Implementation Paper of Computational Trust System on Cloud Environment

Mr.Varpe Y.D[1], Prof.Nirmal M.D[2]
[1]Dept of Computer Engineering
[2]Assistant Professor, Dept of Computer Engineering
[1, 2] PREC, Loni,Savitribai Phule Pune University, Pune India.

Abstract- *Now a days the Cloud computing is fast changing the digital service landscape. A explosion of Cloud providers has emerged, the difficulty of consumer decisions is rise. Trust issues have been recognized as a factor holding back Cloud adoption. Trust is a key that signifies backtracking Cloud implementation. The risks and challenges inherent within the implementation of Cloud services square measure well recognized within the computing literature. In combination with these risks, the comparative innovation of the online environment as a context for the supply of business services will increase consumer perceptions of indecision. Due to the lack of transparency the indecision is worsened in a Cloud context, from the user perspective, into the service types, operational conditions and the quality of service offered by the various providers. The Previous approaches failed to provide an suitable medium for communicating trust and trustworthiness in Clouds. A new approach is required to improve consumer assurance and trust in Cloud providers. In this paper presents the operation of a trust label system designed to communicate trust and trustworthiness in Cloud services.*

We explain the technical in details and implementation of the trust label components. Based on a use case scenario, an first evaluation was carried out to test its operations and its usefulness for increasing consumer trust in Cloud services.

Keywords- Service Monitoring, Trustmark, Cloud Services, Data Location, Trust Label, Cloud Computing, Trustworthiness.

I. INTRODUCTION

Cloud Computing is fast transforming the Information Technology and methods of improving digital services and their means of utilization. Gartner (2015) describe Cloud Computing as the foundation of digital business, as it support and facilitates new methods of deliver digital services to customers. Predictions of the market of the global Cloud Computing industry guess that it will reach U.S 241 billion by 2020. As a result, Cloud Computing has become a key component of Information Technology and business strategy, combining the benefits of Information Technology competence and business alertness. It offers many benefits to consumers including: economy of scale, on-demand resource provisioning, and a pay-as you go billing model that replace capital expenses with operational expenses. Cloud services include different layers of resources, ranging from infrastructure at the low layer to software applications at the high. The advantages of Cloud Computing contain instant access to hardware resource; minor IT barriers to innovation, easier scaling for service provisioning and minor cost of entry for small firms engaged in compute concentrated tasks. Despite these significant advantages, the acceptance of Cloud Computing has come up against a number of barriers such as data influence and location, security and trust, portability and technology clearness, business-related barrier and industrial policy. Along with these barriers, consumer trust has been measured a most important hind to Cloud uptake due to the large-scale and conceptual nature of Cloud services. Consumers not have insight into Cloud service operations and as a result find it not easy to trust them. In addition, the impact of trust on implementation of, and interaction with, information communication technology is widely recognized. Experts in the field argue that the major Impediment to Cloud adoption is likely to be attitudinal rather than technological. This suggest that researchers should take a holistic approach to the study of Cloud acceptance, incorporate considerations of consumer attitudes along with technological advances.

II. PROBLEM STATEMENT

The Problem is to determine as follows,

1. To growth of authorization mechanism for secure information access by a numbes of user in an open environment is an important problem in the ever-growing Internet world.
2. To Propose a dynamic trust model for user authorization, rooted in findings from social science. Unlike most existing computational trust models, this model differentiate trusting belief in consistency from that in competence in different contexts and accounts for subjectivity in the evaluation of a particular trustee by different thruster.

3. Simulation studies were conducted to compare the performance of the proposed integrity belief model with other trust models from the literature for different user behavior patterns. Experiments show that the proposed model achieve higher performance than other models particularly in predicting the behavior of unbalanced users.

III. LITERATURE SURVEY

S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, The evolution of cloud computing over the past few years is potentially one of the most important advances in the history of computing. However, if cloud computing is to achieve its potential, there needs to be a clear understanding of the various issues concerned, both from the perspective of the providers and the consumers of the technology. Even as a lot of research is currently taking place in the technology itself, there is an equally imperative need for understanding the business-related issues immediate cloud computing. In this article, we identify the strengths, weaknesses, opportunities and threats for the cloud computing industry. We then identify the various issues that will affect the different stakeholders of cloud computing. We also issue a set of recommendations for the practitioners who will provide and manage this technology. For IS researchers, we outline the different areas of research that need attention so that we are in a position to advice the industry in the years to come. Finally, we outline some of the key issues facing governmental agencies who, due to the unique nature of the technology, will have to become intimately involved in the regulation of cloud computing.

