Journal of
Information Technology & Software Engineering

Baraithiya and Pateriya, J Inform Tech Softw Eng 2017, 7:5
DOI: 10.4172/2165-7866.1000215

Review Article Open Access

# An Analysis of Hybrid Authentication and Authorization Model for Web Based Application

**Harish Baraithiya* and RK Pateriya**

*Department of Computer Science and Engineering, MANIT, Bhopal, India*

## Abstract

An Identify Access Management (IAM) system is very important and trusted source for accessing the website related information. Now in real world it is always need for safe the personal and sensitive information of website from malicious insiders. It always needs a well-defined authentication and authorization mechanism to ensure only the right persons only can access the right applications at a right time with the given privilege. The website is having many users with different Identity and its Access Management via using authentication and authorization. The existing models have some limitations in the implementation phase in this research. This research having analysis of hybrid authentication and authorization model for secure and user-friendly web-based applications. It also compares different access control models and their features with the proposed hybrid model.

**Keywords:** Web usage mining; Authentication; Authorization; Web access control; Web-based applications; Security

## Introduction

Organizations in Industry and Education are predominantly using web-based applications to manage their day-to-day activities. It also manages other functionality of office with the effective running of their business. It is hosted in the organization's internal networks or online storage with the diverse domains in a cloud environment. Some of the applications are even managed and maintained by vendors or trusted third party providers. Securing those applications and also business information of organization from any kind of malicious activities is vital for any organization. Now there is a requirement for the web based applications secure. The organizations also require a well-defined authentication and access control mechanism has to be implemented. Generally, such authentication and authorization mechanisms are collectively known as Identity and Access Management (IAM) system. There are specific IAM process models to accomplish all these identity and access related organizational requirements in a structured way. Some types of access control models are Discretionary Access Control (DAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC).

Each existence model has its own advantages and disadvantages because they manage different credentials for authentication to each application. It is an inconvenience for employees as well as organizations. Now the Organizations commonly use Single Sign On (SSO) mechanism to avoid such inconveniences. The advantage of SSO mechanism is that the employees require only a single set of credentials to access the different application in an organization.

## Related Work

Laverdiere MA [1] proposes Pattern Traversal Flow Analysis (PTFA) that analyzes the traversal pattern of web users by using the derived formal models. This analysis automatically computes the counter for its definite protection properties with the privilege protection losses. It monitor the state changes by computed the privilege protections (Figure 1).

So the privilege protection state is managing their losses by third party or own release pairs system. It shows that the distribution of counter lengths with credential in the network. This functionality with file boundaries is to reduce unauthorized access. So finally the privilege protection counter characteristic is very helpful for the attention web security in developers' point of view.

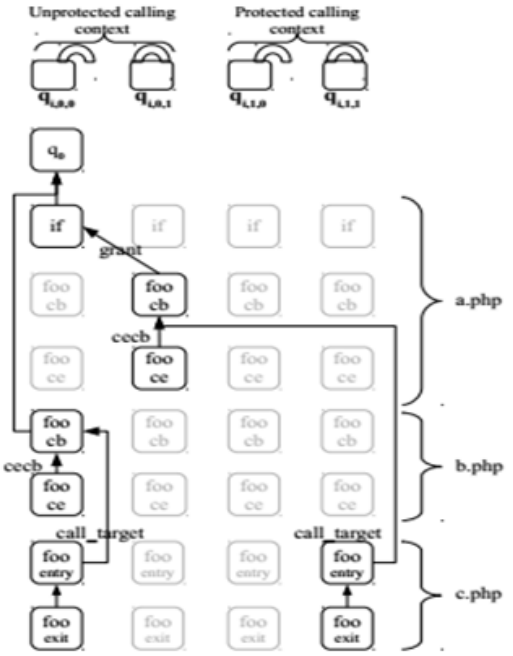


**Figure 1:** PTFA model for in running state.

Weili H [2] research shows that comprehensively study on the differences between passwords from English and Chinese web domain users. First it searches those Chinese preference digits when the web user is composing their passwords using letters in website. It provides the password strength based on its guessing similar. Second, it observes that both group of user's preferences the patterns that they are familiar

