The International Journal Of Engineering And Science (IJES)
|| Volume || 3 || Issue || 9 || Pages || PP 70-73|| 2014 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Identity Access Management and Multi-Tier Cloud Infrastructure for Secure Voting System

[1]Bhosale Poonam, [2]Vethekar Priyanka, [3]Thorat Lata, [4]Suchitra Shinde, [5]Archana Lomte
[1,2,3,4,5]*Department of Computer Science,JSPM'S BSIOTR Wagholi*

----------**ABSTRACT**----------
Integrity of election process will determine the integrity of democracy itself. So the election system must be secure and robust against a variety of fraudulent behaviours, should be transparent and comprehensible that voter and candidates can accept the result of election. But in history, there are examples of election being manipulated in order to influence their outcome. Anonymity of ballot should be preserved both to guarantee that voter have no proof that proves which candidates receive their votes. Architecture to manage identity and access in Multi-tier cloud infrastructure, in which most services are supported by massive-scale data centre over the internet. Multi-tier cloud infrastructure uses tier-based model from software engineering to provide resources in different tiers. In this paper we focus on design and implementation of centralized identity and access management system for the multi-tier cloud infrastructure. First we discuss identity and access management requirement in such an environment and propose our solution to address these requirements. Next we discuss approaches to improve performance of the IAM system and make it scalable to billion of users.

KEYWORDS : *IAM (Identity Access Management) SAVI, (Smart Application On Virtual Infrastructure) , Encryption, Decryption, multi-tier cloud*

Date of Submission: 08 September 2014 Date of Publication: 25 September 2014

I. INTRODUCTION

Identity access management and multi-tier cloud for secure voting system using IAM and steganography at the same time to voter account. The scheme uses as cover object for steganography and as keys for identity access management. Proper uses of identity access management reduce risks in this system hackers have to find the both secret key. The basic idea is match the symmetric key with the cover image on the basis of key image. The stego image not detectable by human eyes. The target of a system is authentication requirement of a voting system .The objective of identity access management and multi-tier cloud for secure voting system is user authentication using IAM and stenography using LSB to hide user voting id. Cloud computing hosting and delivery of service of over the internet .Most services have been supported by massive scale distant data-centres located at sites however, sub-services will require low latency the Smart applications virtual infrastructure like SAVI. Project has been established with a focus on future platform applications enablement.

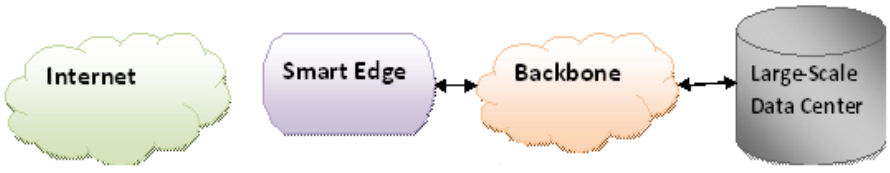

Fig. 1. Multi-Tier Cloud Infrastructure

The smart application on virtual infrastructure that is SAVI project has established with a focus on future application for platform designed [2]. As shown in figure1.1 SAVI consider a multi-tier cloud infrastructure that is a internet to include smart/core edges where user work together large data centre to provide best service

quality. The secure communication video sharing and fast wireless access control are the rising application for which the smart edge should go by node convention cloud resource

II. PROPOSE DESIGN SYSTEM

Identity access management by using on line voting system for avoid fake voting system or producing true result not fake result. The On line voting system the client register our data in intermediate server .The intermediate server send the data to the centralize server save this data send the encrypted key to the intermediate server .Intermediate server send one key to the user and same key send centralize server which is symmetric key format. In this system we use AES (Advance encryption standard) and minutia based approach for fingerprint .This system uses figure print device for avoid hacking.

Caching layer cache the data from user and caching prevent redundant access to the database and avoid the unnecessary data formatting. Cache layer is middle layer of identity access management system which is called inter mediate server.

By using IAM solution for the multi tier solution that is SAVI [2]. SAVI include core node, edge node resources that are used for creating application. The SAVI IAM is a centre identity manager with distributed middle ware based [1]. In IAM architecture there are six basic component like Manifesting Management ,Identity Management, Policy Management, Token Management, Authentication Management and Middle ware Fig.2.1 show the this component how to interact to each other .The Manifesting Management list can be updated, retrieve and create. The next component is used to Identity Management which is store manipulate user same as Policy management component store access management. Policies to perform create, update,retrieves,delete operation on the Policies. Token Management generate authentication services. It supports two formats Universally Unique Identifier and Public key Infrastructure [1].

Middleware reside in front of resource provider to capture request. IAM has two Middleware authentication and authorization. Authentication check the request action again the Policy and Authentication validate the security token.

