

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

Harvinder Singh¹, Er. Amandeep Kaur²

^{1,2}Desh Bhagat University, Mandi Gobindgarh

Abstract: *Cloud computing is an emerging, on-demand and internet-based technology. It provides variety of services over internet such as, software, hardware, data storage and infrastructure. The cloud platforms are consisted of a larger number of servers along with networking and security appliances connected together. The heavier amounts of data are stored on these cloud platforms. The data accessibility becomes the major issue in the cloud platforms. The existing access control models are based on the Mandatory access control (MAC), Role based access control (RBAC), Rule based access control (RB-RBAC) and Provenance based access control (PBAC), etc. or offered in the various combinations for the effective data access handling on the cloud platforms. We propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication and performs decentralized key management. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification and reading data stored in the cloud. We also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against replay attacks. The communication, computation and storage overheads are comparable to centralized approaches. The proposed model will ensure the security, data privacy and rich-user experience by the proposed access model.*

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

1. Introduction

Cloud Computing is where applications and files are hosted on “cloud” consisting of thousands of computers and servers, linked together and can be accessed by using Internet. Research in cloud computing is receiving a lot of attention from both academic and industrial worlds. In cloud computing, users can outsource their computation and storage to servers (also called clouds) using Internet. This frees users from the hassles of maintaining resources on-site. Clouds can provide several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure).

Cloud Computing is the emerging technology where we can get platform as a service, software as a service and infrastructure as a service. When it comes to storage as a service, data privacy and data utilization are the primary issues to be dealt with. To handle the transaction of files to and from the cloud server, the files are encrypted before being outsourced to the commercial public cloud. Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Organizations often use these IT systems to store and process vast quantities of sensitive data, which, if disclosed, could be potentially damaging to an organization. At best, an organization may be embarrassed by an unauthorized disclosure; at worst, it may lose its competitive stance in the market if the information were a proprietary trade secret, or may be sued if the information were confidential customer information. Some companies have gone out of business when the damage from an unauthorized access proved too great for them to weather.

Security and privacy are thus very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user. Cloud Computing Technologies are grouped into 4 sections - they are, SaaS, PaaS, IaaS and DSaaS.

- **SaaS (Software as a Service)** is an on-demand application service. It delivers software as a service over the Internet. It eliminates the need of installing and running the application on the customer's own computers.
- **PaaS (Platform as a Service)** is an on-demand platform service to host customer application. PaaS is delivery of computing platforms and/or solution stack as a service, often consuming cloud infrastructure and sustaining cloud applications. It provides deployment of applications without any cost and complexity of buying and managing the underlying hardware and software layers.
- **IaaS (Infrastructure as a Service)** is an on-demand infrastructure service. It delivers the computer infrastructure – typically a platform virtualization environment – as a service, along with raw (block) storage and networking. Rather than purchasing servers, software, data-center space or network equipment, clients can buy those resources as a fully outsourced service.
- **DSaaS (Data Storage as Services)** is an on-demand storage service. Cloud computing provides internet-based on demand back up storage services to a customer. In this service, customers can keep their data backup remotely over internet servers.

These backup data maintenance is taken care by DSaaS service Provider. Cloud DSaaS service providers are responsible for keeping the customer data confidential. Here

customers need not worry on setting up the large discs array to keep their huge amount of data.

To access these cloud services securely, cloud authentication systems are using different methods like: i) Simple text password ii) Third party authentication iii) Biometric and iv) 3D password object. i) The weakness of textual password authentication system is that it is easy to break and vulnerable to dictionary or brute force attacks. ii) Third party authentication is not preferred for smaller cloud deployment. iii) Bio-metric authentications such as, fingerprints, palm prints, hand geometry, face recognition, voice recognition, iris recognition, and retina recognition, have been proposed in literature. Each bio-metric recognition scheme has its own advantages and disadvantages based on many factors such as consistency, uniqueness, and acceptability. iv) 3D- password does not support the multiple levels of authentication. Another simple approach is to use one/combination of the above techniques in multi-level authentication, so that, probability of breaking such a password is reduced to a large extent. Hence it has motivated us to introduce a multi-level authentication technique in secure cloud transmission for ensuring the strict authentication.

2. Literature Review

A literature review goes beyond the search for information and includes the identification and articulation of relationships between the literature and our field of research. While the form of the literature review may vary with different types of studies, the basic purposes remain constant:

[2014] **Ruj, Sushmita et. al.** have proposed a decentralized access control with anonymous authentication of data stored in clouds. Authors proposed a new decentralized access control scheme for secure data storage in cloud, that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing data.

