IJCSE International Journal of Computer Science and Engineering Open Access
Research Paper Volume-2, Issue-3 E-ISSN: 2347-2693

Empirical Auditing for Computing in Preserving Manner

R. Krishna Prakash[1*] and B.Sivananthan[2]

[1*]*Dept. of Computer Science & Engineering, Gnanamani College of Engineering, Namakkal, India, rkrishprak@gmail.com*
[2]*Dept. of Computer Science & Engineering, Gnanamani College of Engineering, Namakkal, India,sivananthan.b@gmail.com*

www.ijcaonline.org

Received: 2 March 2014 Revised: 12 March 2014 Accepted: 22 March 2014 Published: 30 March 2014

Abstract — Cloud server technology is widely used nowadays for huge and secure Data Storage. However a recent study in wireless devices noticed that usage of data traffic is immense in size. It is found that application does not follow the power distribution law with the observations made in popular Social networking & Map navigation applications. Most traffic is due to extraneous data like presence information from GPS, Availability at instantaneous rate will overload the traffic. The transmitted data will have replicate values and it is almost useless to transfer the data repeatedly. This paper proposes the Intellectual Dynamic Audit Service (IDAS) is a superset of Third Party Auditor (TPA), which will instantly help to reduce the notification of traffic data in the client device itself without disturbing the Quality of service (QOS). QOS level is well maintained by usage of Firewall Anomaly Management Environment (FAME) normally used in the verification of packets send from the application to server. Pre-audit for cloud storage is activated for traffic data reduction. Hence the originality of data to be transferred can be checked easily using snapshot created by IDAS.

Keywords—Cloud Computing, Distributed Server, Data Storage, Presence Services, Cost Effective, Mobile Computing

1. INTRODUCTION

Internet chat communication using social network application on wireless devices has seen enormous growth over the last several years. A social networking service is a platform to build social networks or social relations among people who, for example, share interests, activities, backgrounds, or real-life connections. A social network service consists of a representation of each user (often a profile), his/her social links, and a variety of additional services [7]. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social networking applications allow users to share ideas, pictures, posts, activities, events, places, and interests with people in their network [9]. Chat sessions, Users Location can either be private, where each user is invited to join the session, or public, where anyone can join the session or locate their presences.

The Global Positioning System (GPS) is a space-based satellite navigation system that provides appropriate location presence information in all weather conditions, anywhere on the earth. A GPS receiver calculates its position by precisely timing the signals sent by GPS satellites high above the Earth. Each satellite continually transmits messages that include the time the message was transmitted satellite position at time of message transmission. In typical GPS operation, four or more satellites must be visible to obtain an accurate result [3]. GPS receiver uses these signals to calculate its three-dimensional location (latitude, longitude, and altitude) [3]. A number of applications for GPS do make use of this cheap and highly accurate timing. These include transfer data, traffic signal timing, and synchronization of cell phone base station [10]. The application provides presence and event notification which make it easy to keep track of the availability of colleagues and friends ("friend" in Google Latitude). The presence service is able to indicate whether other users are online or not and if they are online, whether they are idle or busy [6].One fundamental aspect of this paradigm shifting is that data are being centralized or outsourced to the cloud server. The protocols used for locating are not standardized, many of them are proprietary, and they are even seen as a control point in this business by the companies involved.

Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes, SMS and MMS messages [7]. Smart phones may additionally contain video, email, web browsing information, location information, and social networking messages and contacts [8]. As with all networked/social applications, Google Latitude and windows location protocols have a large potential design space and uses extraneous data. This exposes some of the dimensions available to a protocol designer and how the systems chose to decide them. Where possible, we especially describe the choice affects replicated data. Like previous work, their focus was to understand the social behavior, not the traffic patterns of Social network users [5]. As of network plans has become a demand one in some country or territory area. We are fortunate to get access to instant messaging traffic from thousands of employees in a large enterprise [5]. Compared to previous studies, our workload not only covers a much larger user base but also has much higher traffic volume on particularly replication of GPS (presences information), availability data [3]. Considering the large size of the outsourced data and the