***Corresponding author:** Harish Baraithiya, Department of Computer Science and Engineering, MANIT, Bhopal, India, Tel: +91 9425495243; E-mail: harishbaraithiya7@gmail.com

**Received** November 06, 2017; **Accepted** November 15, 2017; **Published** November 21, 2017

**Citation:** Baraithiya H, Pateriya RK (2017) An Analysis of Hybrid Authentication and Authorization Model for Web Based Application. J Inform Tech Softw Eng 7: 215. doi: 10.4172/2165-7866.1000215

with Chinese and English words for English-dominant users. It evaluates and shows that the impacts of various Chinese input methods. Third, it observes that both Chinese and English-dominant users prefer conventional format for the construct passwords for that date.

Bourouis A [3] use the Symbolic Observation Graph (SOG) for the composition of Web services. This service is verifying the opacity of systems. It shows the verification of three kind of opacity in SOG. Web services are translated to the opacity of their composites in the website.

An open Work-Flow net is defined by a tuple -

N = (P, T, F, W, m0, I, O, $m_f$) where:

• (P, T, $F_{P\times T}$ , $W_{P\times T}$ ) is a WF-net;

• $m_0$ (where i is the sole place containing a token) is the initial marking;

• I (resp. O) is a set of input (resp. output) places (IUO represents the set of interface places) satisfying:

– (IUO)∩P = ∅;

– ∀p ∈ I: ˙p = ∅ (input interfaces places);

– ∀p ∈ O: p• = ∅ (output interface places);

• $m_f$ (where o is the sole place containing a token) is a final marking (Figure 2).

The proposed services establish a suitable abstraction that allows checking these opacity variants locally to each component of a composite WS using SOG.

Liu L [4] proposed an algorithm called the improved Bayesian attack graph (I-BAG) model. First the I-BAG takes attack management after that control the threat factors with its consideration. The website is having fewer security risks from using this one as compared to the existing attack graph models. It is used to improve Bayesian attack graph to optimized website attack graph with attack benefit nodes. It manages the threat factor nodes as well as the local conditional probability distribution. It calculates the probability of attack in website with the risk value based on the level of nodes. It is having the set of tuple in the following manner (Figure 3).

BGA = (V, A, E, T, S, P)

Now it compared with the traditional Bayesian attack graph model. So the improved model contains a set E and a set T. E is the set of attack benefit nodes, and T is the set of threat factor nodes. Since the set S contains four kinds of directed edges, S can be expressed as follows:

S = (V × A) U (T × A) U (A × V) U (A × E)

Mingqiang L [5] proposed a cloud storage model where a unified multi cloud storage solution is available for users. It is work as outsource backup data with reliability and security. It always provides some services with the cost efficiency guarantees. This service builds by using an augmented secret sharing scheme called convergent dispersal. It supports deduplication in the data by using deterministic content derived hashes as inputs to secret sharing (Figure 4).

In the proposed CDStore model it combines convergent dispersal by using with two-stage deduplication for the achievement of bandwidth as well as storage savings. It is also robust against side channel attacks that can be launched by a malicious user on the client side. It demonstrates the cost analysis to achieve significant monetary cost savings by using baseline cloud storage solutions.

