



GNITED MINDS
Journals

*International Journal of
Information Technology
and Management*

*Vol. VI, Issue No. I,
February-2014, ISSN 2249-
4510*

**ACCESSING THE INFORMATION WITHIN THE
CLOUD IN CONJUNCTION WITH AN AUDITING
MECHANISM**

AN
INTERNATIONALLY
INDEXED PEER
REVIEWED &
REFEREED JOURNAL

Accessing the Information within the Cloud in Conjunction with an Auditing Mechanism

Kashetti Vigna¹, Bussary Pranaya², Koppula Mounika³, Karne Supriya⁴, Chandran Madan Kumar⁵

¹Student, Department of Computer Science and Engineering, Varadha Reddy College of Engineering, Warangal, India

²Student, Department of Computer Science and Engineering, Varadha Reddy College of Engineering, Warangal, India

³Student, Department of Computer Science and Engineering, Varadha Reddy college of Engineering, Warangal, India

⁴Student, Department of Computer Science and Engineering, Varadha Reddy College of Engineering, Warangal, India

⁵Assistant Professor, Department of Computer Science and Engineering, Varadha Reddy College of Engineering, Warangal, India

Abstract – Cloud computing allows extremely ascendable services to be simply consumed over the web on Associate in Nursing as-needed basis. a significant feature of the cloud services is that users' information area unit typically processed remotely in unknown machines that users don't own or operate. whereas enjoying the convenience brought by this new rising technology, users' fears of losing management of their own information (particularly, money and health data) will become a major barrier to the wide adoption of cloud services. to handle this downside, here, we tend to propose a completely unique extremely decentralized info answerability framework to stay track of the particular usage of the users' information within the cloud. Specifically, we tend to propose Associate in Nursing object-centered approach that permits envelopment our work mechanism in conjunction with users' information and policies. we tend to leverage the JAR programmable capabilities to each produce a dynamic and traveling object, and to confirm that any access to users' information can trigger authentication and automatic work native to the JARs. To strengthen user's management, we tend to additionally offer distributed auditing mechanisms. We offer intensive experimental studies that demonstrate the potency and effectiveness of the projected approaches.

Key Terms : cloud, distributed auditing, framework, Nursing

I. INTRODUCTION

CLOUD computing presents a replacement thanks to supplement this consumption and delivery model for IT services supported the web, by providing for dynamically ascendable and sometimes virtualized resources as a service over the web. To date, there are a unit variety of notable business and individual cloud computing services, together with Amazon, Google, Microsoft, Yahoo, and Sales force [19]. Details of the services provided area unit abstracted from the users United Nations agency not got to be consultants of technology infrastructure. Moreover, users might not understand the machines that really method and host their information. whereas enjoying the convenience brought by this new technology, users additionally begin worrying regarding losing management of their own information. the information processed on clouds area unit usually outsourced, resulting in variety of problems associated with

answerability, together with the handling of personally recognizable info. Such fears are getting a major barrier to the wide adoption of cloud services [30]. To allay users' considerations, it's essential to supply an efficient mechanism for users to watch the usage of their information within the cloud. for instance, users got to be able to make sure that their information area unit handled in line with the service level agreements created at the time they sign up for services within the cloud standard access management approaches developed for closed domains like databases and operating systems, or approaches employing a centralized server in distributed environments, don't seem to be appropriate, because of the subsequent options characterizing cloud environments. First, information handling are often outsourced by the direct cloud service provider (CSP) to different entities within the cloud and theses entities also can delegate the tasks to others, and so on. Second, entities area unit allowed to affix and leave the cloud

in a very versatile manner. As a result, information handling within the cloud goes through a fancy and dynamic graded service chain that doesn't exist in standard environments on top of issues, we tend to propose a completely unique approach, particularly Cloud info answerability (CIA) framework, supported the notion of data answerability [44]. in contrast to privacy protection technologies that area unit designed on the hide-it-or-lose-it perspective, info answerability focuses on keeping the information usage clear and traceable. Our projected United States intelligence agency framework provides end-to-end answerability in a very extremely distributed fashion. One amongst the most innovative options of the United States intelligence agency framework lies in its ability of maintaining light-weight and powerful answerability that mixes aspects of access management, usage management and authentication. By suggests that of the United States intelligence agency, information house owners will track not solely whether or not or not the service-level agreements area unit being honored, however additionally enforce access and usage management rules as required related to the answerability feature, we additionally develop 2 distinct modes for auditing: push mode and pull mode. The push mode refers to logs being sporadically sent to the information owner or neutral whereas the pull mode refers to an alternate approach whereby the user (or another licensed party) will retrieve the logs as required.

