IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 11, November 2017

A Robust Mechanism for Enhancing Privacy Preserving Security in Public Cloud Data Protection

Syed Suhaila[1]

Assistant Professor, Department of Computer Science Engineering, Alagappa Chettiar Government College of Engineering and Technology, Karaikudi, India[1]

Abstract: Cloud computing represents a transformative paradigm in the realm of computing, facilitating flexible, on-demand, and cost-effective access to computing resources. However, this model involves outsourcing data to cloud servers, which raises significant privacy concerns. Numerous strategies utilizing attribute-based encryption have been developed to enhance the security of cloud storage. Nonetheless, the majority of existing research primarily concentrates on the privacy of data contents and access control, while insufficient emphasis is placed on privilege control and identity privacy. In this paper, we introduce a semi-anonymous privilege control scheme, termed AnonyControl, which aims to safeguard not only data privacy but also user identity privacy within current access control frameworks. AnonyControl mitigates identity leakage by decentralizing the central authority, thereby achieving a level of semianonymity. Furthermore, it expands the concept of file access control to encompass privilege control, allowing for meticulous management of all operational privileges concerning cloud data. Additionally, we present AnonyControl-F, which effectively eliminates identity leakage and ensures complete anonymity. Our security analysis confirms that both AnonyControl and AnonyControl-F maintain security under the decisional bilinear Diffie–Hellman assumption, while our performance evaluation demonstrates the practicality of our proposed schemes.

Keywords: Cloud Computing, privacy, encryption, access control.

I. INTRODUCTION

Cloud computing represents a modern computing paradigm in which a vast array of systems is interconnected through private or public networks, facilitating a dynamically scalable infrastructure for the storage of applications, data, and files. The emergence of this technology has significantly lowered the costs associated with computation, application hosting, and content storage and delivery. It offers a pragmatic solution for realizing direct cost savings and has the capacity to transform a data center from a capital-intensive model to one characterized by variable pricing. The core principle underlying cloud computing is the "reusability of IT capabilities." Unlike traditional concepts such as "grid computing," "distributed computing," "utility computing," or "autonomic computing," cloud computing expands possibilities beyond organizational boundaries. Forrester characterizes cloud computing as "a pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end customer applications and billed by consumption." Essentially, cloud computing leverages the internet and centralized remote servers to manage data and applications [1].

Cloud service providers categorize their offerings into three primary types. 1. Software as a Service (SaaS): This model delivers a fully functional application to customers on a demand basis. A single instance of the application operates in the cloud, serving multiple end users simultaneously. Customers benefit from not having to invest in servers or software licenses upfront, while providers reduce costs by hosting and maintaining only one application. Prominent SaaS providers include Google, Salesforce, Microsoft, and Zoho. 2. Platform as a Service (PaaS): In this model, a software layer or development environment is provided as a service, enabling the creation of additional services. Customers can develop their own applications that operate on the provider's infrastructure. To ensure manageability and scalability, PaaS providers offer a specific combination of operating systems and application servers, such as the LAMP stack (Linux, Apache, MySQL, and PHP), restricted J2EE, and Ruby. Notable examples of PaaS include Google's App Engine and Force.com. Infrastructure as a Service (IaaS): IaaS delivers fundamental storage and computing resources as standardized services over the internet. It pools servers, storage systems, networking equipment, and data center space to manage workloads effectively. Customers typically install their own software on this infrastructure. Common IaaS providers include Amazon, GoGrid, and 3 Tera [2].

Organizations have the option to implement applications on Public, Private, or Hybrid cloud infrastructures. Cloud Integrators play a crucial role in guiding each organization toward the most suitable cloud solution.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 11, November 2017

Public Cloud: Public clouds are managed by third-party providers and offer significant economies of scale, as the costs associated with infrastructure are distributed among a diverse user base. This results in an appealing low-cost, "Pay-as-you-go" pricing structure for individual clients. All users share the same infrastructure, which comes with limited customization, security measures, and variations in availability, all of which are overseen by the cloud provider. A notable benefit of public clouds is their potential size, which allows for seamless scaling as needed. Private Cloud: Private clouds are designed specifically for a single organization, addressing data security concerns and providing enhanced control that is often absent in public cloud environments. There are two types of private clouds: On-premise Private Cloud: Also referred to as internal clouds, on-premise private clouds are hosted within the organization's own data centre. This model offers a more standardized approach and enhanced protection, although it may be limited in terms of size and scalability. IT departments must also bear the capital and operational expenses associated with the physical resources. This option is ideal for applications that necessitate complete control and customization of infrastructure and security. Externally hosted Private Cloud: This variant of private cloud is hosted by a third-party cloud provider, which creates a dedicated cloud environment that ensures privacy. This option is preferable for organizations that are hesitant to utilize public clouds due to concerns about resource sharing. Hybrid Cloud: Hybrid clouds integrate both public and private cloud models. By employing third-party cloud providers either fully or partially, hybrid clouds enhance computing flexibility. The hybrid cloud environment [3].