Corresponding Author: R.Krishna Prakash, rkrishprak@gmail.com

user's constrained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for the cloud users [2]. Moreover, the overhead of using cloud storage should be minimized as much as possible, such that a user does not need to perform too many operations to use the data (in additional to retrieving the data). For the reduction of workload at cloud user's side we have implemented a protocol named IDAS. Intellectual Dynamic Audit Service (IDAS) is proposed to control the user's availability notification & presences information such that traffic load & outsourced data can be reduced. Also in addition the usage of power volts can be marginally saved which can increases the battery usage of the devices.

2. TRAFFIC LOAD ANALYSIS USING IDAS

Our IDAS has three phases: initialization, audit, and transmission. To simplify our discussion, we focus on storing, auditing, and retrieving a single customer object. For each of these phases, we describe how to handle both the original value and replicate values. With a social network application the status update of users & Location, traffic load to a presence server is highly related with the behavior patterns of users. The login/logoff interval, online behavior, and the number of contacts all have impact on the traffic load to a cloud server [6]. Each outcome message to a presence server can invoke creating a transaction and the number of transactions processed or maintained by a cloud server is an important parameter that determines the IDAS's capability.

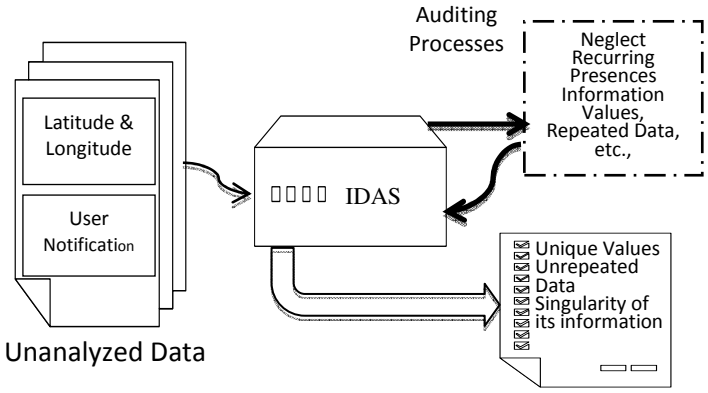

Figure 1: Overview of IDAS

2.1 Initialization: The traffic load data analysis using IDAS behavior is shown as in the Fig. 1. Interface of IDAS is not present only the protocol rules are set by customer or from the default setting. The transaction message from the IDAS are have the characteristics of Unique values (Latitude: 18.2" N, Longitude: 58.7" E), Unrepeated data (Notifications Messages/ Messages), Singularity of the all information that needs to be transferred to cloud server through Internet services provider.

2.2 Audit: In the auditing phase, the internal auditor repeatedly checks the stored data using a challenge-response protocol. Each check establishes the data's integrity immediately before the check. With minimal long-term state, an IDAS can efficiently and repeatedly check stored contents on behalf of the customer. In these audits, the service must prove that contents are completely unchanged. All our protocols do not reveal the data contents to the third party [2]. Our auditing protocols are zero-knowledge, providing no added information to the server by default.

2.3 Transmission: The IDAS allows verifying the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users. As mentioned previously the data will be replicated many times if the presences / notification data does not changes then the storage capacity is unutilized at the cloud server. The final audited data is sorted and made as a snapshot for the verification of Adversary content and unwanted coding parts. The model is unique it allows the server to access small portions of the file in generating the data; all other techniques must access the entire information. Within this model, we give the first auditing services during transaction at client devices.

The distinct features of IDAS have:

1). Predominately reduce the traffic data that needs to be transferred to server.
2). Voided the exact copy of user information.
3). Minimize the power usage and utilize it.