Currently, we tend to concentrate on image files since pictures represent a really common content kind for finish users and organizations (as is tested by the recognition of Flickr [14]) and area unit more and more hosted within the cloud as a part of the storage services offered by the utility computing paradigm featured by cloud computing. Further, pictures usually reveal social and private habits of users, or area unit used for archiving vital files from organizations. Additionally, our approach will handle personal recognizable info provided they're keep as image files (they contain a picture of any matter content, for instance, the SSN keep as a .jpg file).

We tend to test our United States intelligence agency framework in a very cloud testbed, the Emulab tested [42], with Eucalyptus as middleware [41]. Our experiments demonstrate the potency, quantifiability and coarseness of our approach. Additionally, we tend to additionally offer an in depth security analysis and discuss the dependability and strength of our design within the face of assorted nontrivial attacks, launched by malicious users or because of compromised Java Running atmosphere (JRE). In summary, our main contributions area unit as follows:

1. We propose a completely unique automatic and enforceable work mechanism within the cloud. To our data, this can be the primary time a scientific approach to information answerability through the novel usage of JAR files is projected.

2. Our projected design is platform freelance and extremely decentralized, in this it doesn't need any dedicated authentication or storage system in place.

3. We transcend ancient access management in this we offer a precise degree of usage management for the protected information once these area unit delivered to the receiver.

4. We conduct experiments on a true cloud tested. The results demonstrate the potency, quantifiability, and coarseness of our approach. we tend to additionally offer an in depth security analysis and discuss the dependability and strength of our design.

This paper is Associate in Nursing extension of our previous conference paper [40] and got created the subsequent new contributions. First, we tend to integrated integrity checks and oblivious hashing (OH) technique to our system so as to strengthen the dependability of our system just in case of compromised JRE. We additionally updated the log records structure to supply further guarantees of integrity and genuineness. Second, we tend to extend the protection analysis to hide a lot of potential attack situations. Third, we tend to report the results of recent experiments and supply a radical analysis of the system performance. Fourth, we've got other an in depth discussion on connected works to organize readers with a far better understanding of background. Finally, we've got improved the presentation by adding a lot of examples and illustration graphs. the remainder of the paper is organized as follows: Section two discusses connected work. Section three lays out our downside statement. Section four presents our projected Cloud info answerability framework, and Sections five and half dozen describe the careful algorithms for machine-controlled work mechanism and auditing approaches, severally. Section seven presents a security analysis of our framework, followed by Associate in Nursing experimental study in Section eight. Finally, Section nine concludes the paper and descriptions future analysis directions.

II. REALTED WORK

During this section, we tend to initial review connected works addressing the privacy and security problems within the cloud. Then, we tend to shortly discuss works that adopt similar techniques as our approach however serve for various functions.

2.1 Cloud Privacy and Security

Cloud computing has raised a variety of vital privacy and security problems [19], [25], [30]. Such problems area unit because of the very fact that, within the cloud, users' information and applications reside—at least for a precise quantity of time—on the cloud cluster that is closely-held and maintained by a 3rd party considerations arise since within the cloud it's

not continually clear to people why their personal info is requested or how it'll be used or passed on to different parties. To date, very little work has been wiped out this house, specifically with relevancy answerability. Pearson et al. have projected answerability mechanisms to handle privacy considerations of finish users [30] so develop a privacy manager [31]. Their basic plan is that the user's non-public information area unit sent to the cloud in Associate in Nursing encrypted kind, and therefore the process is completed on the encrypted information. The output of the process is deobfuscated by the privacy manager to reveal the proper result. However, the privacy manager provides solely restricted options in this it doesn't guarantee protection once the information area unit being disclosed. In [7], the authors gift a stratified design for addressing the end-to-end trust management and answerability downside in federate systems. The authors' focus is incredibly totally different from ours, in this they principally leverage trust relationships for answerability, at the side of authentication and anomaly detection. Further, their resolution needs third-party services to finish the observation and focuses on lower level observation of system resources.