European Commission, Cloud Computing and Social Network Sites (SNS) are among the most controversially discussed developments in recent years. The opportunities of using powerful computing resources on demand via the web are considered as a possible driver for the growth of the European economy. However, there are also critics arguing that economic, social and technical risks prevail or even dismiss the potentials of Cloud Computing and SNS. This project sheds light on these aspects and analyzed more specifically, the latest technological and economic developments, driving factors and barriers in Europe, the main actors and their respective interests, the impacts on citizens, business and public administrations and, a broad range of technical, economic, cultural, legal, regulatory issues and their impacts. It showed that at the moment, there is a chance to achieve multiple Cloud Computing and SNS related goals simultaneously. There are no contradictions between assuring European citizens, secure, privacy aware, legally certain and fair use of Cloud Computing and SNS and in increasing the competitiveness of European ICT industries. Moreover it is possible to exploit the potential of Cloud Computing and SNS to the benefit of both the European economy and society at large. Based on this a set of options for European policy makers grouped into four themes with in total 16 options was derived.

K. Hwang and D. Li, Trust and security have prevented businesses from fully accepting cloud platforms. To protect clouds, providers must first secure virtualized datacenter resources, uphold user privacy, and preserve data integrity. The authors suggest using a trust-overlay network over multiple data centers to implement a reputation system for establishing trust between service providers and data owner. Data coloring and software watermarking techniques protect shared data objects and massively distributed software modules. These techniques defend multi-way authentications, enable single sign-on in the cloud, and tighten access control for sensitive data in both public and private clouds.

T. Lynn, L. van der Werff, G. Hunt, and P. Healy, Low consumer trust presents a significant hurdle to cloud service acceptance and the growth of the cloud industry. The cloud environment is generally apparent to have high levels of uncertainty and risk. Trust plays a central role in allowing consumers to overcome this risk when making adoption decisions. This paper discuss the characteristics of cloud services that form the basis for consumer trust decisions and argues that service providers need a more transparent, accessible method of communicating these characteristics to potential consumers. As such, this paper is straight related to conference tracks discussing consumer-oriented digital services and in particular the topic of consumer trust in digital society. Drawing on the nutrition label concept and aspects of previous computational trust models, we propose a dynamic trust label for cloud computing. The cloud trust label aims at present real time and cumulative metrics to consumers in an easily understandable format. In doing so, the label can be used to aid knowledge based trust decisions and ultimately encourage implementation of cloud services.

IV. EXISTING SYSTEM

1. Many Existing models and security mechanisms rely on a social network structure.
2. Pujol et al. propose an approach to extract reputation from the social network topology that encodes reputation information.
3. Walter et al. propose a trust model for social networks, based on the concept of feedback centrality. The model, which enables computing trust between two disconnected nodes in the network through their neighbor nodes, is suitable for application to recommender systems.

4. Lang proposes a trust model for access control in social networks, based on the assumption of transitivity of trust in social networks, where a simple mathematical model based on fuzzy set membership is used to calculate the trustworthiness of each node in a trust graph symbolize connections between network nodes.

DISADVANTAGES OF EXISTING SYSTEM:

- The ordinary Research efforts for user authorization mechanisms in environments where a potential people permission set is not already define mostly focus on role-based access control.Which divides the authorization procedure into the role-permission.
- The existing approach do not consider "context" as a factor affecting the value of trust, which prevent an accurate representation for practical life situations.

V. PROPOSED SYSTEM

- To Propose a computational dynamic trust model for user authorization. Mechanisms for building trusting belief using the first-hand as well as second-hand information are integrated into the model. The contributions of the model to computational trust literature are:
- The model is rooted in findings from social science, i.e., it provides automated trust management that mimics trusting behaviors in the society, bringing trust computation for the digital world closer to the evaluation of trust in the real world.
- Unlike other trust models in the literature, the proposed model accounts for different types of trust. Specifically, it distinguishes trusting belief in integrity from that in competence.
- The model takes into account the subjectivity of trust ratings by different entities, and introduces a mechanism to eliminate the impact of subjectivity in reputation aggregation.

VI. MODULE

Data Owner:

Register with cloud server and login(username must be unique). Send request to Private key generator to generate IBE Key on the user name. Browse file and request Private key to encrypt the data, Upload data to cloud service provider. Verify the data from the cloud.

Public Key Generator:

Receive request from the users to generate the key, Store all keys based on the user names. Check the username and provide the private key. Revoke the end user (File Receiver if they try to hack file in the cloud server and un revoke the user after updating the private key for the corresponding file based on the user).

Auditor :

Receive all files from the data owner and store all files. Check the data integrity in the cloud and inform to end user about the data integrity. Send request to PKG to Update the private key of the user based on the date parameter (Give some date to update Private Key). List all files, List all updated Private Key details based on the date and users, List all File attackers and File Receive Attackers.

End User :

In this module receiver first has to Register and login, Request secret key, Request available files in the cloud and receive files.

VII. ALGORITHM

Encryption:

Encryption means convert plain text into cipher text. AES algorithm for encryptions as follows.

Input:

Encryption object as follows,

1. Encrytedstring ->NULL
2. Secret key->key

Literal type as follows,
Byte plaintext, encrypted Text

Output:

1. START
2. Init -> (ENCRYPT MODE, key)
3. Plaintext --> UNICODE FORMAT/input
4. EncryptedText - do Final (plaintext)
5. EncryptedString -> Base64.encodeBase64 (encrypted Text)
6. Return encrypted String.