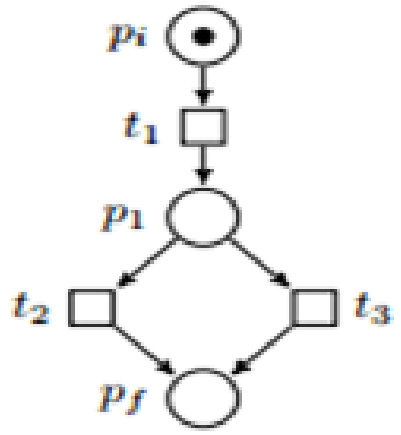


**Figure 2:** A wf-net.

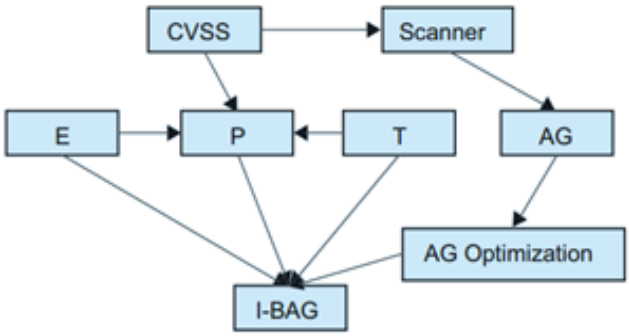


**Figure 3:** Building of I-BAG.

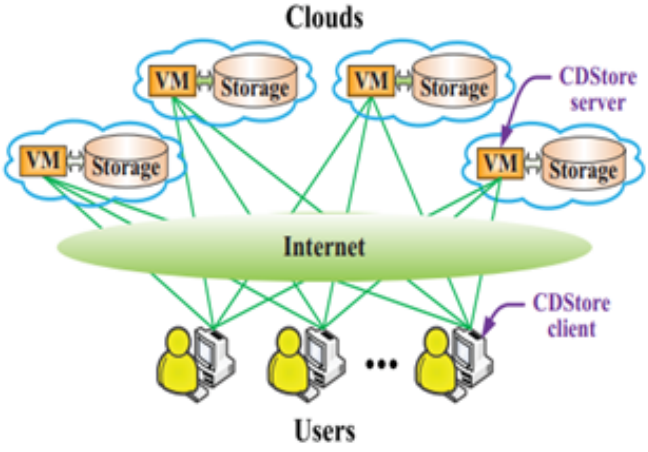


**Figure 4:** CD store architecture.

Anand PMR [6] shows that comparative analysis of different access control models. It shows that their features with the proposed hybrid model in the existing Organizations are using the Identity and Access Management (IAM) systems. It take care the utility management for the employees' identity and the access privileges of web users (Figure 5).

An IAM system acts as a single trusted with the source of identity and its access information. It is used to secure this sensitive information from malicious web user's cyber cell is responsible for the successful

operation of any organization. It provides a well-defined authentication and authorization mechanism just like a hybrid mechanism so that only the right persons at a right time can access the right applications with the provided privileges.

Joseph KL [7] introduces a new fine-grained two-factor authentication (2FA) access control system. It is used for web-based application which provides cloud computing services. The proposed approached is based on an attribute-based access control mechanism which is implemented using user secret key and a lightweight security device. Application user cannot access the system if it does not having the correct information of both the keys. It is manage the attribute-based control in the system to restrict the access to those users which having the same set of attributes to maintain the user privacy (Figure 6).

Wei S [8] proposes a role based access as well as data provenance model for secure the cross-domain interactions. This approach maintains a role-based data provenance scheme which handles the roles of originators of a data object to evaluate data trustworthiness (Figure 7).

It utilizes the secure data information as well as the derived data quality attributes in the cross domain access. This integrated model is providing better security and trustworthiness for many multi-domain service-based applications.

Hussain SU [9] presents the first Built-In-Self-Test scheme for on-the-fly evaluation of functions. It takes care of management for the access the desired statistical properties of TRNGs of machine (Figure 8).