[2014] **Bharathy, S. Divya** have 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** have 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. We discuss in depth the variations of PBAC authorization deployment architecture within the OpenStack platform and implement a proof-of-concept prototype. The authors have analyzed 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 user's 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. The empirical results appear promising, which reflects that such a multifactor decision support technique can be applied to real world identity management and authentication systems.

[2013] **Krikelas, Ilias and Ioannis Xydias** have developed graphical user authentication in mobile device using the web RGB color palette. This paper describes a prototype system providing graphical authentication of mobile devices over the Internet, covering both usability and security aspects. Color images are assigned to the mobile users and authentication is achieved by modifying the Red-Green-Blue (RGB) color intensity values of the assigned image.

[2013] **Wazan, Ahmad Samer and Gregory Blanc** have worked on attribute-based mining process for the organization-based access control model. Authors have propose to bridge the gap between the theory of access control models and the reality of organizations by defining an attribute-based mining process.

3. Research Gaps

- 1) In the existing technique, there was no multi-tier authentication security, all the existing systems was mostly based on one or two level security which includes simple text based Id Passwords, Biometric authentication, 3D object passwords, Graphical authentication etc. as a security input.
- 2) Various Cloud platform 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.
- 3) In the existing technique, to access the data from cloud platforms from the touch-based devices, the users face difficulty in providing the different level of text based passwords.
- 4) In this proposed technique, self can improve the user-experience on the touch-based devices using a multi-tier access control authentication using the graphical techniques of different types.

4. 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 difficulty 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.

5. Proposed Model

As the trend of mobile devices is on the rise, every kind of Internet application is being easily accessible locally using mobile apps. In the proposed model multi-level authentication would be implemented by using security questions and image based for the login protection in cloud platforms on mobile devices and software systems for computers. 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. By using first level, will be mitigating the autobot/botnet/spam threats by differentiating between the user and the bots using its unique word matching password pattern. After second level of authentication user can access more private data and sensitive operation according to access control model. 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. Then, the last step consists the Unique Identification Number (UIN) as a registration ID Number which can be provided to the user at the time of Sign-Up, which can be used by the user for viewing or downloading the data after logging in the ID, without providing the correct UIN user cannot view or download the file. The proposed technique will improve the efficiency of data access control models on the cloud platforms by removing the hindrance of the repeated password inputs. It will lead to renovate the deftness of data access control models on the cloud platforms. First step towards the research is the literature study of the existing algorithms for word matching and graphical passwords, especially password patterns. Literature study will lead towards the development of the algorithm for the touch screen and computer systems. This 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 failings and to improve them.

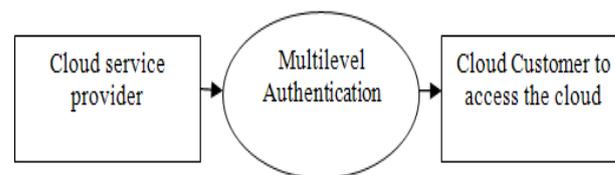


Figure: Data Flow Diagram to show the overview of Multi-Level Authentication

6. Conclusion and Future Work

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. In the future the proposed model will be enhanced with more functionality and higher level of authentication security; 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] Ruj, Sushmita, Milos Stojmenovic, and Amiya Nayak. "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" *Parallel and Distributed Systems*, IEEE Transactions on 25, no. 2 (2014): 384-394.
- [2] Bharathy, S. Divya, and T. Ramesh. "Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control" (2014).
- [3] Nguyen, Dang, Jaehong Park, and Ravi Sandhu. "Adopting provenance-based access control in OpenStack cloud IaaS" In *Network and System Security*, pp. 15-27. Springer International Publishing, 2014.
- [4] 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 It's Application (ICCA'013)*, vol. 24, pp. 172-175. 2013.

- [5] Kabir, M.E., Wang, H., and Bertino, E. (2012), “**A Role-involved Purpose-based Access Control Model**”, Information Systems Frontiers, 14(3), 809-822
- [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] 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).
- [9] Krikelas, Ilias, Ioannis Xydas, and Pierre-François Bonnefoi. “**Graphical User Authentication in Mobile Device using the web RGB color palette**” In BCI (Local), p. 65. 2013.
- [10] 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.
- [11] A B Lewko and B Waters, “**Decentralizing attribute based encryption**”, springer 2011.