International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Access Control Model for Cloud Platforms Using Multi-Tier Graphical Authentication

Harvinder Singh[1], Amandeep Kaur[2]

Abstract: ***In case, somebody once see a user entering the graphical password can easily remember or guess the pattern and can take access to the device. Our major goal is to overcome this security issue and to use the password on the cloud platforms for the administrator panels for various cloud applications. Using this password scheme, the touch screen friendly secure administration interfaces can be developed to give the administrators an easy access to the administration panel. In this research, a multi-level password authentication scheme has been proposed for the administrator panels, where the administrators would be prompted to enter the first-level password at first and second-level password can be used to access more critical administration areas in order to protect the power user accounts from hacking attempts. A user when signup creates and stores a pattern by joining the number points or by selecting the images to create a password, the password is converted into a hash which is further sent to the server for the authentication purposes. The server returns the decision logic which is responsible to accept or deny the login request. To gain the access to the device, the user has to remember the graphical passwords and need to enter the same sequence every time drawing a pattern. The proposed scheme has been evaluated as effective, robust, ease of access and wide adaptability of the scheme for the various smart phone platforms. The proposed scheme has been evaluated under various situations. Both of the graphical password schemes have been evaluated individually with various password combinations. The new multi-level graphical password scheme can be considered as a secure scheme for cloud platforms.***

Keywords: Cloud Storage, Access Control Model, Attribute based signatures, Multi-tier authentication, Graphical authentication

1. Introduction

Computing as we all know it speaks the truth to change: all applications and archives are going to move from the desktop into the cloud. Cloud computing, where applications and records are facilitated on a "cloud" comprising of a huge number of PCs and servers, all connected together and open through the Internet. With cloud computing, all that we do is presently online or web based as opposed to being desktop based. Cloud computing forecasts a major change by the way we store data and run applications. Rather than running projects and information on an individual desktop PC, everything is facilitated in the "cloud"— an amorphous gathering of PCs and servers got to by means of the Internet. Cloud computing gives you a chance to get to every one of your applications and reports from anyplace on the planet, liberating you from the bounds the desktop and making it less demanding for gathering individuals in different areas to work together. There are 3 essential sorts of Cloud Service Models, which are **Infrastructure as a service, Platform as a Service and Software as a Service.**

Cloud Deployment Models

A Cloud Deployment model represents a specific type of cloud environment, primarily distinguished by ownership, size and access. There are four common cloud deployment models:

- **Private Cloud (**worked exclusively for a single association**)**
- **Public Cloud (**services and infrastructures are given to different customers**)**
- **Hybrid Cloud (**creation of two or more models**)**
- **Community Cloud (**shared by a few associations**)**

Access Control Models

Access control is a fundamental aspect of information security that is directly tied to the primary characteristics such as confidentiality, integrity and availability. Cloud computing service providers should provide the following basic functionalities from the perspective of access control:

1) Control access to the service features of the cloud based on the specified policies and the level of service purchased by the customer.
2) Control access to a consumer's data from other consumers in multi-tenant environments.
3) Control access to both regular user functions and privileged administrative functions.
4) Maintain accurate access control policy and up to date user profile information.

Access control models can be traditionally categorized into three types:

- **Discretionary Access Control -** In the discretionary access control (DAC) model, the owner of the object decides its access permissions for other users and sets them accordingly.
- **Mandatory Access Control -** The Mandatory access control (MAC) the access permissions are decided by the administrator of the system, and not by the subject.
- **Role-based Access Control -** In a Role-based access control model (RBAC), a user has access to an object based on his/her assigned role in the system. Roles are defined based on job functions.

2. Literature Survey

- ***[2014] Bharathy, S. Divya*** has developed securing data stored in clouds using privacy preserving authenticated access control. Authors proposed a privacy preserving

access control scheme for data storage, which supports anonymous authentication and performs decentralized key management. In the proposed scheme, the cloud adopts an access control policy and attributes hiding strategy to enhance security.

