MONITORING AND DETECTING ABNORMAL BEHAVIOUR IN MOBILE CLOUD INFRASTRUCTURE

[1]HATTARKI.POOJA, [2]SHRUTI.Y.H

Department of Computer Science,
Appa Institute of Engineering and Technology Gulbarga,
Karnataka, India

***ABSTRACT*: Mobile devices with cloud based service are highly effective and they are very flexible and adaptable. Mobile cloud infrastructure is a new concept where mobile devices and cloud services are clubbed together. As it a commodity, service providers should know the security issues. In this paper various security threats are widely discussed based on situation. A new methodology is proposed in order to detect the abnormal behavior. By detect the host and the communication channel certain malicious programs are injected in the test bed in order to identify the abnormal behavior. Using machine learning algorithm, these suspicious programs are detected. To find the next neighboring node and to detect the fault, FDMC algorithm is implemented.**

***Keywords*: Fault Detection, Virtual Mobile Instances Signature based**

INTRODUCTION

Different mobile services are provided as application to electronic gadgets like smart phones, tables and cloud based mobile services benefit users by providing enormous flexibility and wealthy communication. Data can be retrieved, processed and send at any time using mobile devices. Flexibility is there when mobile devices are accessed using cloud computing. Each virtual instance is denoted by a mobile device and users can connect and make use of it. Virtualization in mobile devices in cloud platform provides virtual instances to the mobile users. Virtual cloud infrastructure gives the virtual mobile instances. These instances are managed using extensive power and storage capacity. Virtual smartphone over IP is a classic example of virtual mobile instances. The threatening thing for the service provider is the security.

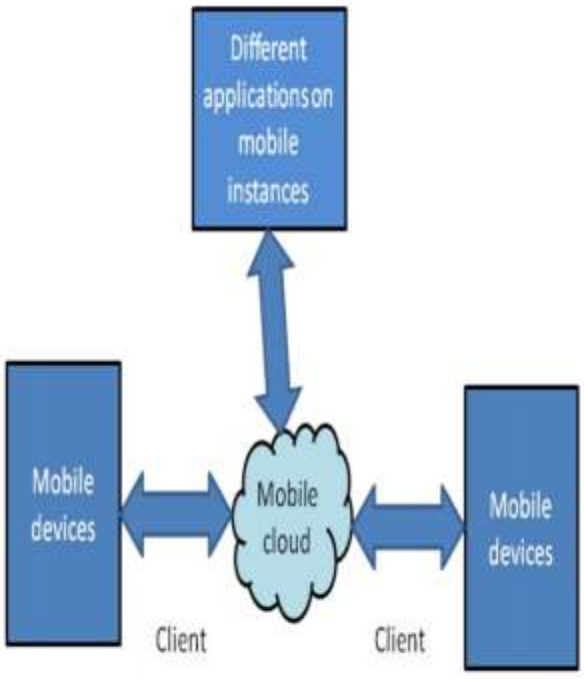

Fig 1: Mobile instances vs. mobile cloud

PROBLEM DEFINITION

User can specify the type of data wanted to file in the link. These filed files will be stored in the specified location. While data sharing if there is any break occurs in the data, normally user wants to start from the beginning; this problem is rectified through this work. If there is any break occurs, if the user initiates again then data sharing starts from the break point. This will reduce the time of creating new data, this work is more focused on fully security because there is chance of hacking data from anonymous

user, in this case the user needs to share data he/she has to be a registered user of this site than the data sharing process is fully secured using the concept of Nymble server, which is the use of computing resources that are delivered as a service over a network.

OBJECTIVE AND SCOPE

The aim of this Nymble server is to Block Misbehaving Users In Anonymous Networks Using Nymble System and Anonymizing networks route traffic through independent nodes in separate administrative domains

Nymble is the proposed system in which the servers can "blacklist" misbehaving users, thereby blocking users without compromising their anonymity. The system detects the misbehaving users and adds them to the blacklist. Thus the server can blacklist the misbehaving users without knowledge of their IP address and allows behaving users to connect anonymously. Those of the users in the blacklist are blocked from accessing the resources for a specified time that is set by the administrators. The proposed system has several important properties which overcomes the drawbacks of the existing system. The properties are anonymous authentication, backward un-linkability, subjective blacklisting, fast authentication speeds, blacklist sharing, rate limited anonymous connections, revocation auditability and also addresses Sybil attacks.

SYSTEM ANALYSIS

INTRODUCTION

During this phase, the analysis has several sub-phases. The first is requirements determination. In this sub-phase, analysts work with users to determine the expectations of users from the proposed system. This sub-phase usually involves a careful study of current systems, manual or computerized that might be replaced or enhanced as part of this work. Next, the requirements are studied and structured in accordance with their inter-relationships and eliminate any redundancies. Third, alternative initial design is generated to match the requirements. Then, these alternatives are compared to determine which alternative best meets the requirement in terms of cost and labor to commit to development process.

EXISTING SYSTEM

Present system is manual. The Project Metrics has to enter all the details of project, documents, and tasks. It also maintains the team information and also efforts estimation. For this purpose the organization maintain the size of the document, source code and update the information about team member's details manually. Which is much of time consuming process and more importantly it is error prone. Limitations of the Manual system

- **Drawbacks of Existing System**

The maintenance of various records and procedure of reporting are being done manually by the department. This leads to many drawbacks some of which are:

1. It leads to error prone results
2. It lacks of data security
3. Retrieval of data takes lot of time
4. Percentage of accuracy is less
5. Reports take time to produce

PROPOSED SYSTEM

After understanding the existing system and understanding the need for developing a new system different people involved in the related activities have been consulted. The data needed for the study has been collected from company records.