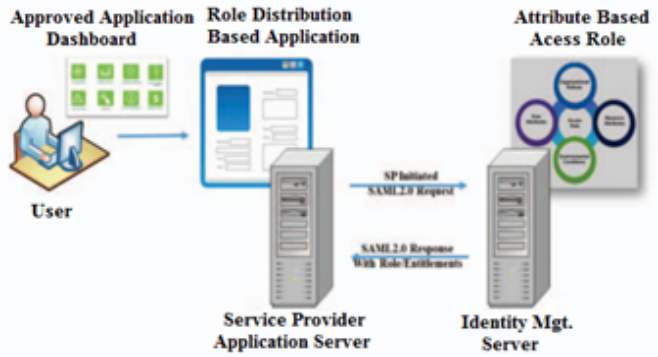


**Figure 5:** Proposed hybrid model for authentication and authorization.


**Figure 6:** Access authentication process.

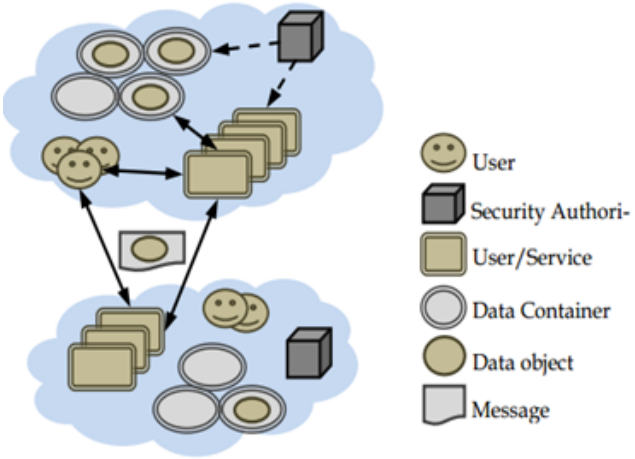


**Figure 7:** System model.

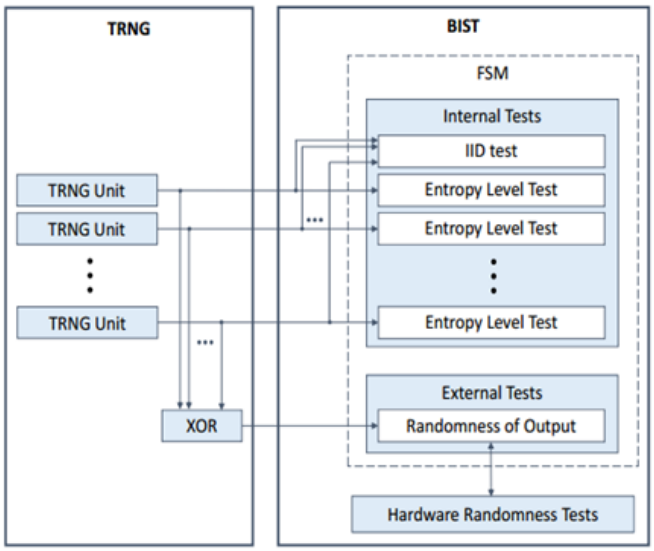


**Figure 8:** Architecture of the TRNG evaluation scheme.

In the scheme function evaluation suites is based on online as well offline. It manages online assessment as well as security properties of all in hardware. This architecture is designed to evaluate unpredictability and stability of functions. It is the first online test suite that evaluates the internal health of the machine. It shows that the statistical properties of the bit stream which is generated in the machine. So it provided very robustness and secure mechanism for the operational, structural, and environmental fluctuations when machine facing variations. It is having very reasonable overhead with the effectiveness and good practicality.

Ashraf MA [10] proposed a novel Service-Oriented framework for heterogeneous Deep Packet Inspection and Analysis (SoDPI). The proposed approach provides diversified DPIA services for the multiple client applications in the network to manage security operations with the high speed (Figure 9).

Now the Proposed framework provides very flexible as well as comprehensive API which is based on service interface for client applications. It is required to register before using these services. So this service is based on hardware commodity to deploys shared set of DPIA

which is related packet processing components. In this management only single copy of passive data is required so that it considerably reduced amount of software and hardware resources management to fulfill heterogeneous DPIA packet processing requirements with lower cost.

Cui L [11] defines an approach for a Policy-Aware and Network-aware VM management scheme. Both Aware are jointly considering DC communication cost reduction by using Virtual Machine (VM) migration. This action is performing the action when meeting network policy is required. It shows that the problem is NP-hard. It also derives an efficient approximate algorithm to reduce communication cost when it uses the policy constraints (Figure 10).

## Analysis of Previous Work

Table 1 shows the analysis of previous and current work.

## Conclusion

In this research, access control models to manage the employee's identity and access privileges. The proposed existing model helps to overcome the pain points of the current research for safe the private information. The hybrid model helps the organizations to implement the governance policies to maintain the dynamic user access control. It maintains the privileges depending upon the environmental conditions as well as user attributes. The key benefit of the existing