- ***[2014] Nguyen, Dang et. al.*** has worked on adopting provenance-based access control in open stack cloud IaaS. Authors presented a cloud service architecture that provides PBAC authorization service and management. Authors discuss in depth the variations of PBAC authorization deployment architecture within the Open Stack platform and implement a proof-of-concept prototype. They analyze the initial experimental results and discuss approaches for potential improvements.

- ***[2014] Malik, Jyoti and Dhiraj Girdhar*** have developed a multifactor authentication using a QR code and a one-time password. The purpose of this paper is to introduce the idea of a one-time password (OTP), which makes unauthorized access difficult for unauthorized users. A OTP can be implemented using smart cards, time-based tokens, and short message service, but hardware based methodologies require maintenance costs and can be misplaced Therefore, the quick response code technique and personal assurance message has been added along with the OTP authentication.

- ***[2014] Abhijit Kumar and Dipankar Dasgupta*** have worked on adaptive approach for active multi-factor authentication. This paper focuses on describing a framework for continuous authentication where authentication modalities are selected adaptively by sensing the users' operating environment (the device and communication media, and historical data). Empirical studies are conducted with varying environmental parameters and the performance of the adaptive MFA is compared with other selection strategies.

3. Problem Formulation –

The cloud applications now-a-days are being developed with mobile apps also. The mobile apps are providing the easy and anywhere access to the cloud users. Cloud users can manage (create, write, edit, etc) their data on various cloud platforms like banking apps, Office 360, Sky Drive, Dropbox etc. These applications use very large amounts of data, which is saved with the complex storage architecture. Various users access different patterns of information on these cloud platforms. The access control authentication can be used to divide the user data access control up to various stages on the bases of multi-level authentication schemes. This will ensure the security of the data storage on the cloud platforms. In order to access these cloud platforms from the touch-based devices, the users face difficultly in providing the different level of text based passwords. We are trying to improve the user-experience on the touch-based devices using a multi-tier access control authentication using the graphical techniques of different types.

4. Research Methodology

The research methodology mainly focuses on access control models. To deal with the problem of usage of large amount of data by the applications and accessing of different patterns of information's on cloud platforms, we are proposing a model with multi-level authentication which would be implemented by using security questions and image based for the login protection and at last level UIN would be used to access the data from the cloud platforms.

- The first- level authentication pattern consists of 4 random words. These 4 words come out of 8 registered words. Each and every time of registration all 8 words will be positioned randomly. The user will have to correctly match the words and their codes for a particular word.
- The second- level authentication pattern consists of various small images of different objects and colors in 3x3 grid formation. The grid points will be used in the random positioning based grid formation to add more security to the first level of authentication. To implement the higher security to reduce the chance of breaking into, some of the fake images as well as the fake secure images can also be shown to the user, the user will need to recognize the correct objects selected during signup and then provide their secure codes correctly in order to gain the access to the sensitive data on the cloud application.
- After second level of authentication user will be able to log in the cloud, but at last step user has to provide the correct UIN (Unique Identification Number) to access the private data and more sensitive operation according to access control model.

First step towards the research is the literature study of the existing algorithms for graphical passwords, especially password patterns. Literature study will lead towards the development of the algorithm for the touch screen devices. This is also very important to get the architecture of the existing graphical authentication techniques. This project would be implemented in the **MATLAB** Simulator. A thorough performance and feature testing model would be formed and utilized to analyze the performance of the security model, to detect the flaws and to recover them.

5. Implementation

We have implemented the new shuffling points based pattern password scheme, which is designed to prevent the security risks of the currently popular pass-go pattern scheme. In this research work, we have used MATLAB for the purpose of implementation of the proposed pattern password scheme. This scheme has been designed using the GUIDE (Graphical User Interface Development Environment) tool of MATLAB, because they are simple and used to create attractive & flexible designs. Also this pattern scheme is developed in the way for dual purpose, because these are widely used for the mobile application development and desktop software purposes.

