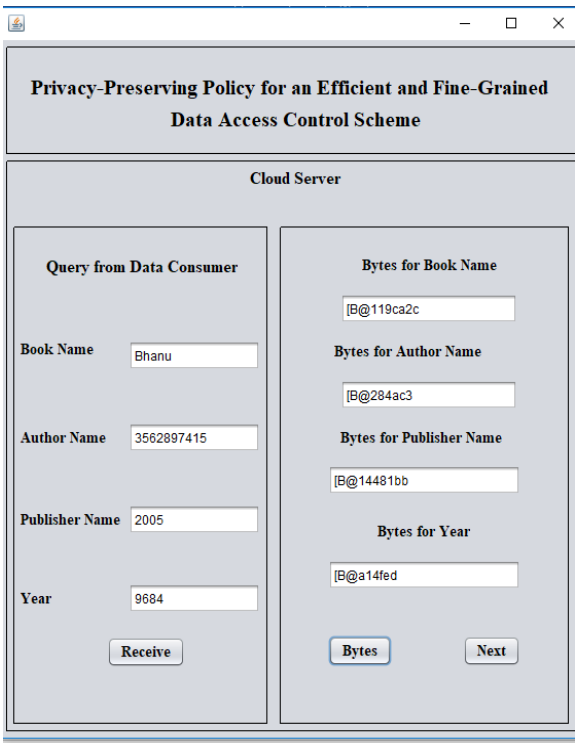

Figure XXIV: Receiving query from data consumer Receiving query from data consumer based on number of bytes of that data based on name, author, publisher and year.

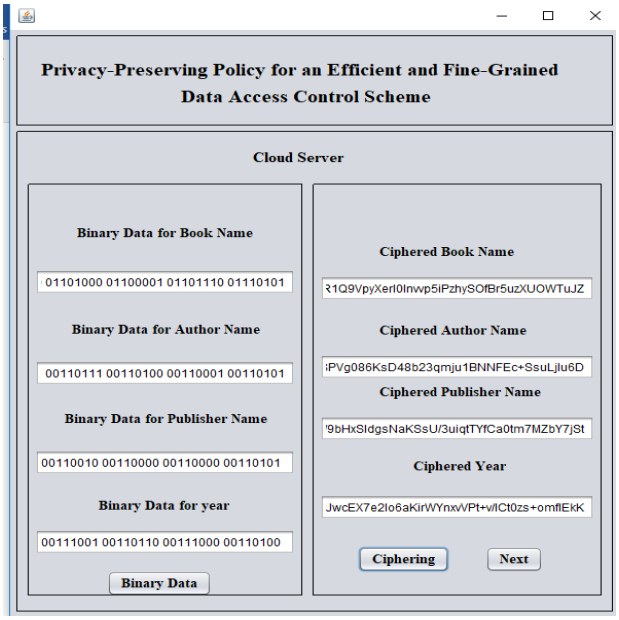

Figure XXV: Ciphering data – ciphering data consumer based on number of bytes of that data based on name, author, publisher and year.

