Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 01, January-2025

Secure Group File Sharing in Cloud Computing Environment

Mohana Santhiya R ,
Assistant Professor of Dept. Computer Science and Engineering and Cyber Security,
Sree Sakthi Engineering College,
Coimbatore, India.

Vinothini S , Pavithra R, Swetha S
Assistant Professor of Dept. Computer Science and Engineering,
Sree Sakthi Engineering College,
Coimbatore, India.

***ABSTRACT* - People store their data on cloud storage very commonly now every day. Security may be a major issue in storing data on clouds. Cryptography techniques are very useful to impose security on data. A hybrid cryptography system is proposed to provide better security on the information which is stored on cloud storage. The proposed approach uses RSA algorithm and DES algorithm and supply a hybrid of the two algorithms to supply more security on the information before storing it on cloud. The proposed algorithm is implemented in JAVA and test on a sample plain text. The project are going to be very useful for IOT applications storing data on cloud. It is verified that the proposed algorithm is functioning well to provide more security on data.**

I. INTRODUCTION

The term “cloud computing” could be a recent buzzwordin the IT world. Behind this fancy poetic phrase there lies a real picture of the longer term of computing for both in technical perspective and social perspective. Though the term “Cloud Computing” isrecent but the thought of centralizing computation and storage in distributed data centers maintained bythird party companies isn’t new but it came in way back in 1990s together with distributed computing approaches like grid computing. Cloud computing is geared toward providing IT as a service to the cloud users on-demand basis with greater flexibility, availability, reliability and scalability with utility computing model.

The origin of cloud computing are often seen as an evolution of grid computing technologies. The term Cloud computing was given prominence first byGoogle’s CEO Eric Schmidt in late 2006. So the birth of cloud computing is incredibly recent phenomena although its root belongs to some old ideas with new business, technical and social perspectives. From the architectural point of view cloud is naturally devolve on an existing grid based architecture and uses the grid services and adds some technologies like virtualization and a few business models. In short cloud is actually a bunch of commodity computers networked together in same or different geographical locations, operating together to serve variety of consumers Cloud Computing provides us a method by which we can access the applications as utilities, over the Internet. It allows us to make, configure, and customize applications online. The term Cloud refers to a Network or Internet. Cloud Computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage,infrastructure and application. Cloud can provide services over network, i.e., on public networks or on private networks, i.e.,WAN, LAN or VPN.Applications like e-mail , web conferencing, customer relationship management.

II. LITERATURE REVIEW

2.1 Towards Trusted Cloud Computing[13]

Nuno Santos, Krishna P. Gummadi and Rodrigo Rodrigues propose Cloud computing infrastructures enable companies to chop costs by outsourcing computations on-demand. However, clients of cloud computing services currently have no means of verifying the confidentiality and integrity of their data and computation. To address this problem to propose the planning of a trusted cloud computing platform (TCCP). TCCP enables Infrastructure as a Service (IaaS) providers like Amazon EC2 to supply a closed box execution environment that guarantees confidential execution of guest virtual machine Trusted cloud computing platform (TCCP) for ensuring the confidentiality with different need and workload on demand basis with the assistance of virtualization. and integrity of computations that are outsourced to IaaS services. The TCCP provides the abstraction of a closed box execution environment for a customer’s VM, guaranteeing that no cloud provider’s privileged administrator can inspect or tamper with its content. Moreover, before requesting the service to launch a VM, the TCCP allows a customer to reliably and remotely determine whether the service backend is running a trusted TCCP implementation. This capability extends the notion of attestation to the whole service, and thus allows a customer to verify if its computation will run securely. within the proposed system, show a way to leverage the advances of trusted compute.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 01, January-2025

2.2 Seeding Clouds with Trust Anchors[15]

Joshua Schiffman and his co-authors proposes the paper for the shoppers security critical processing needs are starting to push back strongly against using cloud computing. Cloud vendors run their computations upon cloud provided VM systems,but customers are worried such host systems might not be ready to protect themselves from attack, ensure isolation of customer processing, or load customer processing correctly. To provide assurance of information processing protection in clouds to customers, user advocate methods to boost cloud transparency using hardware-based attestation mechanisms.