2.2 Different connected Techniques:

With relevancy Java-based techniques for security, our strategies area unit associated with self-defending objects (SDO) [17]. Self-defending objects area unit Associate in Nursing extension of the object-oriented programming paradigm, wherever software package objects that provide sensitive functions or hold sensitive information area unit accountable for protective those functions/data. Similarly, we tend to additionally extend the ideas of object-oriented programming. The key difference in our implementations is that the authors still deem centralized information to take care of the access records, whereas the things being protected area unit control as separate files. In previous work, we tend to provide a Java-based approach to stop privacy outpouring from categorization [39], that may well be integrated with the United States intelligence agency framework projected during this work since they build upon connected architectures. In terms of authentication techniques, Appel and Felten [13] projected the Proof-Carrying authentication (PCA) framework. The PCA includes a high order logic language that permits quantification over predicates, and focuses on access management for net services whereas associated with ours to the extent that it helps maintaining safe, superior, mobile code, the PCA's goal is extremely totally different from our analysis, because it focuses on substantiating code, instead of observation content. Another work is by Mont et al. United Nations agency projected Associate in Nursing approach for powerfully coupling content with access

management, exploitation Identity-Based coding (IBE) [26]. We additionally leverage IBE techniques, however during a very totally different manner. we tend to don't deem IBE to bind the content with the foundations. Instead, we tend to use it to supply robust guarantees for the encrypted content and therefore the log files, like protection against chosen plaintext and ciphertext attacks.

Additionally, our work could look the same as works on secure information beginning [5], [6], [15], however really greatly differs from them in terms of goals, techniques, and application domains. Works on information beginning aim to ensure information integrity by securing the information beginning.

III. DOWNSIDE STATEMENT

We start this section by considering Associate in Nursing illustrative example that is the idea of our downside statement and can be used throughout the paper to demonstrate the most options of our system.

Example 1. Alice, an expert artist, plans to sell her images by exploitation the SkyHigh Cloud Services. For her business within the cloud, she has the subsequent requirements:

1. Her images area unit downloaded solely by users United Nations agency have bought her services.
2. Potential patrons area unit allowed to look at her footage initial before they create the payment to get the transfer right.
3. Due to the character of a number of her works, solely users from bound countries will read or transfer some sets of images.
4. For some of her works, users area unit allowed to solely read them for a restricted time, in order that the users cannot reproduce her work simply.
5. In case any dispute arises with a shopper, she needs to possess all the access info of that shopper.
6. She needs to confirm that the cloud service suppliers of SkyHigh don't share her information with different service suppliers, in order that the answerability provided for individual users also can be expected from the cloud service suppliers.

IV. ALGORITHMS

Pushing or actuation methods have attention-grabbing tradeoffs. The pushing strategy is helpful once there is a unit on outsized variety of accesses to the information among a brief amount of your time. during this case, if the information don't seem to be pushed out of times enough, the log file could become terribly massive, which can increase value of operations like repeating information (see Section 8). The pushing mode could also be most well-liked by information house owners United Nations agency area unit organizations and want to stay track of the information usage systematically over time. For such information house owners, receiving the logs mechanically will lighten the load of the information analyzers. the utmost size at that logs area unit pushed out could be a parameter which may be simply organized whereas making the faller part. The pull strategy is most required once the information owner suspects some misuse of his data; the pull mode permits him to watch the usage of his content at once. A hybrid strategy will really be enforced to profit of the consistent info offered by pushing mode and therefore the convenience of the pull mode. Further, as mentioned in Section seven, supporting each pushing and actuation modes helps protective from some nontrivial attacks.

V. SECURITY DISCUSSION

We tend to currently analyze potential attacks to our framework. Our analysis relies on a semi honest someone model by presumptuous that a user doesn't unarms his master keys to unauthorized parties, whereas the assaulter could attempt to learn further info from the log files. we tend to assume that attackers could have comfortable Java programming skills to break apart a JAR file and previous data of our United States intelligence agency design. we tend to initial assume that the JVM isn't corrupted, followed by a discussion on the way to make sure that this assumption holds true. The foremost intuitive attack is that the assaulter copies entire JAR files. The assaulter could assume that doing therefore permits accessing the information within the JAR file while not being detected by the information owner. However, such attacks are detected by our auditing mechanism. Recall that each JAR file is needed to send log records to the harmonizer. specifically, with the push mode, the harmonizer can send the logs to information house owners sporadically. That is, although the information owner isn't conscious of the existence of the extra copies of its JAR files, he can still be able to receive log files from all existing copies. If attackers move copies of JARs to places wherever the harmonizer cannot connect, the copies of JARs can before long become inaccessible. this can be as a result of every JAR is needed to write down redundancy info to the harmonizer sporadically. If the JAR cannot contact the harmonizer, the access to the content within the JAR are disabled. Thus, the faller part provides a lot of transparency than standard log files encryption; it permits the information owner to observe once