II. RELATED WORK

Regular removal of unnecessary files is essential for ensuring the security and privacy of cloud files. To address this issue, Ateniese et al. introduced a novel framework for MONA that automatically eliminates unwanted files once the sharing period defined by the data owner has elapsed, thereby enhancing the system's performance in terms of both security and efficiency. Meenakshi introduced a visual cryptography scheme, a cryptographic method that enables the encryption of visual information including printed text, handwritten notes, and images in a manner that allows decryption through the human visual system without requiring computer assistance. The effectiveness of visual cryptography schemes is influenced by several factors, including pixel expansion, contrast, security, accuracy, computational complexity, the meaningfulness of generated shares, the type of secret images (whether binary or color), and the number of secret images (either single or multiple) that the scheme encrypts. This paper aims to examine and analyze the performance of visual cryptography schemes based on pixel expansion, the number of secret images, image format, and the type of shares produced. The primary challenge associated with data sharing in the cloud pertains to privacy and security concerns. Numerous strategies exist to enhance user privacy and facilitate secure data sharing [4].

Droste et al. proposed a framework to address secure data sharing, which includes methods such as forward security for data sharing, secure data sharing for dynamic groups, attribute-based data sharing, encrypted data sharing, and a Shared Authority Based Privacy-Preserving Authentication Protocol for managing access control of outsourced data. Cloud data sharing is a method that enables users to easily access information stored in the cloud. Data owners choose to outsource their data to the cloud primarily for cost savings and the numerous advantages offered by cloud services. However, this arrangement limits the data owner's control over their information, as the cloud service provider acts as a third-party entity. Jadav provided a comprehensive analysis of cryptographic methods aimed at ensuring secure and efficient data sharing within cloud storage environments. Cloud computing enables both individuals and organizations to utilize applications without the need for installation, allowing access to personal files from any internet-enabled device. The key aggregate cryptosystem designed for cloud data sharing features an efficient public key encryption scheme that facilitates flexible delegation, permitting any subset of the ciphertexts to be decrypted using a fixed-size decryption key [5].

While cloud computing enhances the appeal of various advantages, it simultaneously introduces new and significant security threats to users' outsourced data. The separation of cloud service providers (CSP) as independent administrative entities means that users effectively relinquish ultimate control over their data. Consequently, the integrity of data stored in the cloud is jeopardized for several reasons. Firstly, despite the superior power and reliability of cloud infrastructures compared to personal computing devices, they remain vulnerable to a wide array of internal and external threats that can compromise data integrity. Instances of outages and security breaches among prominent cloud services are not uncommon. Secondly, there are various incentives for CSPs to act unethically regarding the status of users' outsourced data. For instance, CSPs may reclaim storage for financial reasons by deleting data that is infrequently accessed or may conceal incidents of data loss to protect their reputation. In summary, while outsourcing data to the cloud presents an economically attractive option for long-term, large-scale storage, it does not inherently guarantee data integrity and availability. If this issue is not adequately addressed, it could hinder the success of cloud architecture. As users no longer have physical possession of their data storage, traditional cryptographic methods for data security cannot be directly applied. Specifically, the approach of downloading all data for integrity verification is impractical due to the high costs associated with I/O and network transmission. Furthermore, merely detecting data corruption upon access is often inadequate, as it fails to provide assurance of correctness for data that has not been accessed and may be too late to recover any lost or damaged data [6].

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 11, November 2017

III. PROPOSED METHOD

The proposed system architecture is displayed in Figure 1. It consists of five modules: Cloud framework creation, Key generation, Secure data storage, Data sharing and Evaluation criteria.