3. RELATED WORK

3.1 Storage-related auditing: Online Service Provider (OSP) must convince customers that their platforms are reliable. Because a customer knows that a provider's primary incentive is to make a profit, not simply to serve the customer's needs. An auditor understands the service level agreement (SLA) between a customer and a provider and quantifies the extent to which a provider might not meet the SLA [1]. The auditor has expertise and capabilities that the customer does not. Auditors understand the threats posed, know best practices, and have the resources to check for process adherence and service quality. They perform these checks through well-defined interfaces to the service. With proper safeguards, auditors can investigate providers who serve multiple customers without fear of information leakage.

3.2 Auditing in general: One of us (Mogul) previously suggested that auditing support would become necessary for IT outsourcing in general [6]. Satyanarayanan proposed dealing with a variety of ``Internet risks" by an audit-like mechanism (``inspection-enforced safety") based on periodic signed, encrypted snapshots of entire virtual machine states, which would then be inspected when necessary (e.g., during legal proceedings) [6]. Others have suggested building accountable systems that provide a non-repudiable history of

their state and actions. These audit trails are useful for detecting and pinpointing problems after the fact, and could support internal and external audits.

3.2.1 Internal vs. external auditing: We illustrate the two types of audits using an analogy to the restaurant business. A restaurant's ``SLA" is to provide its diners with enjoyable and safe meals at reasonable expense. We can audit restaurants simply by trying out the service or (using third parties) by relying on recommendations from friends or food critics [1]. This corresponds to external auditing of a service. External audits evaluate the quality of service through externally available interfaces, and usually assume that one can predict future success (``reputation") from limited samples. With this approach, we can determine whether the restaurant is enjoyable, but it might not warn us in advance if the food is sometimes contaminated.

So we also rely on health inspectors to go into the kitchen and identify procedures that might result in sick customers. This corresponds to internal auditing, which determines the extent to which a service follows best practices. Internal audits evaluate the structure and processes within a service to ensure that the service can continue to meet its objectives (SLAs). To do so, these audits need specialized interfaces that reveal and test the inner workings of a service. Other examples of internal audits include fire marshal inspections of office buildings to check electrical codes, and accounting firms checking whether corporations meet perfect standards. As with health inspections, these internal audits warn customers of practices that could lead to impending disasters. Customers can use this information to choose between services or complement one service with another.

3.3 Minimize auditing cost: Auditing imposes costs on OSPs, which should not outweigh its benefits [4].

3.4 Audit results must be trustworthy: Audits should not be biased either toward the OSP or the customer. Our auditing protocols are zero-knowledge, providing no added information to the auditor [4]. This new IDAS allows for updates, deletions, and appends to the stored file. To make storage services accountable for data loss, we present protocols that allow a third-party auditor to periodically verify the data stored by a service and assist in returning the data intact to the customer. Most importantly, in that they never reveal the data contents to the auditor. Our solution removes the burden of verification replicated data, alleviates both the customer's and storage service's fear of data leakage, and provides a method for independent arbitration of data retention contracts.

The auditor verifies the integrity of the data file and the server's possession. This scheme only works for the auditor to maintain state, and suffers from bounded usage, which potentially brings in online burden to users when the repeated values are used up. In other related work, thoroughly study set of requirements which ought to be satisfied for a remote data possession checking protocol to be of practical use. Their proposed protocol supports unlimited times of file integrity verifications and allows preset tradeoff between the protocol running time and the local storage burden at the user [1].

4. FIREWALL ANOMALY MANAGEMENT ENVIRONMENT (FAME)

A firewall policy consists of a sequence of rules that define the actions performed on packets that satisfy certain conditions. The rules are specified in the form of (condition, action). A condition in a rule is composed of a set of fields to identify a certain type of packets matched by this rule and proceed with the action according to the specified rule.

4.1 Permission Elimination: Since the IDAS works by default setting and for the user convenience purpose some settings like "Time-out, Repeat Keywords, Send more than" have the write permission by the user in ordinance with the future purposes. But this FAME tool is Read-only tool that is begin executed each the IDAS is activated to outsourced data for against the Adverse / malware addition.

