International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Enhanced e-Government Process Model with Customer Centric Cloud

Sreekanth D.*[1], Gladston Raj S. [2]
*[1]Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore, Tamilnadu, India
[2]Assistant Professor, Department of Computer Science, Govt. College, Nedumangad- University of Kerala, Trivandrum, India

ABSTRACT

The adoption of perfect technologies in the area of e-governance improves service delivery in a cost effective and secured manner. The success of every e-governance projects fully depends upon the utilisation of the end user, so that the wide range of acceptability and security should be assured through the significant approach of system design. Every customer centric systems should provide better services, fast and reliable information to every citizen. A review of literature indicates that the majority of the e-governance projects again undergoes with the manual processing due to the insignificant design of the system. Here we propose an improved service delivery, secured, customer centric and multi tired authentication system by adopting cloud environment as a service. The architecture proposes service delivery at various levels and there will be no lack in providing the service even if the concerned person in the department is unavailable. Every validation processes of each service will be processed by the system with the available data sources, which is already available with other e-governing systems.

Keywords : Cloud Computing, e-Government, LSGI, Cloud Security

I. INTRODUCTION

In the traditional hosting, system storage and usage are fixed, but the current trend in business requires dynamism in computer and data storage. This leads to the development of cloud model. Cloud computing proposes a new perspective model in the computing infrastructure such as Resource, Platform and Software. It provides the appropriate structure, allocation and reallocation of resources when required, virtual storage and networking facility. It satisfies the demand requirements of the user. Cloud computing establishes a sharable resource "as a- service" unit. For the institution, the system facilitates data management points to make their information available all over the world. It eradicates the liability of local nodes for maintaining their data and cloud supports optimized resources on the web. Cloud Service Providers manages resources and data management automatically via the application software.

II. CUSTOMER CENTRIC CLOUD

The proposed system will be able to provide the end-to-end facility to every customer or people who all are visiting the LSGI's (Local Self-Governing Institutions) or requesting the services of the LSGI. The system can do the verifications and validations as a part of the requisition process. Approval, disapproval and querying facilities are provided to the sanctioning authorities and the official hierarchy approvals also can be managed.

The customer centric cloud works based on cloud computing. The technology provides major information sharing among the organisations. Each activities or services of every LSGI's can be tuned by the onetime and initial settings. The various levels of sanctions among the employees of LSGI's depend upon the hierarchy of employees and can be set up. Customers can request for the services and depends upon the request category the system will be automatically tracks the information from various respective servers. On the basis of the priority levels among the

organisation/ LSGI management, the divisions in each levels can be taken by the assigned officials. In case of various levels for the request sanctioning can be passed with comments from each levels of officials.

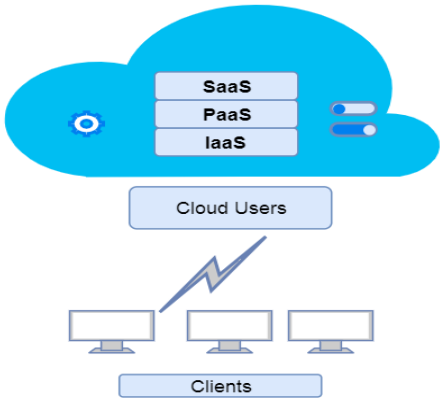

Figure 1. Cloud Users and Layers

There are several security concerns connected with cloud computing but these concerns fall into two broad categories: Security issues connected with cloud providers (organizations providing cloud services) and security issues faced by their customers. In most of all cases, the organization must ensure that the services provided by them is secure and their clients' data and applications are protected, and the customer should have an assurance that the service provider has taken the proper security measures to protect their information in a significant manner.

Though Cloud offers sophisticated storage and access environment, it is not hundred percent reliable; the challenge exists in ensuring the authorized access. The third parties make such decisions about our data, and therefore security remains as a big concern. So cloud applications must ensure that the data accessed is by the authorized users. Cloud computing uses n-domain environments and each of them required to have different perspectives for security. Authentication and identity management can help the users to authenticate and getting services based on their credentials. Key issue about identity management in cloud is various kinds of protocols and its interoperability.

III. SYSTEM ARCHITECTURE

Cloud infrastructure provides computation, software, data access, and storage resources without pointing out the location and other details of the computing infrastructure. The key features being centralized processors, memory, storage, and bandwidth allocation. Cloud server hosting solutions reduce the overhead cost of server hardware and other applications. Cloud services are fully redundant and multi server systems which are easily scalable and can be virtualized on demand. This security implementation using authentication will provide a new platform designed to cope with the increasing demand for data and cloud based services.