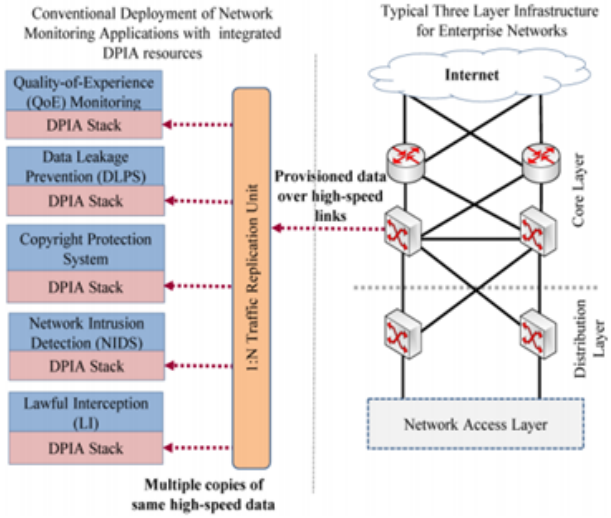


**Figure 9:** Conventional deployment approach for DPIA based systems.

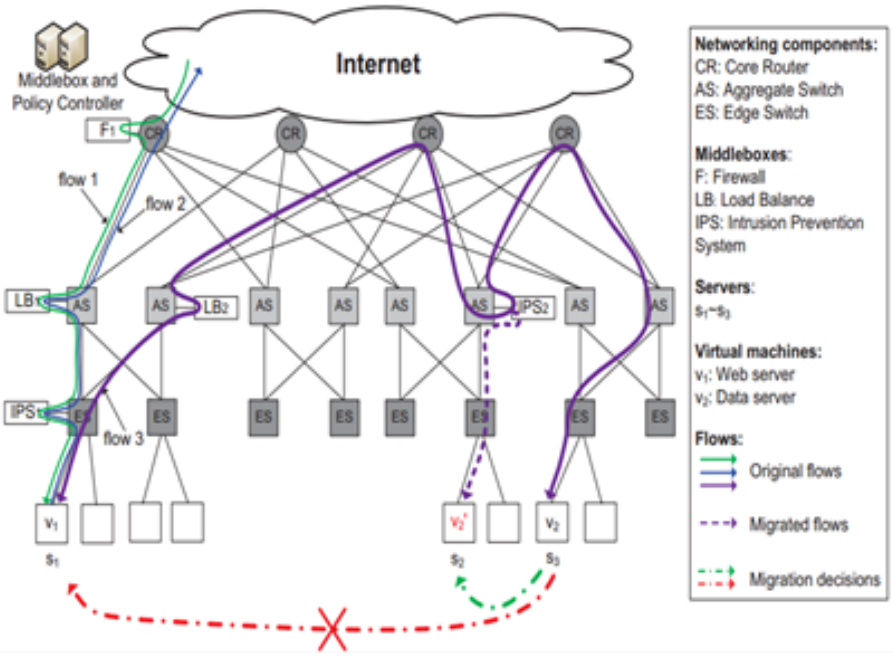


**Figure 10:** Flows traversing different sequences of middle boxes in DC networks.

| SN. | Authors | Title | Advantage | Disadvantage |
|---|---|---|---|---|
| 1. | Laverdiere MA [1] | Computing Counter-Examples for Privilege Protection Losses using Security Models | It is very helpful to focus developers' attention for security reviews. | It suffers from privilege protection loss in a release pair when it was definitely protected on all execution paths. |
| 2. | Han W [2] | Regional Patterns and Vulnerability Analysis of Chinese Web Passwords | It sheds light on understanding the impact of regional patterns on passwords. | The observed composition rules into the guessing rule set. |
| 3. | Bourouis A [3] | On the Verification of opacity in web services and their composition | The verification of three different types of opacity in SOG-abstracted WSs is good translated to the opacity of their composites. | The verification of their opacity without need for the original models. |
| 4. | Lin L [4] | A website security risk assessment method based on the I-BAG Model | It takes attack benefits and threat factors into consideration. | The local conditional probability distribution of each node, which is calculated accordingly. |
| 5. | Mingqiang L [5] | CDStore: Toward Reliable, Secure, and Cost-Efficient Cloud Storage via Convergent Dispersal | Cost savings over baseline cloud storage solutions with three aspects - reliability, security, and cost efficiency. | It adopts two-stage deduplication to achieve bandwidth. |
| 6. | Anand PMR [6] | Hybrid Authentication and Authorization Model for Web based Applications | It helps the organizations to implement the governance policies and dynamic user access control over the privileges depending upon the environmental conditions and user/application attributes. | It have limitations in the implementation phase. |
| 7. | Liu JK [7] | Fine-grained Two-factor Access Control for Web-based Cloud Computing Services | It restricts the access to those users with the same set of attributes while preserving user privacy. | Attributes comparison is more complex. |
| 8. | She W [8] | Role based integrated access control and data provenance for SOA based net centric systems | It enhances data provenance and access control, providing better security and trustworthiness. | It has many multi-domain service-based applications. |
| 9. | Hussain SU [9] | A Built-In-Self-Test Scheme for Online Evaluation of Physical Unclonable Functions and True Random Number Generators | It have good utilization for assessing the desired statistical properties of TRNGs. | The need for analysis and evaluation of the PUF input-output behavior. It concerned only with testing statistical quality of the TRNG output. |