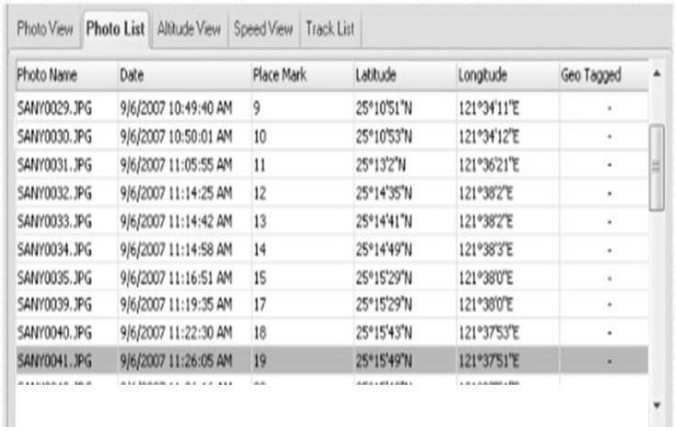

Figure 2: Model Snapshot of Data check from IDAS

4.2 Activity Procedure: Based on the audited data from Intellectual Dynamic Audit Service (IDAS) they listed as shown in figure 2. This is taken as input to the FAME in the snapshot format by hiding the text content inside the image and matching with the default rules of FAME and if it violates the rules then appropriate actions are performed according to the protocol mentioned in the application used by the user.

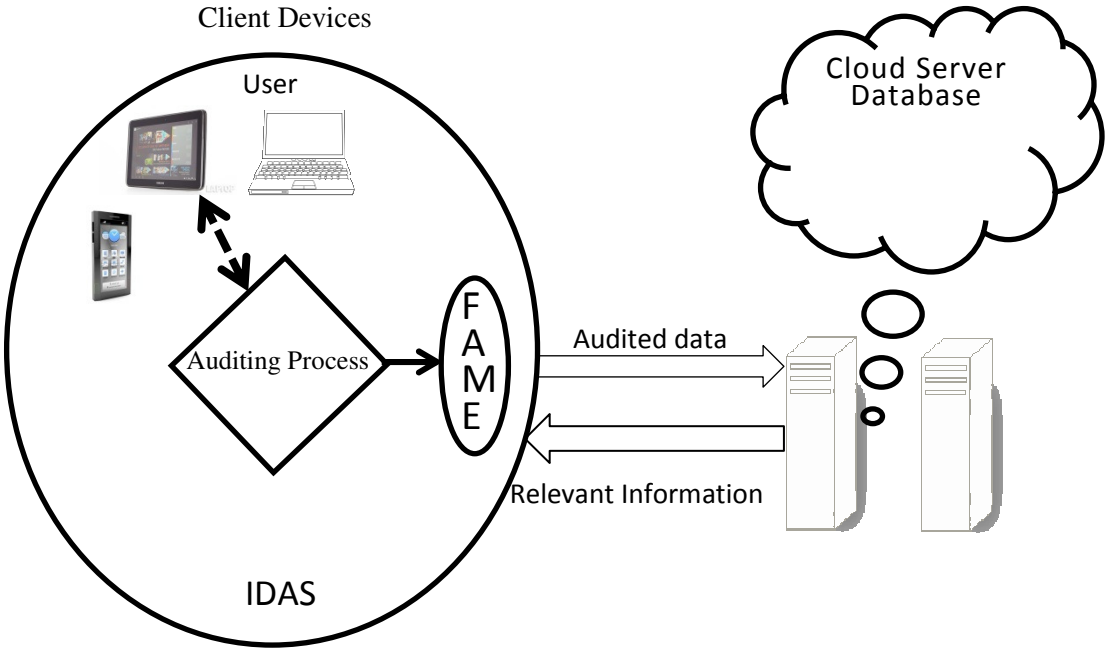

Figure 3: Workflow of Data from Client to Server through IDAS

5. TYPICAL WORKFLOW OF IDAS IN DECENTRALIZED DEVICES

The proposed Intellectual Dynamic Audit Service (IDAS) in the Decentralized device will act as auditing services for data work and it will follow to perform their actions as shown in the Fig. 3.