For the backend programming, i.e. the result retrieval, MATLAB is used. MATLAB is used to create the number sequence, which acts as a numerical representation of the

front-end pattern password and saved in the MATLAB arrays. The users are provided with two types of password authentication schemes and unique id. The first scheme is used to authenticate the user for the first level, where the user will get the privileges to access the data stored on cloud server, which may be used to run some specific small-sized or semi mid-sized applications on the cloud platforms. The second scheme is used to authentication the users for the more privileged interface, where the user can access all the data stored on cloud server. The second level password is based on a 3x3 graphical password grid and irrespective of any pattern. The second password scheme is repeatable and overlapping password pattern scheme. The user will be capable of drawing an overlapping pattern, which is always difficult for the hacking trying to crack the passwords using shoulder surfing attacks. When a user enters the pattern passwords, a numerical code for the pattern password is generated on the basis of the grid point indexing numbers. MATLAB code is divided into the various functions to perform the various types of functions.

Algorithm for Level 1 Registration –

1) User runs the Simulation.
2) A set of 8 words would be displayed on screen.
3) User enters a password or security answer against each word.
4) User enters the UIN (Unique Identification Number).
5) Password array is stored.
6) If all fields are filled then Registration is Successful else, Registration is failed and returns to step 2.

Algorithm for Level 1 Login –

1) User runs the Simulation.
2) Randomly 4 words would be displayed on screen.
3) User enters the password in sequence for each word.
4) User enters the UIN (Unique Identification Number).
5) If all 4 passwords & UIN match with stored array then data will be displayed and user can access the data.
6) Else data will not be displayed and simulation returns to step 2.

Algorithm for Level 2 Registration –

1) User runs the Simulation.
2) Display 3x3 grid of graphical pattern.
3) User selects the pattern of 4 graphical images.
4) User enters the UIN (Unique Identification Number).
5) Password array is stored.
6) If all fields are filled then Registration is Successful else, Registration is failed and returns to step 2.

Algorithm for Level 2 Login –

1) User runs the Simulation.
2) Display 3x3 grid of graphical pattern.
3) User inputs the images in sequence as stored in the array.
4) User enters the UIN (Unique Identification Number).
5) If sequence of images & UIN matches with stored then data will be displayed and user can access the data.
6) Else data will not be displayed and simulation returns to step 2.

6. Results

The implemented work includes the new multi-level password scheme which is designed to prevent the security risks of the currently popular graphical password schemes. The new scheme has been proposed for its use in the power user portal for data access on cloud server. In this research work, MATLAB has been used for the purpose of implementation of the proposed pattern password scheme. This scheme is designed using the GUIDE (Graphical User Interface Development environment) tool of MATLAB, because they are simple and used to create attractive & flexible designs. Also this pattern scheme is developed in the duo, because these two are widely used for the mobile application development and computer software purposes. For the backend programming, i.e. the result retrieval, MATLAB is used. MATLAB is used to create the number sequence, which acts as a numerical representation of the front-end pattern password and saved in the database. When a user enters the pattern passwords, a numerical code for the pattern password is generated on the basis of the grid point indexing numbers.