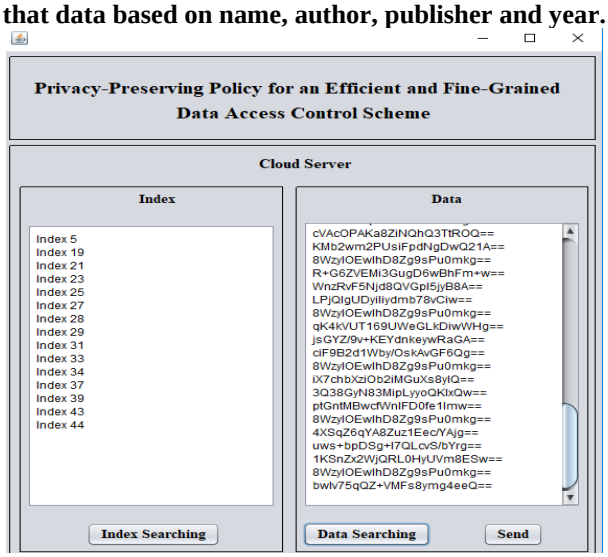

Figure XXVI: Searching Index And Data

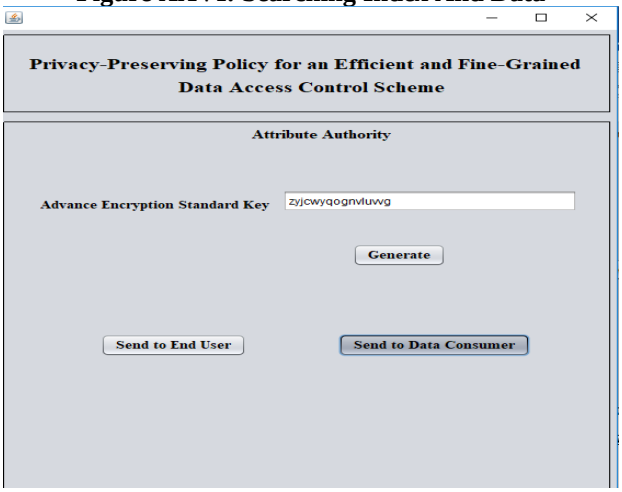

Figure XXVII: Attribute Authority – Here The Attribute Authority Can Be Generated And Sent To End User Or Data Consumer.

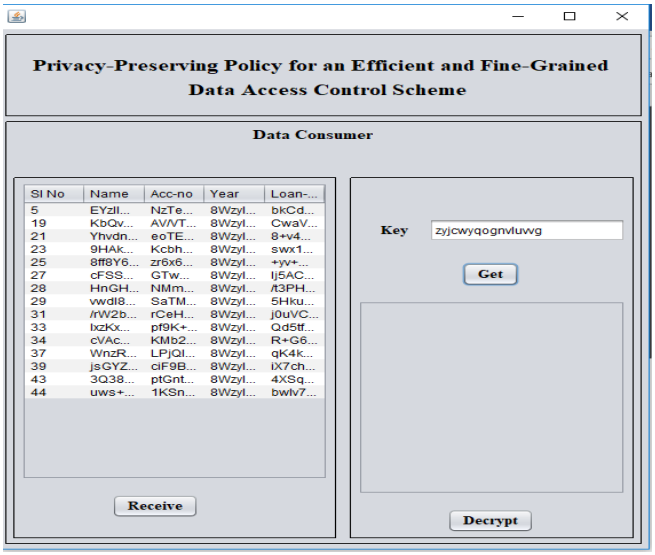

Figure XXVIII: Key to data consumer –

Here end user can select the received encrypted data and then can get the decrypted data by clicking.

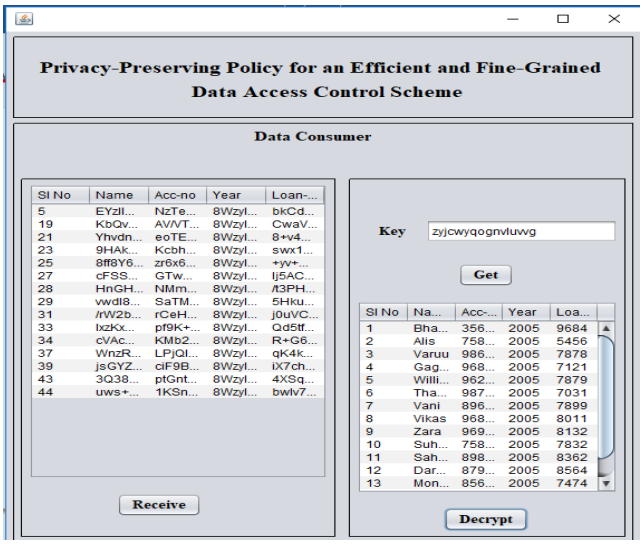

Figure XXIX: Decryption –

Here the decrypted data can be viewed by the end users.

VI. CONCLUSION

A proficient and fine-grained information access control scheme for big data is given, where the entrance strategy won't release any protection data. The framework can hide the entire characteristic (as opposed to just its qualities) in the entrance strategies. To improve the effectiveness, a novel Attribute Bloom Filter is utilized to assess whether a property is in the entrance strategy and find the precise position in the entrance arrangement in the event that it is in the entrance approach. Just the clients whose properties fulfill the entrance approach are qualified to unscramble the information. This framework performs just for the content records. In our fats paced and associated world where Big Data is top dog, it is basic to comprehend the significance of security as we process and dissect enormous measures of information.