The Flow of data from the client devices (Mobiles, Tablets, Laptops) which are all having the Global Positioning System (GPS) Devices in inbuilt / additional one will start to send the Presence information about the Latitude & Longitude value to the cloud server for the notification of the user location based upon the preferences saved by the owner. This information and related data like user's availability about his current status then option selected by the client are all send as the transmitted message to the cloud server for storing. This data will contains replicate and sending of this information will have the loss of storing and unutilized data. Here the auditing process will follows some policy like Predominately reduce the traffic data that needs to be transferred to server, Voided the exact copy of user information, Minimize the power usage and utilize it.

We need both internal and external audits of OSPs. External audits can only confirm past behavior, so without internal audits, we could not predict upcoming problems or assess risk exposure. On the other hand, internal audits might not be exhaustive and might be based on incomplete failure models; we can use external audit results to assess whether internal audits are really working.

The following are two additional important assumptions about customers that shape our IDAS. First, customers have an incentive to claim data's to be transmitted, for instance, to receive payment for losing data as specified by the retention contract. Second, customers want to keep their data private from third parties. If the service returns the original copies, the auditor accepts and forwards the data to the IDAS and forwards enough information for the customer to efficiently compute the originality information.

After completion of auditing process the "Audited Data" is passed to cloud server by the network service provider or some means of communicating method. Since the Auditing is done at the Client device itself so the usage of data is slightly been reduce based upon the report send by GPS, Notification Status by Social network application [11]. Evaluation of data (Auditing) is done based upon the protocol set by the user and this protocols are editable by client if he needs to change the pattern of data in/out. In whole the process the privacy of data is perfectly been maintained not even a single bit of data is outsourced to the third party users in the network environment [11] .

Based on the user session id k, with h as audited data then R is the originality content with replicate values and v as temporary space for auditing & L as the audited replicated values.