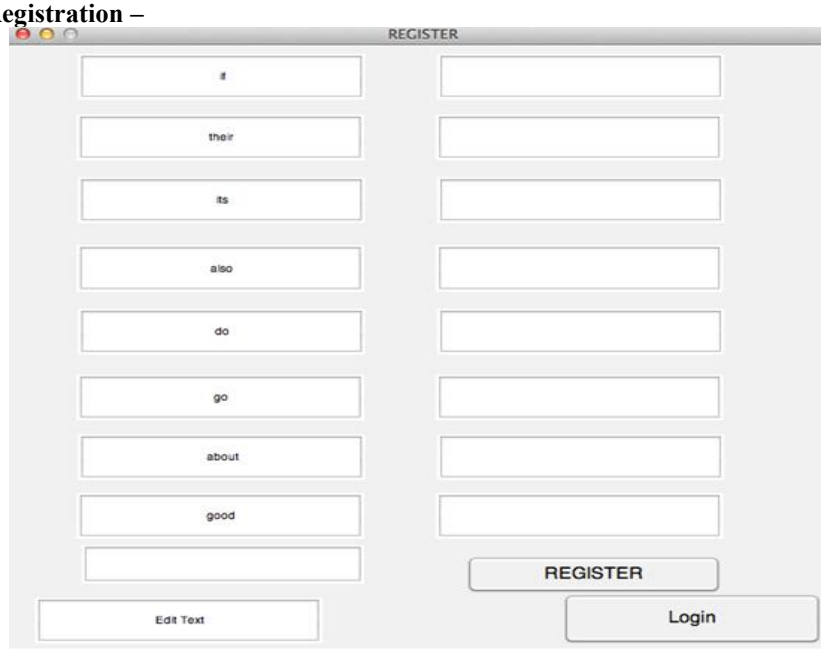

Figure 1: The word based password pattern for 1st level registration

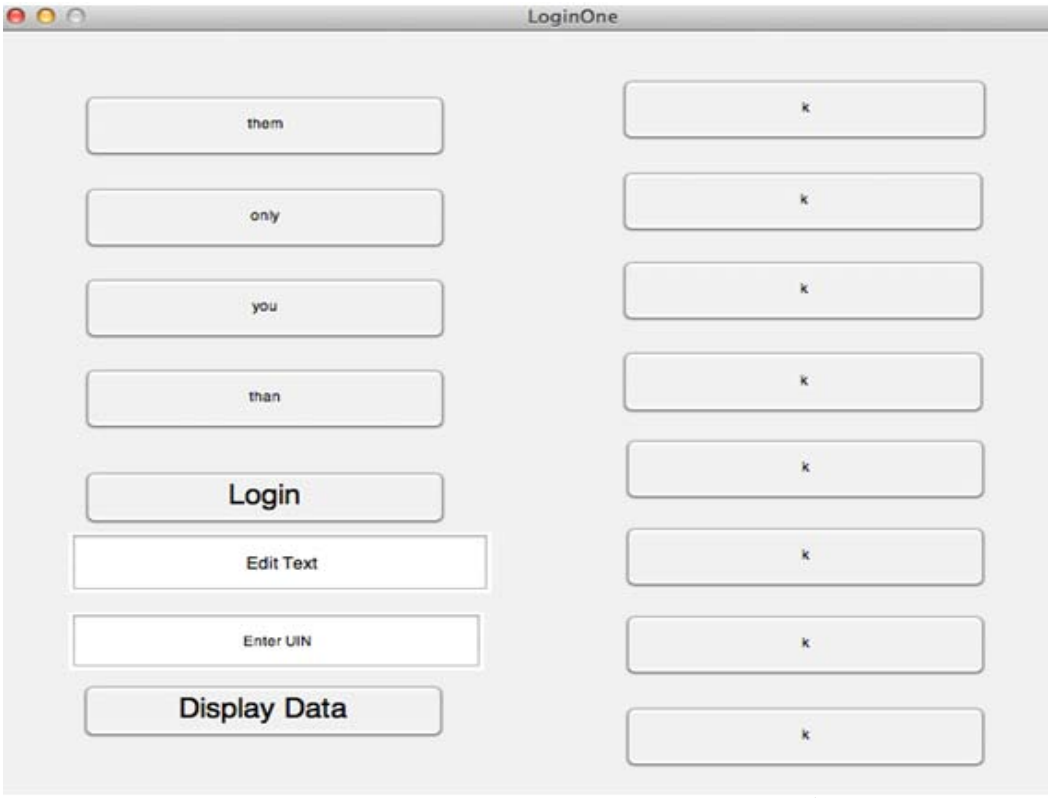

Figure 2: The password input with 4 registered words for 1st level

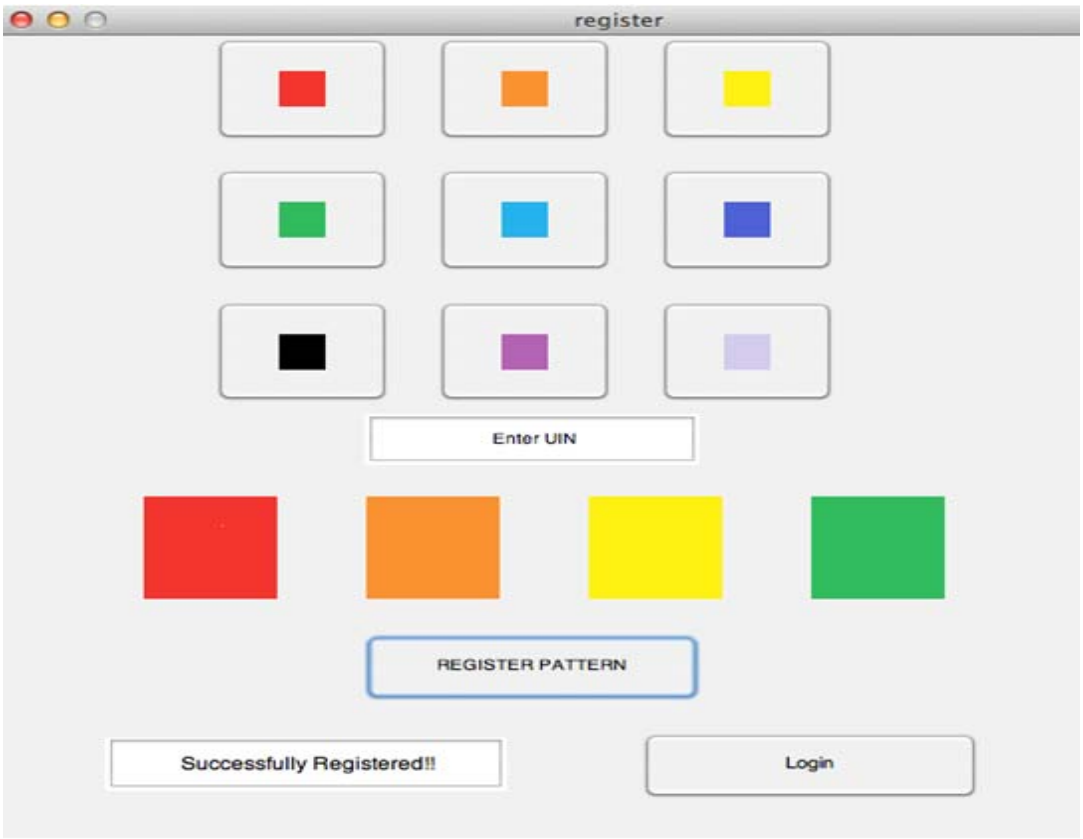

Figure 3: The 3X3 graphical grid registration for 2nd level

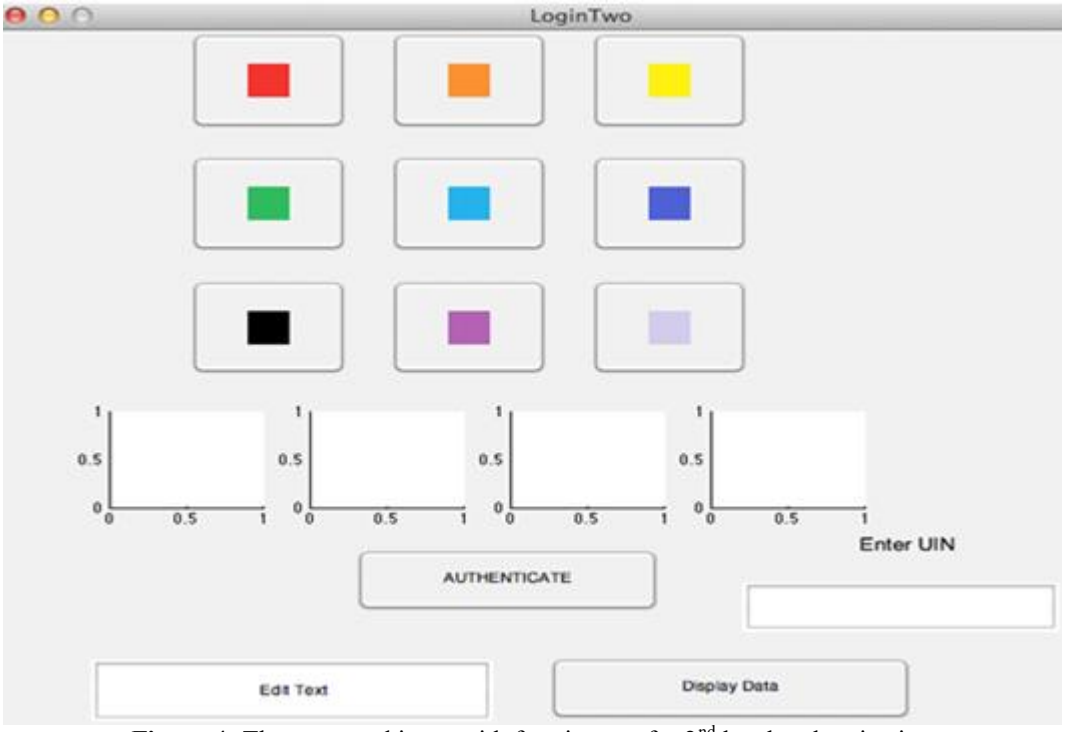

Figure 4: The password input with four images for 2nd level authentication

7. Comparison with Other Methods

The proposed scheme has been evaluated for various applications under various situations. The comparison of the proposed techniques has been made with the previous techniques in order to understand the functional or security differences between the proposed model and the existing models. The proposed model has been evaluated for its method of working, ease of use, merits and demerits. The merits and demerits of the proposed model have been evaluated as the best model among the others.

Table 1: Comparison with other Methods

Schemes	*Method*	*Ease of use*	*Advantages*	*Disadvantages*