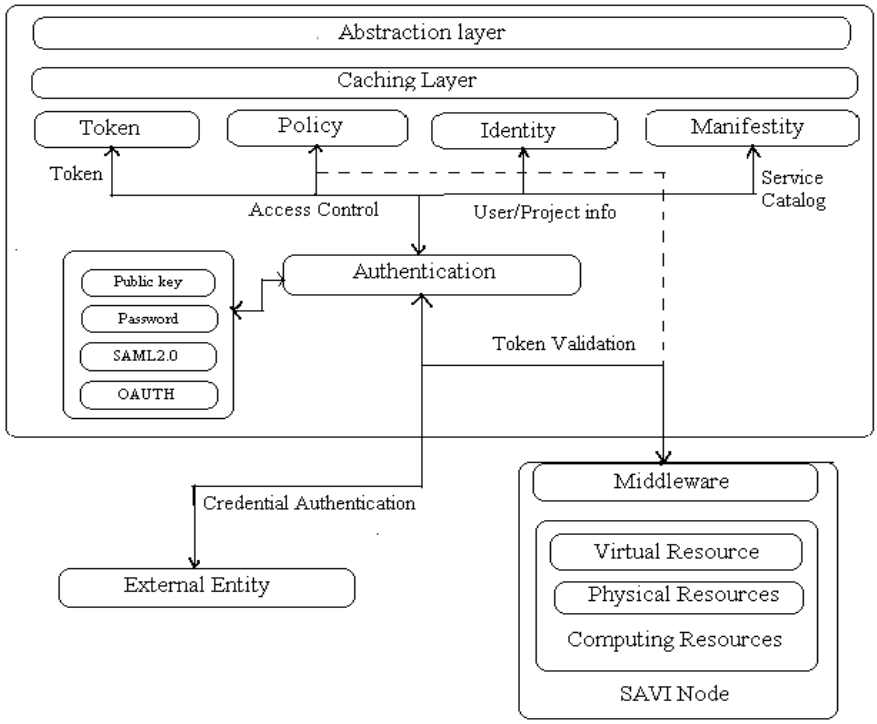

Fig. 2. IAM Architecture

This application used multi-tier architecture there are three layer client, intermediate server and centralize server .This three layer relate to each other. Intermediate server work as each state. This system used intermediate server because it reduce the centralize server load .The centralize server store data which is gain from each state level intermediate server. In On line Voting system firstly client register our information on the intermediate server . Intermediate server generate symmetric key. That same key pass client and centralize server. For generating key by using algorithm AES(Advance Encryption Standard). At the registration time for best security we used fingerprint device by using algorithm Minutia Based approach for fingerprint. Without

registration client can't do the voting because client does not know about key. when client goes to voting that time client login

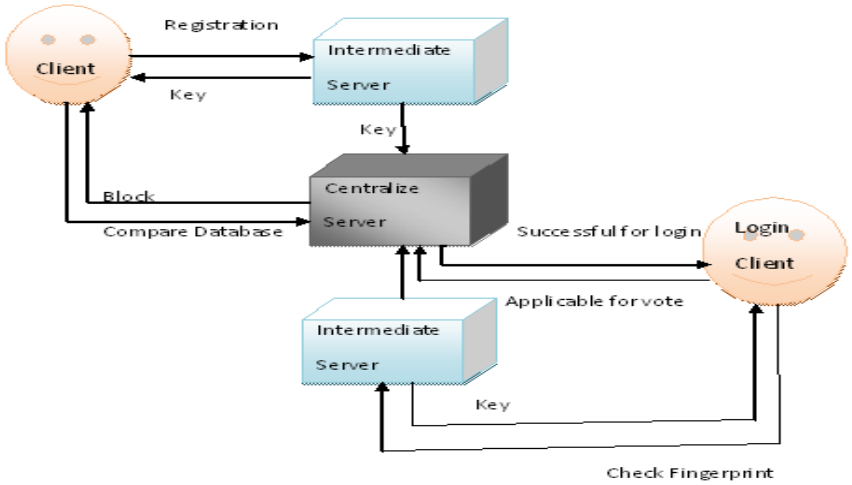

Fig. 3. Online Voting System Architecture

III. LITERATURE SURVEY

In past we have traditional voting system in which voter must have to go their own town for voting due to a migration. And also in election system there are many possibilities of fraudulent behaviours. Because of all this reason of migration and fraud behaviour voter run away from election. So to avoid all this in voting system, whether it is traditional paper ballots or electronic system, the system must have to meet following criteria:

1. Invisibility: Invisibility of ballots should be preserved; both to guarantee the voter safety when voting against a malevolent candidate and to guarantee that voter have no proof that proves which candidates received their votes.
2. Tamper-resistant: To avoid the wide range of attacks, including ballots stuffing by voters and incorrect tallying by insiders the voting system must be tamper-proof.
3. Human factors: A voting system must be robust and usable by entire citizen regardless of age and illiteracy[6].