Associate in Nursing assaulter has created copies of a JAR, and it makes offline files un-come-at-able. Another potential attack is to break apart the JAR file of the faller so arrange to extract helpful info out of it or spoil the log records in it. Given the benefit of disassembling JAR files, this attack poses one amongst the foremost serious threats to our design. Since we tend to cannot forestall Associate in Nursing assaulter to realize possession of the JARs, we tend to deem the strength of the cryptographical schemes applied to preserve the integrity and confidentiality of the logs.

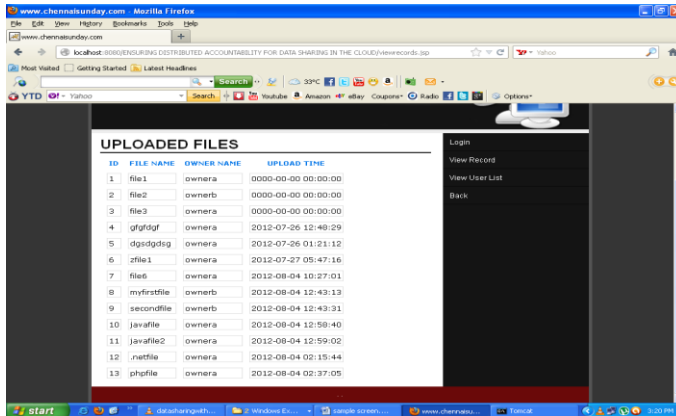
Once the JAR files area unit disassembled, the assaulter is in possession of the general public IBE key used for encrypting the log files, the encrypted log file itself, and the *.class files. Therefore, the assaulter should deem learning the non-public key or subverting the coding to browse the log records.

ID	FILE NAME	OWNER NAME	UPLOAD TIME	COST	Refund and Cost	Click Here
1	file1	ownera	2000-00-00 00:00:00	\$300	\$150	Download
2	file2	ownerb	2000-00-00 00:00:00	\$500	\$250	Download
3	file3	ownera	2000-00-00 00:00:00	\$1000	\$500	Download
4	gfgtqfz	ownera	2012-07-26 12:48:29	\$800	\$400	Download
5	dqsdqsdq	ownera	2012-07-26 11:01:13	\$680	\$340	Download
6	zfile1	ownera	2012-07-27 00:47:18	\$500	\$250	Download
7	file6	ownera	2012-08-04 19:27:01	\$500	\$250	Download
8	myfirstfile	ownerb	2012-08-04 12:43:11	\$1000	\$500	Download
9	secondfile	ownerb	2012-08-04 12:43:31	\$600	\$300	Download
10	janafie	ownera	2012-08-04 12:58:40	\$60	\$30	Download
11	janafie2	ownera	2012-08-04 12:59:00	\$80	\$40	Download
12	netfile	ownera	2012-08-04 02:15:44	\$650	\$325	Download
13	phpfie	ownera	2012-08-04 03:27:05	\$900	\$450	Download

To compromise the confidentiality of the log files, the assaulter could attempt to establish that encrypted log records correspond to his actions by mounting a selected plaintext attack to get some pairs of encrypted log records and plain texts. However, the adoption of the Weil Pairing algorithmic program ensures that the United States intelligence agency framework has each chosen ciphertext security and chosen plaintext security within the random oracle model [4]. Therefore, the assaulter won't be able to decode any information or log files within the disassembled JAR file. although the assaulter is a licensed user, he will solely access the particular content file however he's ineffective to decode the other information together with the log files that area unit visible solely to the information owner.¹ From the disassembled JAR files, the attackers don't seem to be able to directly read the access management policies either, since the first ASCII text file isn't enclosed within the JAR files. If the assaulter needs to infer access management policies, the sole potential manner is thru analyzing the log file. This is, however, terribly arduous to accomplish since, as mentioned earlier, log records area unit encrypted and breaking the coding is computationally arduous.

Also, the assaulter cannot modify the log files extracted from a disassembled JAR. Would the

assaulter erase or tamper a record, the integrity checks other to every record of the log won't match at the time of verification (see Section five.2 for the record structure and hash chain), revealing the error. Similarly, attackers won't be able to write faux records to log files while not going undiscovered, since they're going to got to sign with a legitimate key and therefore the chain of hashes won't match. The Reed-Solomon cryptography accustomed produce the redundancy for the log files, the log harmonizer will simply observe a corrupted record or log file.