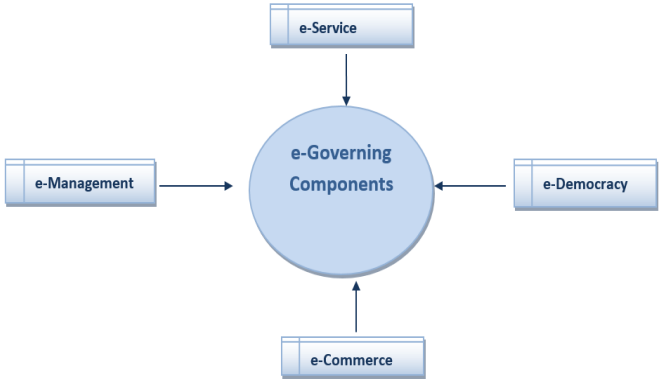

Figure 2. System Architecture

IV. EXISTING SYSTEM

The half-automated system is placed as a part of e-governance implementation in the LSGI's. The system proposes the fully automation and it cannot be treated as fully automated is the real output of the existing system. The existing system provides the facility to collect the service requisitions from the customers the LSGI officials and have to do all the verification and validation works manually before providing the service to the customer. The motivation behind the proposed system is a fully automated, request, response, and decision-making system to every LSGI's.

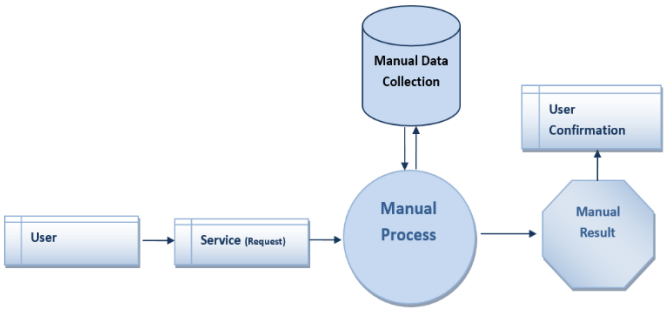

Figure 3. Existing System

A. WORK FLOW

- Customer requests the service
- E- Governing system verifies the relevant fields
- Verifies the fields / ID's feeds by the customer with existing cloud servers.
- Make decisions on the customer request by verifying the relevant fields.
- Reports to the respective official about the decision generated on customer's request.
- In case of higher official's authorization, the job/service will be transferred to the respective official.
- The final decision on the customer request can be generated by the official based on the report of the decision support system.

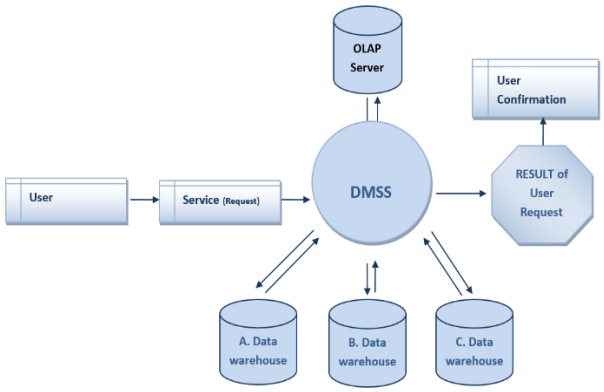

Figure 4. Proposed System's Flow

V. SYSTEM RELIABILITY

The cloud reliability model is service oriented and hierarchical, which is tractable and effective in addressing such a large and complex system. The reliability of the cloud computing is very critical but hard to analyze due to its characteristics of heterogeneous Software/hardware components, massive-scale service sharing, WAN, and complicated interactions among them. This new model considers various types of failures that have significant influences on the success/failure of cloud services including overflow, timeout, data resource missing, computing resource missing, software failure, database failure, hardware failure, and network failure.

VI. APPLICATION STRUCTURE

While using the cloud services it requires to register with personal information that may be used while authentication and authorization process. Also, Cloud is a great target for attackers who may get or examine the personal information during sending and receiving such information, which causes to harm on privacy protection. When third party comes in focus it becomes more crucial to manage it. Personally, identifiable information (PII): any information that could be used to identify or locate an individual (e.g. name, address) or information that can be correlated with other information to identify an individual (e.g. Mobile number, credit card number, postal code, Internet Protocol (IP) address). The work flow of the proposed system as follows.