The centralized management of cloud data centers is right for attestation frameworks, enabling the development of a practical approach for customers to trust within the cloud platform. Specifically, propose a cloud verifier service that generates integrity proofs for patrons to verify the integrity and access control enforcement abilities of the cloud platform that protect the integrity of customer's application VMs in IaaS clouds. While a cloud-wide verifier service could present a major system bottleneck, demonstrate that aggregating proofs enables significant overheadreductions. As a result, transparency of knowledge security protection will be verified at cloud-scale.The main three challenges has been discussed are that cloud providers face when generating proofs that may placate a user's concerns: First that cloud vendors provide a symbol of information security protection of their hosts and customer processing; Second proofs have a clear desiring to cloud customers; and Third proofs may be generated effectively and efficiently in a cloud computing environment.

2.3 Domain Based Storage Protection with Secure Access Control for the Cloud[9]
Nicolae Paladi, Antonis Michalas and Christian Gehrmann proposes cloud computing has evolved from a promising concept to one of the fastest growing segments of the IT industry. However, many businesses and individuals still view cloud computing as a technology that risks exposing their data to unauthorized users. To introduce an confidentiality and integrity protection mechanism for Infrastructure as a Service (IaaS) clouds, which relies on trusted computing principles to supply transparent storage isolation between IaaS clients. The system also address the absence of reliable data sharing mechanisms, by providing an XML-based language framework which enables clients of IaaS clouds to securely share data and clearly denies access rights granted to peers. The proposed improvements are prototyped as a code extension for a well-liked cloud platform. Full-disk encryption has emerged as a primary solid solution for data confidentiality protection and is additionally mentioned in as an answer to the "dirty disks" problem. However, fulldisk encryption creates hurdles for data sharing, widely recognized as an necessary feature for cloud applications. Despite the range of accessible open source cloud management platforms (e.g OpenStack, Eucalyptus, Open Nebula), allocation of read-write permissions for shared data between collaborating tenants still remains an open problem. The system improve and extend previous work by adding capabilities to both grant access to data to other IaaS cloud clients and assign access permissions.

2.4 Security Aspects of e-Health Systems Migration to the Cloud[7]
Antonis Michalas et al proposed As adoption of e- health solutions advances, new computing paradigms like cloud computing bring the potential to enhance efficiency in managing medical health records and help reduce costs. However, these opportunities introduce new security risks which can't be ignored. supported our experience with deploying a part of the Swedish electronic health records management system in an infrastructure cloud, we make an summary of major requirements that must be considered when migrating e-health systems to the cloud. Furthermore,comprehensive a replacement attack vector inherent to cloud deployments and present a unique data confidentiality and integrity protection mechanism for infrastructure clouds. This contribution aims to encourage exchange of best practices and lessons learned in migrating public e-health systems to the cloud.
Visions of an electronic healthcare system are more than twenty years old. Researchers aimed for a paperless medical system where patients and doctors are ready to book appointments via the Internet, create electronic prescriptions and store their anamnesis in a very central database, easily accessible from anyone with appropriate access rights. During these years, there has been a gentle increase in research focus and funding reaching to modernize existing healthcare systems and supply reliable and value effective e-health services. Both private organizations, like Microsoft, Google and IBM, and public administration bodies have taken steps towards e-health.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 01, January-2025