The screenshot shows a web browser displaying a page titled 'UPLOADED FILES'. It contains a table with columns: ID, FILE NAME, OWNER NAME, and UPLOAD TIME. The table lists 13 files. To the right of the table is a sidebar with 'Login' and 'View Record' links. The browser's address bar shows 'localhost:8080/VIEWING-DISTRIBUTED-ACCOUNTABILITY-FOR-DATA-SHARING-IN-THE-CLOUD/ViewRecords.jsp'.

ID	FILE NAME	OWNER NAME	UPLOAD TIME
1	file1	ownera	0000-00-00 00:00:00
2	file2	ownerb	0000-00-00 00:00:00
3	file3	ownera	0000-00-00 00:00:00
4	gfgdgdg	ownera	2012-07-26 12:48:29
5	dgedgdsg	ownera	2012-07-26 01:21:12
6	zfile1	ownera	2012-07-27 05:47:16
7	file6	ownera	2012-08-04 10:27:01
8	myfirstfile	ownerb	2012-08-04 12:43:13
9	secondfile	ownerb	2012-08-04 12:43:31
10	javafile	ownera	2012-08-04 12:58:40
11	javafile2	ownera	2012-08-04 12:59:02
12	.natfile	ownera	2012-08-04 02:15:44
13	phfile	ownera	2012-08-04 02:37:05

Finally, the assaulter could attempt to modify the Java class loader within the JARs so as to subvert the category files after there area unit being loaded. This attack is prevented by the protection techniques offered by Java. protection ensures that each one packages among the JAR file return from constant ASCII text file [27]. protection is one amongst the Java properties, that permits making a signature that doesn't enable the code within the JAR file to be modified. a lot of significantly, this attack is stopped because the JARs check the class loader every time before granting any access right. If the class loader is found to be a custom class loader, the JARs can throw Associate in Nursing exception and halt. Further, JAR files area unit signed for integrity at the time of creation, to avoid that Associate in Nursing assaulter writes to the JAR. Although Associate in Nursing assaulter will browse from it by disassembling it—he cannot “reassemble” it with changed packages. Just in case the assaulter guesses or learns the information owner's key from somewhere, the entire JAR files exploitation constant key are compromised. Thus, exploitation totally different IBE key pairs for various JAR files are safer and stop such attack.

VI. CONCLUSION

We tend to project innovative approaches for mechanically work Associate in Nursing access to the information within the cloud in conjunction with an auditing mechanism. Our approach permits the information owner to not solely audit his content

however additionally enforces robust back-end protection if required. Moreover, one amongst the most options of our work is that it allows {the information|the info|the information} owner to audit even those copies of its data that were created while not his data. Within the future, we tend to conceive to refine our approach to verify the integrity of the JRE and therefore the authentication of JARs [23]. For instance, we are going to investigate whether or not it's potential to leverage the notion of a secure JVM [18] being developed by IBM. This analysis is aimed toward providing software package tamper resistance to Java applications. Within the long run, we tend to conceive to style a comprehensive and a lot of generic object-oriented approach to facilitate autonomous protection of traveling content. We would like to support a spread of security policies, like categorization policies for text files, usage management for executables, and generic answerability and beginning controls.

VII. REFERENCES:

- [1] P. Ammann and S. Jajodia, “Distributed Timestamp Generation in platelike Lattice Networks,” *ACM Trans. portable computer Systems*, vol. 11, pp. 205-225, Aug. 1993.
- [2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable info Possession at Untrusted Stores,” *Proc. ACM Conf. portable computer and Comm. Security*, pp. 598-609, 2007.
- [3] E. Barka and A. Lakas, “Integrating Usage management with SIP-Based Communications,” *J. portable computer Systems, Networks, and Comm.*, vol. 2008, pp. 1-8, 2008.
- [4] D. Boneh and M.K. Franklin, “Identity-Based secret writing from the Weil Pairing,” *Proc. Int'l science Conf. Advances in science*, pp. 213-229, 2001.
- [5] R. Bose and J. Frew, “Lineage Retrieval for Scientific info Processing: A Survey,” *ACM Computing Surveys*, vol. 37, pp. 1- 28, Mar. 2005.
- [6] P. Buneman, A. Chapman, and J. Cheney, “Provenance Management in Curated Databases,” *Proc. ACM SIGMOD Int'l Conf. Management of data (SIGMOD '06)*, pp. 539-550, 2006.
- [7] B. Chun and A.C. Bavier, “Decentralized Trust Management and answerability in federate Systems,” *Proc. Ann. Hawaii Int'l Conf. System Sciences (HICSS)*, 2004.