Election allows the citizen to choose their candidates and express their priorities for how they will be governed. The integrity of voting process is fundamental to integrity of democracy. The voting process must be efficiently robust to withstand a variety of fraudulent behaviours and must be sufficiently transparent and comprehensible that voters and candidate can accept the result of an election [7]. The design of a "good" voting system whether electronic or using traditional paper ballots or mechanical devices must satisfy a number of sometimes competing criteria. The existence of such evidence would allow votes to be purchased by candidates. As in traditional voting system, voters have to go their home precinct and prove that they are allowed to votes there, perhaps by presenting an ID card, although some states allow voters to cast votes without any identification at all. After this, the voter is typically given a PIN, a smartcard, or some other token that allows them to approach a voting terminal, enter the token that allows them to approach a voting terminal, enter the token and then vote for their candidates of choice [10].

Also there has been cryptographic research on electronic voting, and there are few approaches such as currently the most viable solution for securing electronic voting machines is to introduce a "voter-verifiable audit trail". A DRE system with a printer attachment or even a traditional optical scan system will satisfy this requirement by having a piece of paper for voters to read and verify that their intent is correct reflected.

IV. CONCLUSION

In this paper, we have developed online voting system using IAM, SAVI, and Multi-tier cloud infrastructure for secure voting environment. In this system we tried to avoid fraud voting. In online voting system result declaration becomes easy, fast and voting becomes possible for migrated user. Online voting system provides fast generation of region wise result. It's a result should be in correct manner. Online voting system increases the system productivity by casting number of votes.

V. ACKNOWLEDGEMENTS

Paper is a test of not only technical skill but also team work. This journey could not be completed without the support of guide and group member. We would like to thanks Prof. A. C. Lomte. To co-ordinate us. And this study provided us the opportunity to work with this best topic and excellent supervision. Finally, we want to thank my expert Staff for always being there.

REFERENCES

[1] Mohammad Faraji, Joon -Myung Kang, Hadi Bannazadeh, and Alberto Leon-Garcia Department of Electrical and Computer Engineering University of Toronto, Toronto, ON, Canada Email: fms .faraji, joonmyung.kang , hadi .bannazadeh, alberto.leongarcia HYPERLINK "mailto:alberto.leongarciag@utoronto.ca" HYPERLINK "mailto:alberto.leongarciag@utoronto.ca"@utoronto.ca

[2] J.-M. Kang, H. Bannazadeh, and A. Leon-Garcia, "Savi testbed: Control and management of converged virtual ict resources," in Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on. IEEE, 2013, pp. 664–667.

[3] K. Gunjan, G. Sahoo, and R. Tiwari, "Identity management in cloud computing–a review," International Journal of Engineering, vol. 1,no. 4, 2012.

[4] A. Jøsang and S. Pope, "User centric identity management," in AusCERT Asia Pacific Information Technology Security Conference. Citeseer, 2005, p. 77.

[5] T. F. Steve Schwab, "Managing identity and authorization for community clouds," Duke University, Tech. Rep., 2012. [Online]. Available: www.exogeni.net/

[6] 2011 Second International Conference on Emerging Applications of Information Technology Shivendra Katiyar, Kullai Reddy Meka, Ferdous A.Barbhuiya,Sukumar Nandi *{s.katiyar, kullai, ferdous, sukumar}@iitg.ernet.in*

[7] The IEEE, appears in *IEEE Symposium on Security and Privacy 2004*. IEEE Computer Society Press, May 2004. This paper previously appeared as Johns Hopkins University Information Security Institute Technical Report TR-2003-19, July 23, 2003.

[8] J.-M. Kang, H. Bannazadeh, and A. Leon-Garcia, "Savi testbed: Controland management of converged virtual ict resources," in Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on. IEEE, 2013, pp. 664–667.

[9] B. Kandukuri, V. Paturi, and A. Rakshit, "Cloud security issues," in Services Computing, 2009. SCC '09. IEEE International Conference on, 2009, pp. 517–520

[10] J. Chase, L. Grit, D. Irwin, V. Marupadi, P. Shivam, and A. Yumerefendi, "Beyond virtual data centers: Toward an open resource control architecture," in in Selected Papers from the International Conference on the Virtual Computing Initiative (ACM Digital Library),ACM, 2007.

[11] P. Liu, S. Jajodia, and C. D. McCollum, "Intrusion confinement by isolation in information systems," Journal of Computer Security, vol. 8, 2000.

[12] N. Gunti, W. Sun, and M. Niamat, "I-rbac: Isolation enabled role-based access control," in Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on, 2011, pp. 79–86.

[13] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Rolebased access control models," Computer, vol. 29, no. 2, pp. 38–47,Feb. 1996. Available: http://dx.doi.org/10.1109/2.485845