This begins with understandings our information and related security strategies in our associations and how they should be implemented. To help information decoding, a novel Attribute Bloom Filter is utilized to assess whether a characteristic is in the entrance arrangement and find the precise position in the entrance strategy on the off chance that it is in the entrance approach. Just the clients whose characteristics fulfill the entrance arrangement are qualified to unscramble the data. This article gave a concise history of information security, concentrated on normal security concerns.

REFERENCES

1. Nishide, T., Yoneyama, K., & Ohta, K. (2008, June). Attribute-based encryption with partially hidden encryptor-specified access structures. In International conference on applied cryptography and network security (pp. 111-129). Springer, Berlin, Heidelberg.
2. Malhotra, S., Doja, M. N., Alam, B., & Alam, M. (2017, May). Bigdata analysis and comparison of bigdata analytic approches. In 2017 International Conference on Computing, Communication and Automation (ICCCA) (pp. 309-314). IEEE.
3. Yamagiwa, S., Kawahara, Y., Tabuchi, N., Watanabe, Y., & Naruo, T. (2015, October). Skill grouping method: Mining and clustering skill differences from body movement BigData. In 2015 IEEE International Conference on Big Data (Big Data)(pp. 2525-2534). IEEE.
4. Nguyen, T. L. (2018, December). A Framework for Five Big V's of Big Data and Organizational Culture in Firms. In 2018 IEEE International Conference on Big Data (Big Data) (pp. 5411-5413). IEEE.
5. Strang, K. D., & Sun, Z. (2016, December). Meta-analysis of big data security and privacy: Scholarly literature gaps. In 2016 IEEE International Conference on Big Data (Big Data)(pp. 4035-4037). IEEE.
6. Liu, H. (2019, January). Research on Feasibility Path of Technology Supervision and Technology Protection in Big Data Environment. In 2019 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)(pp. 293-296). IEEE.
7. Albalawi, U. (2018, December). Countermeasure of Statistical Inference in Database Security. In 2018 IEEE International Conference on Big Data (Big Data) (pp. 2044-2047). IEEE.
8. Li, H., Liu, D., Alharbi, K., Zhang, S., & Lin, X. (2015). Enabling Fine-grained Access Control with Efficient Attribute Revocation and Policy Updating in Smart Grid. TIIS, 9(4), 1404-1423.
9. Yang, K., & Jia, X. (2013). Expressive, efficient, and revocable data access control for multi-authority cloud storage. IEEE transactions on parallel and distributed systems, 25(7), 1735-1744.
10. Patil, H. K., & Seshadri, R. (2014, June). Big data security and privacy issues in healthcare. In 2014 IEEE international congress on big data (pp. 762-765). IEEE.
11. Yang, K., Han, Q., Li, H., Zheng, K., Su, Z., & Shen, X. (2016). An efficient and fine-grained big data access control scheme with privacy-preserving policy. IEEE Internet of Things Journal, 4(2), 563-571.
12. Lai, J., Deng, R. H., & Li, Y. (2011, May). Fully secure cipertext-policy hiding CP-ABE. In International conference on information security practice and experience (pp. 24-39). Springer, Berlin, Heidelberg.
13. Ramireddy, G. & Mounica, BSS (2018). An Efficient Bloom Filter to Evaluate the Access Policy and Locate an Attribute. International Journal & Magazine of Engineering, Technology, Management and Research, 5(2), 185-188. Retrieved from: http://www.ijmetmr.com/olfebruary2018/GujjulaRamireddy-BSSMounica-24.pdf?cv=1
14. Verma, O. P., Jain, N., & Pal, S. K. (2019). Design and analysis of an optimal ECC algorithm with effective access control mechanism for big data. Multimedia Tools and Applications, 1-27.
15. Bao, F., & Weng, J. (Eds.). (2011). Information Security Practice and Experience: 7th International Conference, ISPEC 2011, Guangzhou, China, May 30-June 1, 2011, Proceedings(Vol. 6672). Springer Science & Business Media.