2.5 Securely Launching Virtual Machines on Trustworthy Platforms in a Public Cloud[1]
Mudassar Aslam et al proposed the Infrastructure-as-a-Service (IaaS) cloud model which allows cloud users to run their own virtual machines (VMs) on available cloud computing resources. IaaS gives enterprises the likelihood to outsource their process workloads with minimal effort and expense. However, one major problem with existing approaches of cloud leasing, is that the users can only get contractual guarantees regarding the integrity of the offered platforms. The actual fact that the IaaS user himself or herself cannot verify the provider promised cloud platform integrity, is a security risk which threatens to stop the IaaS business in normally. The author address this issue and propose a completely unique secure VM launch protocol using Trusted Computing techniques. VM launch protocol allows the cloud IaaS users to securely bind the VM to a trusted computer configuration such that the clear text VM only will run on a platform that has been booted into a trustworthy state. The aptitude builds user confidence and can serve as a vital enabler for creating trust in public clouds. To judge the feasibility of our proposed protocol via a full scale system implementation and perform a system security analysis. IaaS gives enterprises the likelihood tooutsource their process workloads with minimal effort. A little company without security skills or an ordinary IT service consumer might trust a public cloud service provider and in some cases prefer cloud services over self-hosted services with a belief that his or her cloud provider can give better security by recruiting specialized staff and equipment. In contrast, most large or medium size enterprises have higher security requirements for their own or their business users sensitive data; and if their data is compromised thanks to a security breach in the cloud provider network, it'll leads to serious legal and business setbacks. Therefore, these enterprises are reluctant to host their services in a public cloud unless they get trusted ways to validate the contractual security guarantees provided by the cloud provider. The main target of our work is to introduce technical ways to verify the protection guarantees provided by the cloud service provider. To achieve this by allowing the cloud user to cryptographically bind the user virtual machine (VM) to a trustworthy state of the provisioned cloud platform. Furthermore, to make sure that the whole launch process meets all expected major security requirements of a top quality public service with respect to authentication and secure transfer. According to suggested VM launch protocol, a particular VM isn't even sent to the provider network if no platform with the expected security guarantees may be offered by the IaaS cloud.

III. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

In Existing system, a knowledge Sharing system model, there are multiple user security who may encrypt according to their own ways, possibly using different sets of cryptographic keys. Letting each user obtain keys from every owner who's Their central idea talks about the impossibility of Fully Homomorphic Encryption (FHE) alone for VM Cloud privacy. Their classification hierarchy of VM Cloud Computing isn't standard model and has few shortcomings as we might discuss duly. The system states the protection and privacy issues from a standard VM Cloud Computing definitions and discuss the challenges involved not only for FHE but also for several other techniques, but this needs too much trust on one authority (i.e., cause the key escrow problem).
Elliptical Curve Cryptography is an arrangement during which the keys needed to decrypt encrypted data are held in ECC in order that, under certain circumstances, a certified third party may gain access to those keys. These third parties may include businesses, who might want access to employees' private communications, or governments, who might need to be able to view the contents of encrypted communications.

3.1.1 Drawbacks of Existing System

- Key information depends on centralized key server.
- Computational and Communication cost is more.
- More resources used for rekeying because it is being done for individual join/leave operation.
- High in Memory usage and encryption key length.
- Data Transmission time and execution is high.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 01, January-2025

3.2 PROPOSED SYSTEM

Implementation of RSA with the DES provides the better result with better accuracy. Proposed System endeavor to study the patient centric, solves the problem of evaluating a function jointly by multiple parties on their private inputs secure sharing of file sharing in VM Cloud stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. It also no assumptions are made on computational resources available with the parties. All the parties would carryout same amount of work which is contrary to VM Cloud Computing setting. Proposed System endeavor to study the patient centric, solves the problem of evaluating a function jointly by multiple parties on their private inputs secure sharing of file sharing in VM Cloud stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. It also no assumptions are made on computational resources available with the parties. All the parties would carryout same amount of work which is contrary to VM Cloud Computing setting. To adapt these techniques for an asymmetric setting like VM Cloud Computing where the server has massive amounts of computing power relative to the users, In order to protect the personal health data stored on a semi-trusted server, we adopt **Diffie Hellman** is better than **ECC** as the main encryption primitive. Precise lower bounds on hard computations, but complexity theorists have had limited success in establishing lower bounds in general, so instead we reason relatively: we show that the hard computations are at least as hard as solving some problem known or assumed (usually the latter, for reasons to be explained in due course) to be hard.

The proof technique for making assertions about the complexity of one problem on the basis of another is called reduction “Using DH, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her file sharing among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved

3.2.1 Advantages of Proposed System

- Key information does should be depend on VM Cloud centralized key server.
- Computational and Communication cost is less.
- Resources used for rekeying is minimized because it is being done for batch of join/leave operations.
- More secure by Boolean logic minimization because session management done by this concept.
- Low Memory Usage.
- High Throughput.

3.3 Diffie-Hellman Key Exchange algorithm.

Diffie-Hellman key exchange offers the best of both worlds -- it uses public key techniques to allow the exchange of a private encryption key. Let's take a look at how the protocol works, from the perspective of Alice and Bob, two users who wish to establish secure communications. We can assume that Alice and Bob know nothing about each other but are in contact.