- [8] OASIS Security Services Technical Committee, "Security Assertion nomenclature (saml) a try of.0," http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security, 2012.
- [9] R. Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu, "A Logic for Auditing responsibility in localized Systems," Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.
- [10] B. Crispo and G. Ruffo, "Reasoning regarding responsibility within Delegation," Proc. Third Int'l Conf. information and Comm. Security (ICICS), pp. 251-260, 2001.
- [11] Y. Chen et al., "Oblivious Hashing: A skulking package Integrity Verification Primitive," Proc. Int'l Workshop information concealment, F. Petitcolas, ed., pp. 400-414, 2003.
- [12] S. Etalle and W.H. Winsborough, "A Posteriori Compliance management," SACMAT '07: Proc. twelfth ACM Symp. Access management Models and Technologies, pp. 11-20, 2007.
- [13] X. Feng, Z. Ni, Z. Shao, and Y. Guo, "An Open Framework for Foundational Proof-Carrying Code," Proc. ACM SIGPLAN Int'l Workshop varieties in Languages vogue and Implementation, pp. 67-78, 2007.
- [14] Flickr, <http://www.flickr.com/>, 2012.
- [15] R. Hasan, R. Sion, and M. Winslett, "The Case of the fake Picasso: Preventing History Forgery with Secure supply," Proc. Seventh Conf. File and Storage Technologies, pp. 1-14, 2009.
- [16] J. Hightower and G. Borriello, "Location Systems for ubiquitous Computing," Computer, vol. 34, no. 8, pp. 57-66, Aug. 2001.
- [17] J.W. Holford, W.J. Caelli, and A.W. Rhodes, "Using Self- defensive Objects to Develop Security Aware Applications in Java," Proc. twenty seventh terra firma Conf. technology, vol. 26, pp. 341-349, 2004.
- [18] Reliable Java Virtual Machine IBM, <http://www.almaden.ibm.com/cs/projects/jvm/>, 2012.
- [19] P.T. Jaeger, J. Lin, and J.M. Grimes, "Cloud Computing and data Policy: Computing in Associate in Nursing extremely Policy Cloud?," J. information Technology and Politics, vol. 5, no. 3, pp. 269-283, 2009.
- [20] R. Jagadeesan, A. Jeffrey, C. Pitcher, and J. Riely, "Towards a Theory of responsibility and Audit," Proc. fourteenth European Conf. Research in computer Security (ESORICS), pp. 152-167, 2009.
- [21] R. Kailar, "Accountability in Electronic Commerce Protocols," IEEE Trans. code Eng., vol. 22, no. 5, pp. 313-328, May 1996.
- [22] W. Lee, A. Cinzia Squicciarini, and E. Bertino, "The vogue and analysis of accountable Grid automatic data processing system," Proc. twenty ninth IEEE Int'l Conf. Distributed Computing Systems (ICDCS '09), pp. 145-154, 2009.
- [23] J.H. Lin, R.L. Geiger, R.R. Smith, A.W. Chan, and S. Wanchoo, technique for Authenticating a Java Archive (jar) for transferrable Devices, US Patent six,766,353, July 2004.
- [24] F. Martinelli and P. Mori, "On Usage management for Grid Systems," Future Generation computer Systems, vol. 26, no. 7, pp. 1032-1042, 2010.
- [25] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: Associate in Nursing Enterprise Perspective on Risks and Compliance (Theory in Practice), first ed. O' Reilly, 2009.
- [26] M.C. Mont, S. Pearson, and P. Bramhall, "Towards accountable Management of Identity and Privacy: Sticky Policies and enforceable Tracing Services," Proc. Int'l Workshop data and sure-handed Systems Applications (DEXA), pp. 377-382, 2003.
- [27] S. Oaks, Java Security. O'Really, 2001.
- [28] J. Park and R. Sandhu, "Towards Usage management Models: on the way aspect ancient Access management," SACMAT '02: Proc. Seventh ACM Symp. Access management Models and Technologies, pp. 57-64, 2002.