16. Sreenu, G., & Durai, M. S. (2018). Big Data Analytics: An Expedition Through Rapidly Budding Data Exhaustive Era. In HCI Challenges and Privacy Preservation in Big Data Security(pp. 124-138). IGI Global.
17. Yilmaz, E., Ferhatosmanoglu, H., Ayday, E., & Aksoy, R. C. (2017). Privacy-preserving aggregate queries for optimal location selection. IEEE Transactions on Dependable and Secure Computing, 16(2), 329-343.

AUTHORS PROFILE

Dr. Niranjanamurthy M received Ph.D. Computer Science degree from JJT University, Rajasthan, INDIA in the year 2016, M.Phil-Computer Science degree from VM University, Tamil Nadu in the year 2009. MCA degree from VT University, Karnataka in the year 2007 and BCA Degree from Kuvempu University in the year 2004. He is an Assistant Professor in the department of Computer Applications, M S Ramaiah Institute of Technology, Bangalore. His areas of interests are software testing, e-commerce and m-commerce, software engineering, web technologies, Cloud Computing, Big data analytics, blockchain Technology, AI. He has been participating in National and International workshops/Conferences on different aspects related to Computer Applications. Guiding Research Scholars, Recognized Ph.D. research examiner National and International. Published many research Articles related to Computer Science.

Dr. Esha Jain has qualified UGC-NET in Management and has 12 years of work experience. She did her Graduation in Commerce, MBA (Finance & Marketing) from Kurukshetra University and PhD in Management (Finance) in 2015 from Pacific University Udaipur. A Certified Technical Analyst (in Stock Market) from Government of NCT of Delhi and Government of India, and Amazon Trained E-commerce Specialist, she has also qualified a module of Financial Markets with Distinction organized by (NSE) National Stock Exchange of India. An awardee of 'Eminent Educationist Award', 'Asia Pacific Gold Star Award', 'Young Woman Educator and Scholar Award', 'Excellence Award 2017', she was also selected for 'Rajiv Gandhi Education Excellence Award' and 'Bharat Vidya Shiromani Award'. She is the Resource Person for Various Faculty Development Programmes in the field of Academics, Research and SPSS. She is also awarded with 27 Honors and Awards, including 15 Best Research Paper Awards and a Dean Committee Choice Award in various International Conferences of repute. She has been invited by IIM Indore for review of 'Institutional Development Plans (IDPs)' under the World Bank supported Madhya Pradesh Higher Education Quality Improvement Project (MPHEQIP) to be submitted to Department of Higher Education, Government of Madhya Pradesh. More than 70 of her research papers are published in various International Journals and Conference Proceedings of repute as well as authored two (2) books, one is on 'Foreign Exchange Management' & other one is on 'Principles of Management with text and cases' under reputed Brands and also contributed chapters in another book on 'Corporate Social Responsibility'. She has also presented around 80 research papers and cases at various national and international conferences as well as has chaired various National and International Seminars and Conferences. She is also associated with 12 various International Journals as Editorial Board Member, Academic Advisor & Research Paper Reviewer, Editor-in-Chief of Asian Journal of Multidimensional Research and an External Examiner for evaluating PhD Thesis for Jain University, Bengaluru, University of Pune and University of Madras.

Dr. Bhawna Nigam received Ph.D. in Computer Engineering from Devi Ahilya University, Indore, M.P. in 2017, M.E. in Software Engineering with distinction from Institute of Engineering & Technology (IET), Devi Ahilya University in 2008 and B.E in 2003 from Institute of Engineering & Technology (IET), Devi Ahilya University, Indore. She is currently with Institute of Engineering and Technology (IET), Devi Ahilya University, Indore, India as Assistant Professor in Information Technology department. She is with Devi Ahilya University since 2007. Her area of interest is Machine Learning, Deep Learning, Data Mining, Big Data. She has published 20+ papers on these topics.

Ms. Sushmitha M. Completed Master of Computer Applications, from M S Ramaiah Institute of Technology, Bangalore Affiliated to VTU, Belgaum. Currently working at IBM Bangalore. Area of Interests are Software testing, software engineering, web technologies, Big data analytics, Fashion Design.