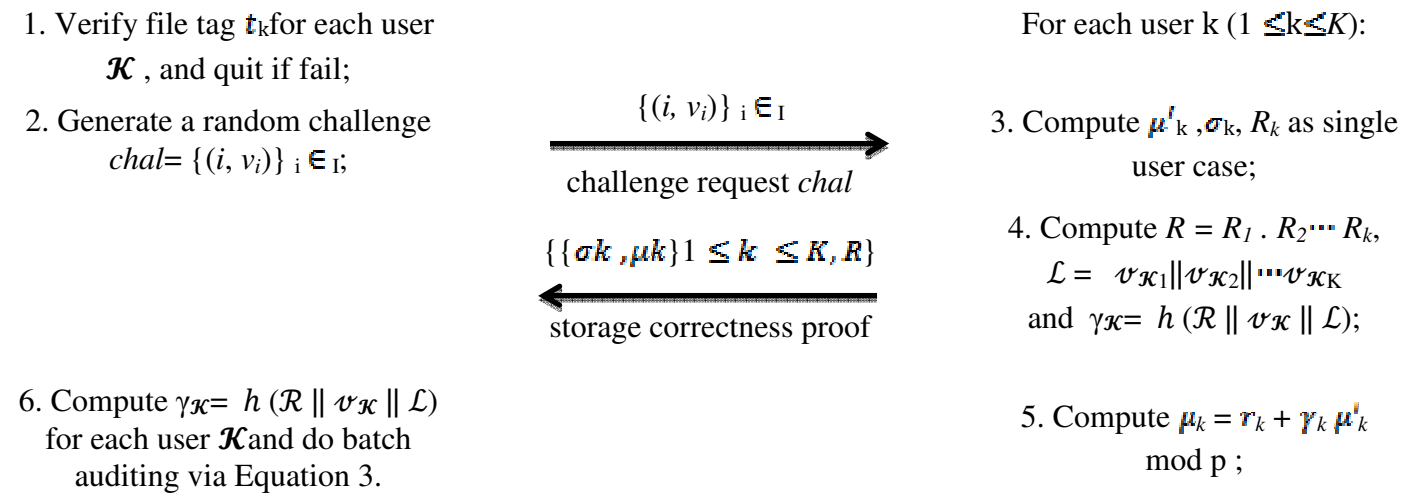

Figure 4: Evaluation of auditing data using IDAS

Fig 4. shows the operation done by Intellectual Dynamic Audit Service (IDAS) and it be can integrated into popular application like Google Latitude, Facebook, Nokia Maps, Google Maps etc., all the application the performs the GPS usage and status updates.

6. CONCLUSION

Storage space in Cloud computing is becoming more essential in the view of Cloud service provider side. So even saving a petty of data in the server will give lot of space when the space is saved in large amount. Also the Network traffic is reducing while the transmission of data is busy. For the Effective enhancement this IDAS can also be implemented in more applications like message, browsers and contacts to avoid the creation of duplicate data and to save the internal storage space even at the client side device also. More innovative techniques and solutions are to be supported in storage of data at cloud server.

REFERENCES

[1]. Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage" IEEE Transactions on Computers, Vol. 62, No. 2, Page no (362- 375), February 2013.

[2]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), Page no (598-609), November 2007.

[3]. Chi-Jen Wu, Jan-Ming Ho, and Ming-Syan Chen, "A Scalable Server Architecture for Mobile Presence Services in Social Network Applications" IEEE Transactions On Mobile Computing, Vol. 12, No. 2, Page No (386-398), Feb 2013.

[4]. M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report No. HPL-2008/186, 2008.

[5]. C. Chi, R. Hao, D. Wang, and Z.-Z. Cao, "IMS Presence Server: Traffic Analysis and Performance Modeling," Proc. IEEE International Conference on Network Protocols (ICNP), ISBN-1-4244-2507-5, 2008.

[6]. M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), Page No (1-6), 2007.

[7]. Z. Xiao, L. Guo, and J. Tracey, "Understanding Instant Messaging Traffic Characteristics," Proc. IEEE 27th International Conference on Distributed Computing Systems (ICDCS), ISBN-0-7695-2837-3, Page No (7-14) 2007.

[8]. Mobile device forensics, http://en.wikipedia.org/wiki/Mobile_device_forensics, 2013.

[9]. Social Networking, http://en.wikipedia.org/wiki/Social_networking, 2013.

[10]. Global Positioning System, http://en.wikipedia.org/wiki/Global_Positioning_System, 2013.

[11]. P. Bellavista, A. Corradi, and L. Foschini, "IMS-Based Presence Service with Enhanced Scalability and Guaranteed QoS for Interdomain Enterprise Mobility," IEEE Wireless Comm., vol. 16,no. 3, Page No (16-23), June 2009.

AUTHORS PROFILE

R.Krishna Prakash received the B.TECH degree in Information Technology from Paavai Engineering College, Affiliated to Anna University, Chennai, in 2011. He is working towards the M.E degree in Computer Science and Engineering from Gnanamani College of Engineering, Affiliated to Anna University, Chennai since September 2012. His research interests include Cloud Computing, Networking, Database management System.

B. Sivananthan received the M.E degree in Computer Science and Engineering from Gnanamani College of Technology, Affiliated to Anna University, Chennai. Received B.TECH degree in the Information Technology from Tamilnadu College of Engineering, Affiliated to Anna University, Chennai in 2008. Now working as Assistant Professor in Gnanamani College of Engineering, Affiliated to Anna University, Chennai Since June 2012. His research interest includes Cloud computing, Networking, VANET. He is a member of the ISTE.