ISSN:0975-9646

Access Control Model with Multi-Tier Authentication for Mobile Platforms – A Review

Yashika Sharma
PURCITM , Mohali

Rekha Bhatia
PURCITM , Mohali

Abstract--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. To solve the problem of the data access, the automatic data access control models are designed to restrict the user access to the unauthorized cloud resources and data sources. The literature is available on many access control models for 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), Provenance based access control (PBAC), etc. or offered in the various combinations for the effective data access handling on the cloud platforms. In this papera model has been proposed for combination of the Role based and Self Learning Rule based access control. The self learning will be based upon the rule formation for the individual users, user groups, etc. The proposed model will ensure the security, data privacy and rich-user experience by the proposed access model.

Keywords: Access Model, Role Based access model, rule based access model, authentication, graphical authentication.

INTRODUCTION

Computer systems and the information that they create, process, transfer, and store have become indispensable to the modern enterprise. In today's on-demand, always connected, data-driven world—and especially in light of the transformation of entire national economies from manufacturing-based paradigms to knowledge-based ones—many organizations rightly count their information systems among their most important assets. 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.

Organizations use access control mechanisms to mitigate the risks of unauthorized access to their data, resources, and systems. Several access control models exist. Their corresponding access control mechanisms—the concrete implementations of those access control models—can take several forms, make use of different technologies and underlying infrastructure components, and involve varying degrees of complexity. In some cases, the more complicated models expand upon and enhance earlier models, while in other cases they represent a rethinking of the fundamental manner in which access control should be done. In many cases, the newer, more complicated models arose not from deficiencies in the security that earlier models provide, but from the need for new models to address changes in organizational structures, technologies, organizational needs, technical capabilities, and/or organizational relationships.

Attribute Based Access Control (ABAC) is an access control model wherein the access control decisions are made based on a set of characteristics, or attributes, associated with the requester, the environment, and/or the resource itself. Each attribute is a discrete, distinct field that a policy decision point can compare against a set of values to determine whether or not to allow or deny access. The attributes do not necessarily need to be related to each other, and in fact, the attributes that go into making a decision can come from disparate, unrelated sources. The recent rise in the availability of cloud services makes them attractive and economically sensible for clients with limited computing or storage resources who are unwilling or unable to procure and maintain their own computing infrastructure. The ever increasing need for computing power and storage accounts for the steady growth in popularity of companies offering cloud services. Clients can easily outsource large amounts of data and computation to remote locations, as well as run applications directly from the cloud.

LITERATURE REVIEW

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 clouds, that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the ser without knowing the user's identity before storing data. 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. This new scheme supports secure and efficient dynamic operation on data blocks, includ-ing: data update, creation, modification and reading data stored in the cloud. Nguyen, Dang et. al have worked on adopting provenance-based access control in openstack 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. Lee, Keunwang, and Haeseok Oh. have conducted a research on access control method by user authority using two-factor authentication. The important information of individuals and businesses is leaked or processed by outside attacks or personal mistakes, thus misused, and thereby considerable damage is occurring. For this reason, the necessity of how to effectively manage personal and corporate information is emerging. This study intends to suggest a method that can protect servers and media information, which requires security. The access control method suggested here uses a way that grants users authority by grade and authenticates users through Two-Factor Authentication method.

Kabir, M.E. have worked on a role-involved purpose-based access control model. The structure of a CPAC model is defined and investigated. Access purpose is verified in a dynamic behavior, based on user attributes, context attributes, and authorization policies. Intended purposes are dynamically associated with the requested data object during the access decision. An algorithm is developed to achieve the compliance computation between access purposes and intended purposes and is illustrated with role-based access control (RBAC). Access purpose authorization and authentication in the model are studied with the hierarchical purpose structure.

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. Krikelas, Ilias and Ioannis Xydas 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. 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. The empirical results appear promising, which reflects that such a multi-factor decision support technique can be applied to real world identity management and authentication systems.

Introduction

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 baking 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.

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. The proposed technique will be using multi-tier double-trap image based authentication for the login protection in cloud platforms on mobile devices. The first-level authentication scheme consists of various small images of different objects and colors in 2x3 or 3x3 or other similar 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. The first stage will be also capable of mitigating the autobot/botnet/spam threats by differentiating between the user and the bots using its unique graphical password input method. The second stage authentication will be used to access the more private data and sensitive operation according to access control model design. The second level authentication will be based on a match-word based algorithm. The users will have to provide some secure codes for some selected images containing different types of easily memorable objects. The user will have to correctly match the secure codes for the object images in the first row with the second row for a specific number of objects. To add more security and to lower the probability of breaking into, some of the fake object images as well as the fake secure images can be also added to the front-end interface, where the user will have to first 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. The proposed will improve the efficiency of data access control models on the cloud platforms by removing the hindrance of the repeated text password inputs. 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 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.

CONCLUSION & FUTURE WORK

The proposed access control models for the cloud data is being implemented using the NS2 simulator. The implementation of the NS2 simulation will begin with the implementation of the basic simulation cloud data storage in the NS2 simulation. The basic cloud data storage simulation must be capable of releasing the data for the index formation. The basic access control model will be based upon the Role based access control model (RBAC). The role based access model enables the user to access the files in its scope according to the powers 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 (SLRB-RBAC). The infusion of both of the access control models i.e. RBAC and SLRB-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. Also, the proposed model will be enhanced for the higher level of security and data privacy.

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 Applicatio (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.