The computerization of this system would avoid the wrong interpretation and bad calculation of data .The system help the user to see any documents, source code, tasks, activities, team information with details at the click of a button. The record data is maintained and backed up such a way that data is not loss. The speed of the system could also increase.

ADVANTAGES OF THE PROPOSED SYSTEM

The proposed system will aim to automate all the activities and eliminates all the drawback of that the existing system of manual operations faces. The important features of functionality of the proposed system are listed below:

1. To generate the quick reports
2. To make accuracy and efficient calculations
3. To provide proper information briefly
4. To provide data security
5. To provide huge maintenance of records
6. Flexibility of transactions can be completed in time

DATA FLOW DIAGRAM

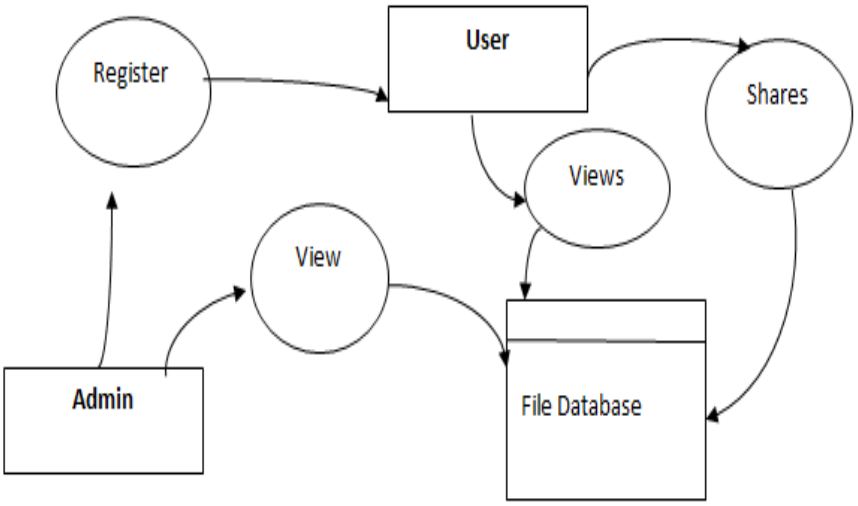

Fig:-Data Flow Diagram

CONCLUSION

We have proposed a comprehensive credential system called Nymble, which can be used to add a layer of accountability to any publicly known anonymizing network. Servers can blacklist misbehaving users while maintaining their privacy and it is seen how these properties can be attained in a way that is practical, efficient, and sensitive to needs of both users and services. Hope that this proposed work will increase the mainstream acceptance of anonymizing networks such as Tor, which has thus far been completely blocked by several services because of users who abuse their anonymity.

We presented Nymble, a system in which servers can "blacklist" misbehaving users, thereby blocking users without compromising their anonymity. Our system is thus agnostic to different servers' definitions of misbehavior—servers can blacklist users for whatever reason, and the privacy of blacklisted users is maintained

REFERENCES

[1] Ateniese.G, J. Camenisch, M. Joye, and G. Tsudik, "A Practical and Provably Secure Coalition-Resistant Group Signature, Scheme," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 255-270, 2000.

[2] Bresson.E and Stern.J, "Efficient Revocation in Group Signatures," Proc. Conf. Public Key Cryptography, Springer, pp. 190-206, (2001).

[3] Camenisch.J and Lysyanskaya.A, "An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 93-118, (2001).

[4] Camenisch.J and Lysyanskaya.A, "Dynamic Accumulators and Application to Efficient Revocation of AnonymousCredentials," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 61-76, (2002).

[5] Chaum.B, "Showing Credentials without Identification Transfeering Signatures between Unconditionally Unlinkable Pseudonyms," Proc. Int'l Conf. Cryptology (AUSCRYPT), Springer, pp. 246-264, 1990.

[6] Dingledine.R, N. Mathewson, and P. Syverson, "Tor: The Second- Generation Onion Router," Proc. Usenix Security Symp., pp. 303- 320, Aug. 2004.

[7] Damgard.I, "Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 328- 335, (1988).

[8] Douceur .J.R, "The Sybil Attack," Proc. Int'l Workshop on Peer-to- Peer Systems (IPTPS), Springer, pp. 251-260, 2002.

[9] Johnson.P.C and Kapadia.A, P.P. Tsang, and S.W. Smith, "Nymble: Anonymous IP-Address Blocking," Proc. Conf. Privacy Enhancing Technologies, Springer, pp. 113-133, (2007).

[10] Lysyanskaya.A, Rivest.R.L, Sahai.A and Wolf.S, "Pseudonym Systems," Proc. Conf. Selected Areas in Cryptography, Springer, pp. 184-199, (1999). Micali.S, "NOVOMODO: Scalable Certificate Validation and Simplified PKI Management," Proc. First Ann. PKI [11] Patrick P. Tsang, Apu Kapadia, Member, IEEE, Cory Cornelius, and Sean W. Smith "Nymble: Blocking Misbehaving Users in Anonymizing Networks" (2011).