| 10. | Ashraf MA [10] | A Heterogeneous Service-Oriented Deep Packet Inspection and Analysis Framework for Traffic-Aware Network Management and Security Systems | It proposed a novel Service-Oriented framework for heterogeneous Deep Packet Inspection and Analysis (SoDPI) that simultaneously provides diversified DPIA services to multiple client applications for network management and security operations in high speed networks. | To manage the load balancing in the network management traffic. |
| 11. | Cui L [11] | PLAN-Joint Policy- and Network-Aware VM Management for Cloud Data Centers | To reduce communication cost while adhering to policy constraints. | Initially it takes more execution time. |

**Table 1:** The analysis of previous and current work.

model compared with the other existing access control models in the organization to ensure the right persons are accessing right applications with right privileges. In future work, other data mining algorithms can be implemented in cloud to efficiency handle big data of many Hospital website in distributed environment for finding any critical diseases.

## References

1. Laverdiere MA (2017) Computing Counter-Examples for Privilege Protection Losses using Security Models. IEEE (SANER). pp: 240-249.
2. Han W, Li Z, Yuan L, Xu W (2016) Regional Patterns and Vulnerability Analysis of Chinese Web Passwords. IEEE Trans. Inf Forensibcs Security 11: 258-272.
3. Bourouis A, Klai K, Hadj-Alouane NB, Touati YE (2017) On the Verification of Opacity in Web Services and their Composition. IEEE Trans Services Computing 10: 66-79.
4. Lin L, Liu L, Huang C, Zhang Z, Fang Y (2016) A Website Security Risk Assessment Method based on the I-BAG Model. IEEE China Commun 13: 172-181.
5. Mingqiang L, Qin C, Li J, Lee PPC (2016) CDStore: Toward Reliable, Secure, and Cost-Efficient Cloud Storage via Convergent Dispersal. IEEE Internet Comput 20: 45-53.
6. Indu I, Anand PMR (2016) Hybrid Authentication and Authorization Model for Web based Applications. IEEE WiSPNET. pp; 1187-1191.
7. Liu JK, Au MH, Huang X, Lu R, Li J (2016) Fine-grained Two-factor Access Control for Web-based Cloud Computing Services. IEEE Trans Inf Forensics Security 11: 484-497.
8. She W, Ling YI, Bastani F, Tran B, Thuraisingham B (2016) Role Based Integrated Access Control and Data Provenance for SOA Based Net Centric Systems. IEEE SOSE 9: 940-953.
9. Hussain SU, Majzoobi M, Koushanfar F (2016) A Built-In-Self-Test Scheme for Online Evaluation of Physical Unclonable Functions and True Random Number Generators. IEEE Trans Multi-Scale Comp Sys 2: 1-15.
10. Ashraf MA, Jamal H, Khan SA, Ahmed Z, Baig MI (2016) A Heterogeneous Service-Oriented Deep Packet Inspection and Analysis Framework for Traffic-Aware Network Management and Security Systems. IEEE Access 4: 5918-5936.
11. Cui L, Tso FP, Pezaros DP, Jia W, Zhao W (2017) PLAN-Joint Policy and Network-Aware VM Management for Cloud Data Centers. IEEE Trans Parallel Distrib Syst 28: 1163-1175.