Here are the nine steps of the process:

- Communicating in the clear, Alice and Bob agree on two large positive integers, n and g, with the stipulation that n is a prime number and g is a generator of$n$.
- Alice randomly chooses another large positive integer, X_A, which is smaller than n. X_A will serve as Alice's private key.
- Bob similarly chooses his own private key, X_B.
- Alice computes her public key, Y_A, using the formula $Y_A = (g^{\wedge}X_A) \bmod n$.
- Bob similarly computes his public key, Y_B, using the formula $Y_B = (g^{\wedge}X_B) \bmod n$.
- Alice and Bob exchange public keys over the insecure circuit.
- Alice computes the shared secret key, k, using the formula $k = (Y_B {\wedge}X_A) \bmod n$.
- Bob computes the same shared secret key, k, using the formula $k = (Y_A {\wedge}X_B) \bmod n$.
- Alice and Bob communicate using the symmetric algorithm of their choice and the shared secret key, k, which was never transmitted over the insecure circuit.

IV. SYSTEM MODEL

The efficient providing user security guarantees in public infrastructure cloud provides to mainly focus as following modules,

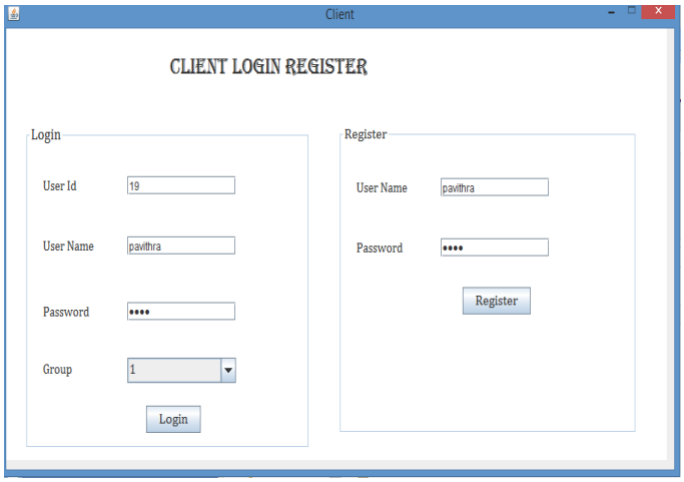
- Registeration and Encryption
- Database Storage
- Group Key Generation within the workgroup
- Keying and Rekeying the group key
- Sharing the data within workgroup

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 01, January-2025

4.1 Registeration and Encryption

The client module the client program was implemented using Java servlets and a JFrame page that invokes the servlet. The user enters the data to be sent via the JFrame page which then invokes the Client servlet. The servlet then encrypts this data using the shared key object generated by the Diffie- Hellman Key Agreement algorithm and the Data Encryption Standard (in ENCRYPT mode) and send it over to the server. The client served uses URL Redirection to send the en



. **Figure 4.1.1 Login**

Figure 4.1.2 Encrypted Text

4.2 Database Storage

The server itself is a simple servlet that is connected to a database. It receives the encrypted message from the client and decrypts it using the shared key object generated by the Diffie-Hellman algorithm and Diffie Hellman (in DECRYPT mode).

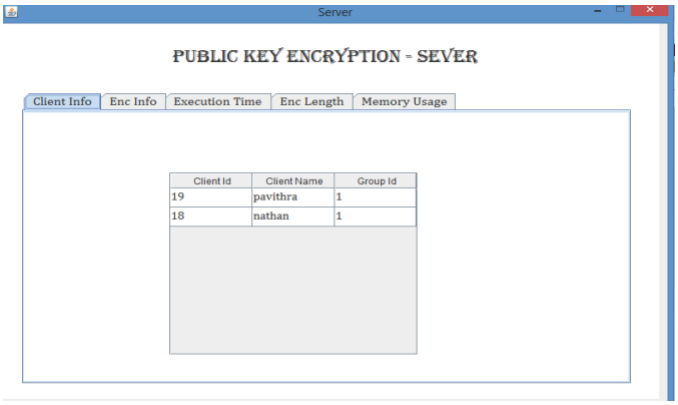


Figure 4.2.1 Client Information

Once the message has been ecrypted the server will store the message into the database, which can be retrieved at a later stage.