Image- based scheme	Single or multiple images are used	Selection of images	Easily remember the password	Very long process selection of number images.
Grid- based scheme	Grid platform is used to accommodate pixels	Simple take and draw scheme	No extra displays are needed grid is Sufficient.	Sequence can be changed or grids may be different
Triangle scheme	Set of images on convex surface	Complex as convex triangle	Crowded Display	Convex surface assigning process takes longer time
Hybrid textual authentication	Words with sequence number is combination	Complex as confusion with colors	Given user only have to remember the rating.	Difficult to remember colors with sequence.
Signature based scheme	User signature on grid platform	Own signature	Denied the access for mistake	Remembering the grid if not simple
Username and image password scheme	Username with selection of images as password	Username password remembrances	More strong authentication process	Access can be given if anyone knows sequence with username
Proposed scheme [Partial]	Color-Grid based graphical scheme	Easy to remember color pattern.	Easy to remember and Flexible. Can be made shoulder surfing proof by adding shuffling patterns.	Not known

Table 2: (Existing Vs Proposed Comparison) on the Basis Of Base Paper

Schemes	**Fine-grained access control**	**Centralized/ Decentralized**	**Write/read access**	**Type of access control**	**Privacy preserving authentication**	**User revocation?**
Existing Scheme	Yes	Decentralized	M-W-M-R	ABE	Authentication	Yes [Only on the basis of number of failed login attempts]
Proposed Scheme	Yes/Flexible Fine Grained	Decentralized	M-W-M-R	Attributed Based Encryption would be used	Complete Authentication, Authorization and Accounting Model	Yes [On the basis of failed login attempts to time comparison]

In this way, more secure passwords can be generated, and also it may help one to generate a more visually complex patter password, which will be definitely difficult to guess and will be less or not prone to the access the data from server.