Decryption:

Decryptions are used to decrypt the message. Convert the cipher text into plain text

Input:

Decryption object as follows,
Decrypted String -> NULL
Secret Key -> key

Literal type as follows,
Byte cipher text, decrypted Text

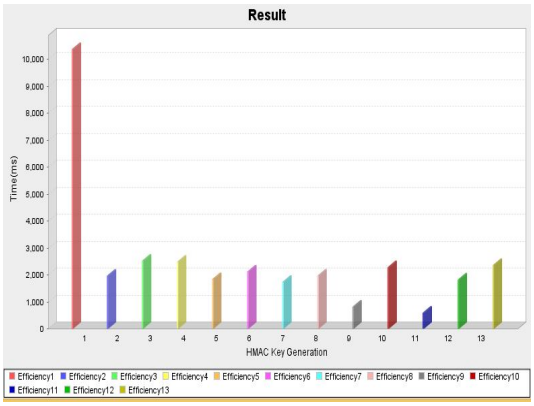
Output:

1. START
2. Init - (DECRYPT MODE, key)
3. Ciphertext - UNICODE FORMAT /input
4. DecryptedText - do Final(cipher text)
5. DecryptedString - Base64.encodeBase64 (decrypted Text)
6. Return decrypted String.

VIII. RESULT ANALYSIS

Discounted cumulative gain (DCG) is a measure of Efficiency Quality of trustee User. In information retrieval, it is often used to measure effectiveness of algorithms or related applications. Using a graded relevance scale of documents in a search engine result set, DCG measures the usefulness, or gain, of a document based on its position in the result list. The gain is accumulated from the top of the result list to the bottom with the gain of each result discounted at lower efficiency of file upload.

fig: DCG of proposed VS existing system



Two assumptions are made in using DCG and its related measures.

1) Highly trustee User on Product
2) HMAC Generation efficiency
3) Verification Efficiency count .

DCG originates from an earlier, more primitive, measure called Cumulative Gain.

Cumulative Gain:-

Cumulative Gain(CG) is the predecessor of DCG and does not include the position of a result in the consideration of the usefulness of a result set. In this way, it is the sum of the graded relevance values of all results in a Revocation result list.

Discounted Cumulative Gain:-

The Premise of DCG is that highly Revocation appearing lower in a result list should be penalized as the graded relevance value is reduced logarithmically proportional to the position of the result.

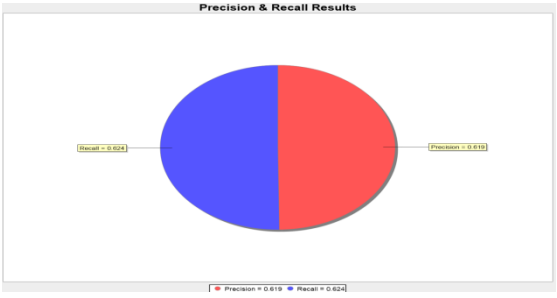


Fig: Precision & Recall Chart

Above diagram show how much range come too precision & Recall

Summary :-

In this chapter we discussed about result comparison with previous algorithms and how our algorithm is better than previous one is defined with the help of graph.

IX. CONCLUSION

To Presented a trust label system, its technical realization and the operationalisation of the complete system. The system was designed for communicating trustworthiness to Cloud consumers.

REFERENCES

[1] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing - the business perspective," Decision Support Systems, vol. 51, no. 1, pp. 176 – 189, 2011.

[2] European Commission, "Potential and impacts of cloud computing services and social network websites," 2014, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/EN.pdf

[3] Bradshaw, David, et al., "Quantitative estimates of the demand for cloud computing in europe and the likely barriers to uptake," 2012,SMART2011/0045.

[4] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," Internet Computing, IEEE, vol. 14, no. 5, pp. 14–22, Sept 2010.

[5] T. Lynn, L. van der Werff, G. Hunt, and P. Healy, "A delphi approach to the development of a cloud trust label," Journal of Computer Information Systems, vol. in press, 2015.

[6] M. Sollner, P. Pavlou, and J. M.Leimeister, "Understanding trust in ¨ it artifacts a new conceptual approach," in Academy of Management Annual Meeting, Orlando, Florida,USA,2013.

[7] P. A. Pavlou and A. Dimoka, "The nature and role of feedback text comments in online marketplaces: Implications for trust building, price premiums, and seller differentiation," Journal of Information System Research, vol. 17, no. 4, pp. 392–414, Dec. 2006.

[8] W. Wang and I. Benbasat, "Attributions of trust in decision support technologies: A study of recommendation agents for e-commerce," Journal of Management Information System, vol. 24, no. 4, pp.249–273,April2008.

[9] N. G. Carr, "The end of corporate computing," MIT Sloan Management Review, vol. 46, no. 3, pp.67–73,2005.

[10] P. A. Pavlou, "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model," International Journal of Electronic Commerce, vol. 7, no. 3, pp. 101–134,Apr.2003.

[11] A. Beldad, M. de Jong, and M. Steehouder, "How shall i trust the faceless and the intangible? a literature review on the antecedents on municipal websites," Government Information Quarterly, vol. 27, no. 3, pp. 238–244, 2010.