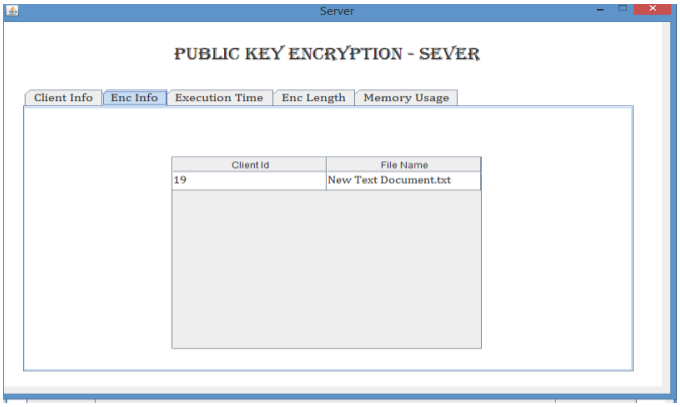


Figure 4.2.2 Encrypted file information

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 01, January-2025

4.3 Group Key Generation within the workgroup

The nodes in the workgroup will form a group key. Each group member will collaboratively contribute its part to the global group key. The group key is generated in a shared and contributory fashion and there is no single-point-of-failure. we are going to generate a group key. The group members are arranged in a logical key hierarchy known as a key tree. In the distributed key agreement protocols we consider, however, there is no centralized key server available. Moreover, an advantage of distributed protocols over the centralized protocols is the increase in system reliability, because the group key is generated in a shared and contributory fashion and here is no single-point-of-failure. To efficiently maintain the group key in a dynamic peer group with more than two members, we use the tree-based group Elliptic Curve Diffie Hellman protocol. Each member maintains a set of keys, which are arranged in a hierarchical binary tree. Each leaf node in the tree corresponds to the individual secret and blinded keys of a group member Mi. Therefore, the secret key held by the root node is shared by all the members and is regarded as the group key.Key tree used in the tree- based group Elliptic Curve Diffie Hellman protocol.

Figure 4.3.1 Key Generation

4.4 Keying and Rekeying the group key Rekeying the group key which resources renewing the keys connected with the nodes of the key tree, this is execute whenever the is any group membership modify including any batch of constituent joins the group.Rekeying means a new collection key will be create by members in the group.Rekeying is also carry out whenever there is any group membership change counting any batch of existing members departure the group.We find that the preceding move toward perform all rekeying steps at the opening of every rekeying time.This results in high processing load during the update occurrence and in that way delays the start of the secure group message.

4.5 Sharing data within the workgroup

With the help of group key generated by the members in the group, the data will be shared securely among the group. The group members will share the resources, namely accessing the files. We are implementing this with RMI (Remote Method Invocation). This feature aids in building distributed applications.

Figure 4.5.1 File Sharing

A remote object is one whose methods can be invoked from another Java virtual machine, potentially on a different host. An object of this type is described by one or more remote interfaces written in the Java programming language. A reference to a remote object can be passed as an argument or returned as a result in any method invocation.

Figure 4.5.2 View File

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 01, January-2025

V. RESULTS AND DISCUSSIONS

This section engages in a simulation to evaluate the proposed algorithm. The experiments have been conducted on the platform of personal computer with 1.5 GHz CPU and 1GB RAM. The operating system is Windows 7, and simulation programs are implemented in Java with Net beans 8.0. The main purpose of our study is to determine whether there is any gap between cryptographic protocol/scheme engineering implementation. Our scheme will be integrated with the security factors with respect to the fact that solving the proposed method is very challenging, and that the shared key is never itself transmitted over the channel. Our Algorithm utilizes basic scientific ideas making execution simpler and in addition avoidance from common Attacks. Security change is useful in light of the fact that proposed Algorithm is the premise of a few security standards and services on the internet..

VI. CONCLUSION

The Cloud computing as a technology would be adopted if the areas of concerns like security of the data will be covered with full proof mechanism. The strength of cloud computing is the ability to manage risks in particular to security issues. Our suggested model will present an outline sketch of architecture to be adopted by architects involved in implementing the cloud computing. Security algorithms mentioned for encryption and decryption and ways proposed to access the multimedia content can be implemented in future to enhance security framework over the network.