8. Conclusion

The proposed access control models for the cloud data has been implemented using the MATLAB simulator. The implementation of the MATLAB simulator will begin with the implementation of the DA-RBAC-2 (dual adaptive role based access control) simulation cloud data storage. The cloud data storage simulation must be capable of releasing the data in the index formation. The adaptive access control model will be based upon the Dual Adaptive Role based access control model (DA-RBAC). The Dual Adaptive role based access model enables the user to access the files in its scope according to the role assigned to it. For example, a database administrator can access the data stored in the databases, whereas a security administrator will be having the access to the firewalls and other security management modules. The cloud access model learns the rules after the evaluation of the needs of the users in order to classify and index the data available under the access and privacy protection rules. The self-learning based rule based access control model (DA-RBAC). The infusion of both of the access control models i.e. DA-RBAC will lead us towards the finalization of the realization of the access model simulation for the cloud platforms.

9. Future Scope

In the future the proposed model will be enhanced with more functionality and higher level of authentication security; it would be implemented by using security questions, image based security for the login protection and at the last level User Identification Number (UIN) would be used to access or view the data in cloud platforms on mobile devices and software systems for computers. It can also use biometric devices to input the password. Also, the proposed model will be enhanced for the higher level of security and data privacy using different type of input passwords and authentication.

References

[1] Bharathy, S. Divya, and T. Ramesh. "Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control." (2014).
[2] Nguyen, Dang, Jaehong Park, and Ravi Sandhu. "Adopting provenance-based access control in Open Stack cloud IaaS." In Network and System Security, pp. 15-27. Springer International Publishing, (2014).
[3] Malik, Jyoti, Dhiraj Girdhar, Ratna Dahiya, and G. Sainarayanan. "Multifactor Authentication Using a QR Code and a One-Time Password." Journal of Information Processing Systems 10, no. 3 (2014).
[4] Nag, Abhijit Kumar, Dipankar Dasgupta, and Kalyanmoy Deb. "An Adaptive Approach for Active Multi-Factor Authentication." In 9th Annual Symposium on Information Assurance (ASIA'14), p. 39. 2014.
[5] Lee, Keunwang, and Haeseok Oh. "Research on access control method by user authority using two-factor authentication." In Proceedings of the 1st International Conference on Convergence and Its Application (ICCA'013), vol. 24, pp. 172-175. 2013.
[6] Nguyen, Dang, Jaehong Park, and Ravi Sandhu. "A provenance-based access control model for dynamic separation of duties." In Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on, pp. 247-256. IEEE, 2013.
[7] Wazan, Ahmad Samer, Gregory Blanc, Hervé Debar, and Joaquin Garcia-Alfaro. "Attribute-based Mining Process for the Organization-Based Access Control Model." In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 421-430. IEEE, 2013.
[8] Ruj, S., Stojmenovic, M., & Nayak, A. (2012, May). "Privacy preserving access control with authentication for securing data in clouds". In *Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on* (pp. 556-563). IEEE.
[9] Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). "Toward secure and dependable storage services in cloud computing". *Services Computing, IEEE Transactions on*, *5*(2), 220-232.
[10] Punithasurya, K., and S. Jeba Priya. "Analysis of Different Access Control Mechanism in Cloud." *International Journal of Applied Information Systems (IJAIS), Foundation of Computer Science FCS* 4.2 (2012).
[11] Ruj, Sushmita, Amiya Nayak, and Ivan Stojmenovic. "Dacc: Distributed access control in clouds." *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*. IEEE, 2011.
[12] Sirisha, Avvari, and G. Geetha Kumari. "API access control in cloud using the Role Based Access Control Model." *Trendz in Information Sciences & Computing (TISC), 2010*. IEEE, 2010.