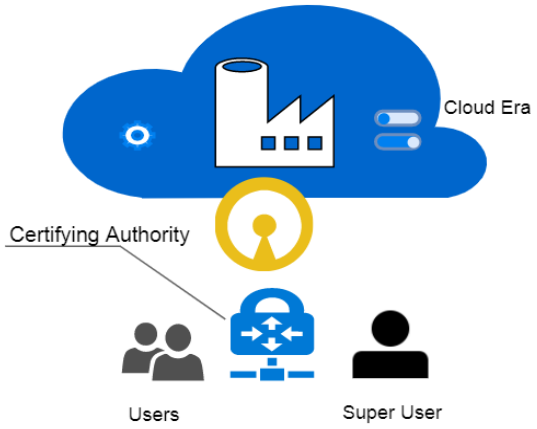

Figure 5. Application Structure

In cloud computing the information being accessed from a centralized storage, and does not need any user to be in a specific place to access it. This is a method in which information is delivered and resources are retrieved, rather than a direct connection to a server. There are so many issues in storing the data securely in the cloud because most of the sensitive information is centralized in to clouds. But the most important aspect arises while access of data.

The user stores their data in the cloud and any authorized person can access those files. In Cloud server we use the mechanism of certificate management for authentication, otherwise on retrieval they can do modification, insertion and deletion in the original files and can store back in clouds. So, the original data can be mishandled, which may cause security problems. So here PKI plays a key role.

VII. SECURITY PERSPECTIVE

We know that the major issue in the cloud applications are that of the security issues. Before adopting this

technology, we should know that we are surrendering all our company's information to a third-party cloud application hoister. This cloud application provider may put our company to great risk. Hence, we need to make perfectly sure that we have chosen the most reliable service provider, who will keep our data totally secure. The various models for cloud service delivery (IaaS, PaaS, and SaaS) have different perspective for the customer when it comes to security.

VIII. CONCLUSION

In this system we have proposed a secured authorised server, scalable middleware architecture that intends to support secure cloud computing for both enterprise and individual user especially for LSGI's. We have implemented a gateway and validation architecture for the perfect automation of the LSGI activities. The data collects and stores into cloud applications with proper encryption standards. The success of the e-governing system fully depends upon the active participation of the citizens and the e-governing level can be attained only using such a well-structured system architecture.

IX. REFERENCES

[1] John Steven, jsteven@cigital.com,Gunnar Peterson, gunnar@arctecgroup.net, A Security Architecture Stack for the Cloud- IEEE SECURITY & PRIVACY.

[2] A Method for Trust Management in Cloud Computing: Data Coloring by Cloud Watermarking Yu-Chao Liu1,Yu-Tao Ma , Hai-Su Zhang De-Yi Li Gui-Sheng Chen - International Journal of Automation and Computing.

[3] A PACS archive architecture supported on cloud services - Luís A. Bastião Silva · Carlos Costa José Luis Oliveira, Received: 10 January 2011 / Accepted: 20 May 2011 / Published online: 16 June 2011 © CARS 2011.

[4] Bertino, E., F. Paci and R. Ferrini, 2009. Privacy-Preserving Digital Identity Management for Cloud Computing. IEEE Data Eng. Bull., 32: 21-27.

[5] Bruening, P.J. and B.C. Treacy, 2009. Cloud Computing: Privacy, Security Challenges. Bureau of Nat'l Affairs.

[6] Catteddu, D. and G. Hogben, 2009. Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA.

[7] Cong, W., W. Qian and R. Kui, 2009. Ensuring Data Security in Cloud Computing. IEEE.

[8] Ko, M., G.J. Ahn and M. Shehab, 2009. Privacy-Enhanced User-Centric Identity Management. Proceeding IEEE.

[9] William, S., 2005. Cryptography and Network Security Principles and Practices. 4th Edn., PHI.

[10] M. Bellare and S. Micali. How To Sign Given Any Trapdoor Function. In Crypto '88, LNCS 403, ages 200{215. Springer-Verlag, 1989.

[11] S. A. Brands. Untraceable Off-line Cash in Wallets with Observers. In Crypto '93, LNCS 773, pages 302{318. Springer-Verlag, 1994.

[12] D. Chaum. Blind Signatures for Untraceable Payments. In Crypto '82, pages 199{203. Plenum, NY, 1983.

[13] K.L et-al (1978) Local government and information technology in the United States

[14] Caldow ,j (1999) 'The quest for electronic government: A defining Vision

[15] West D.M. (2004) e-government and the transformation of service delivery and citizen attitude.

[16] Lee (2005) e-government : key success factors for value discovery and realization

[17] Chen et-al (2006) e-government strategies in developed and developing countries: An implementation framework and Case study