The proposed system explore our work by providing algorithm implementations and producing results to justify our concepts of security for cloud computing. In order for this approach to work as intended, the cloud service provider must co- operate with the user in implementing solution. Some cloud service providers base their business models on the sale of user data to advertisers. These providers probably would not be willing to allow the user to use their applications in a way that preserves user privacy.

VII. REFERENCES

[1] M. Aslam, C. Gehrmann, L. Rasmusson, and M. Bj ¨orkman,(2012), "Securely launching virtual machines on trustworthy platforms in a public cloud - an enterprise's perspective.," in CLOSER, pp. 511– 521, SciTePress,.

[2] B. Blanchet,(2001), "An efficient cryptographic protocol verifier based on prolog rules," in Computer Security Foundations Workshop, IEEE, pp. 0082–0082, IEEE Computer Society.

[3] D. Dolev and A. C. Yao,(1983), "On the security of public key protocols," Information Theory, IEEE Transactions on, vol. 29, no. 2.

[4] S. Graf, P. Lang, S. A. Hohenadel, and M. Waldvogel,(2012) "Versatile key management for secure cloud storage," Reliable Distributed Systems, IEEE Computer Society, pp. 469– 474.

[5] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh, (2003),"Terra: A virtual machine- based platform for trusted computing," in ACM SIGOPS Operating Systems Review, vol. 37, ACM.

[6] S. Kamara and C. Papamanthou,(2013), "Parallel and dynamic searchable symmetric encryption," in Financial Cryptography and Data Security, pp. 258–274, Springer.

[7] Michalas, N. Paladi, and C. Gehrmann,(2014), "Security aspects of e-health systems migration to the cloud," in E-health Networking, Application & Services (Healthcom' 14), pp. 228–232, IEEE.

[8] N. Paladi, C. Gehrmann, M. Aslam, and F. Morenius, (2013), "Trusted Launch of Virtual Machine Instances in Public IaaS Environments," in Information Security and Cryptology (ICISC'12), vol. 7839 of Lecture Notes in Computer Science, pp. 309–323, Springer.

[9] N. Paladi, C. Gehrmann, and F. Morenius,(2013),"Domain-Based Storage Protection (DBSP) in Public Infrastructure Clouds," in Secure IT Systems, pp. 279–296, Springer.

[10] N. Paladi, A. Michalas, and C. Gehrmann,(2014), "Domain based storage protection with secure access control for the cloud," in Cloud Computing, ASIACCS '14, (New York, NY, USA), ACM.

[11] A.R. Sadeghi and C. St ´ uble,(2004) "Property-based attestation for computing platforms: Caring about properties, not mechanisms," New Security Paradigms, NSPW '04, (New York, NY, USA), pp. 67–77, ACM,.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 01, January-2025

[12] Sahai(2007), “Ciphertext-policy attribute- based encryption,” on Security and Privacy, . A. Sahai and B. Waters,(2005), “Fuzzy identity-based encryption,” in Advances in Cryptology–EUROCRYPT, Springer,.

[13] N. Santos, K. P. Gummadi, and R. Rodrigues,(2009), “Towards trusted cloud computing,”in Cloud Computing, HotCloud’09, (Berkeley, CA, USA), USENIX Association.

[14] N. Santos, R. Rodrigues, K. P. Gummadi, and S. Saroiu,(2012), “Policy-Sealed Data: A New Abstraction for Building Trusted Cloud Services,” in Presented as part of the 21st USENIX Security Symposium (USENIX Security 12), (Bellevue, WA), pp. 175–188, USENIX.

[15] J. Schiffman, T. Moyer, H. Vijayakumar, T. Jaeger, and P. McDaniel, (2010), “Seeding Clouds With Trust Anchors,” in Cloud Computing Security, CCSW ’10, (New York, NY, USA), pp. 43–46, ACM.

[16] Seshadri, M. Luk, N. Qu, and A. Perrig,(2007), “SecVisor: A tiny hypervisor to provide lifetime kernel code integrity for commodity OSes,” ACM SIGOPS Operating Systems Review, vol. 41, no. 6.