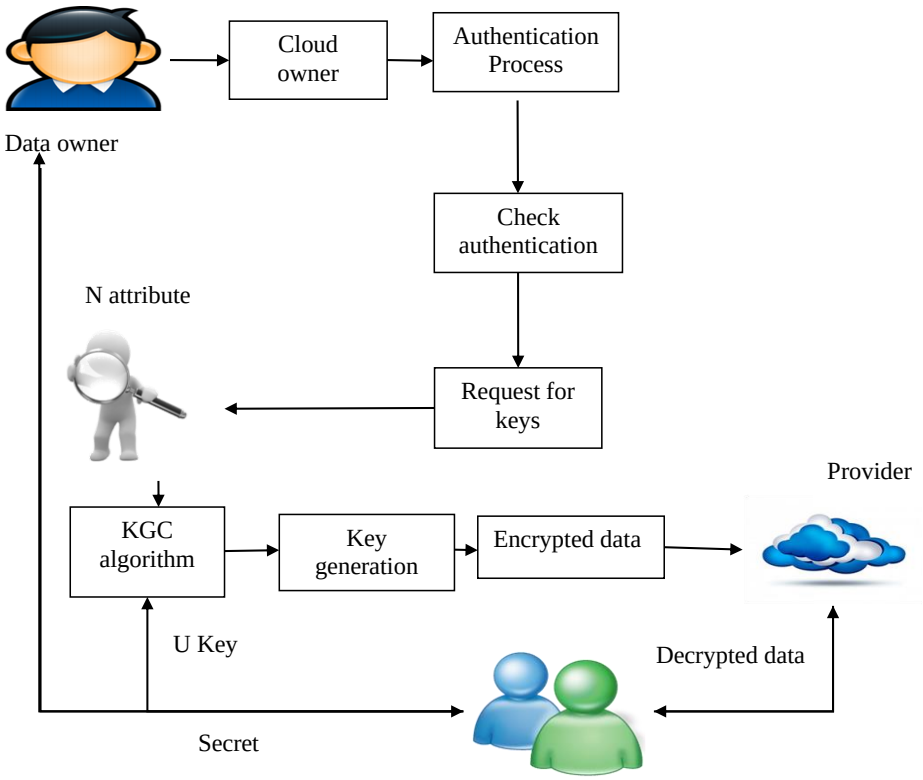

Fig 1: Proposed System Architecture

Cloud framework creation:
This module discusses the cloud data storage service, which involves three distinct entities: the cloud user, who possesses a substantial volume of data files requiring storage in the cloud; the cloud server, overseen by the cloud service provider, which offers data storage services and is equipped with considerable storage capacity and computational resources; and the third-party auditor, who possesses specialized knowledge and skills that the cloud users may lack, and is entrusted to evaluate the reliability of the cloud storage service on behalf of the user when requested.

Key Generation system:
A protocol for remote data integrity checking that ensures privacy preservation, accommodates data dynamics, and allows for public verifiability utilizes a Remote Data Integrity Checking Protocol. This protocol enables public verifiability independently, without the involvement of a third-party auditor.

Secure cloud storage:
In this module, the Security and Efficiency Manager (SEM) verifies the integrity of data storage to ensure that no fraudulent cloud server can successfully pass the SEM's audit without genuinely preserving users' data. This process guarantees that the Third-Party Auditor (TPA) cannot extract users' data content from the information gathered during the auditing procedure. Additionally, a batch auditing scheme is implemented to equip the SEM with a secure and efficient auditing capability, allowing it to handle multiple auditing requests from a potentially large number of different users simultaneously. The auditor oversees the interactions between the data owner and the cloud service provider, receiving the metadata of the data components, the tag generation key, and a random challenge from the data owner. Upon making a request to the cloud server, the auditor retrieves the metadata of the data components and, prior to processing the request, verifies authentication and cross-checks it with the metadata received from the data owner. The data owner stores the data on cloud servers, where the data is fragmented and encrypted. The data owner can access the information whenever necessary from the cloud server. The auditor can access the information for auditing purposes, provided they are authenticated, and submits the access request to the data owner as needed.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 11, November 2017

Data sharing:
In this module, users can access the file by decrypting it with any of the content utilized for its encryption as a keyword. This allows them to decrypt the data and gain access to it. Users can also decrypt files stored in the cloud using ranking scores and indexing methods. Additionally, they can examine indexing terms to retrieve the most relevant documents based on similarity metrics.

Evaluation criteria:
This module focuses on assessing performance, facilitating scalable and efficient privacy-preserving public storage auditing in the cloud. Our approach specifically enables batch auditing, allowing multiple delegated auditing tasks from various users to be conducted simultaneously while maintaining privacy. Additionally, it includes a mechanism for duplicate checks upon receiving requests for duplicate data from users. We introduce a privacy-preserving public auditing framework aimed at enhancing data storage security within Cloud Computing. Security in cloud computing is a critical concern that warrants attention. By utilizing a Key Generation Centre (KGC), we can ensure the accuracy and integrity of data stored in the cloud. Our system employs a public key-based protocol with batch auditing capabilities to uphold data security while preserving privacy. This instils confidence in clients regarding the cloud storage services provided, as the Third-Party Auditor (TPA) acts on behalf of the data owner. The system's performance is further enhanced through the use of a Glassfish server, known for its user-friendly management and superior processing power. The attacking module implemented is designed to identify altered data in the cloud during storage or updates. It has been observed that batch auditing significantly reduces the KGC computation costs by 20% compared to individual auditing.

IV. RESULTS AND DISCUSSION

The results of the proposed are presented in this section. The web development sector has recently experienced significant growth. As the Internet and technology continue to thrive, web development has emerged as a highly sought-after field. However, this industry is also marked by intense competition, with numerous skilled professionals proficient in programming. Consequently, mastering effective PHP development techniques is essential. For those with a background in programming languages and coding, PHP should feel intuitive. Its versatility allows for both basic and highly sophisticated programming, enhancing its appeal to developers. Before embarking on website creation, it is crucial to determine the programming language that will be employed to achieve a professional appearance [7-9]. PHP stands out as one of the most user-friendly programming languages, compatible with various operating systems. Its cost-free nature is a significant advantage. PHP proves invaluable for tasks such as managing database connections, formatting dates, editing strings, and handling emails. Additionally, it can be easily extended to incorporate specific functionalities desired for your website. The reliability of PHP is exceptional, as it operates on millions of servers globally, making it robust enough to handle even the most demanding applications. This language offers web developers greater freedom in crafting websites, equipped with remarkable features and the ability to utilize common elements effectively. PHP is particularly effective for developing dynamic websites. Programmers using PHP benefit from open-source code, allowing for the flexibility to edit, modify, and update the source code as needed [10-12].

Fig 2: Owner details

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 11, November 2017

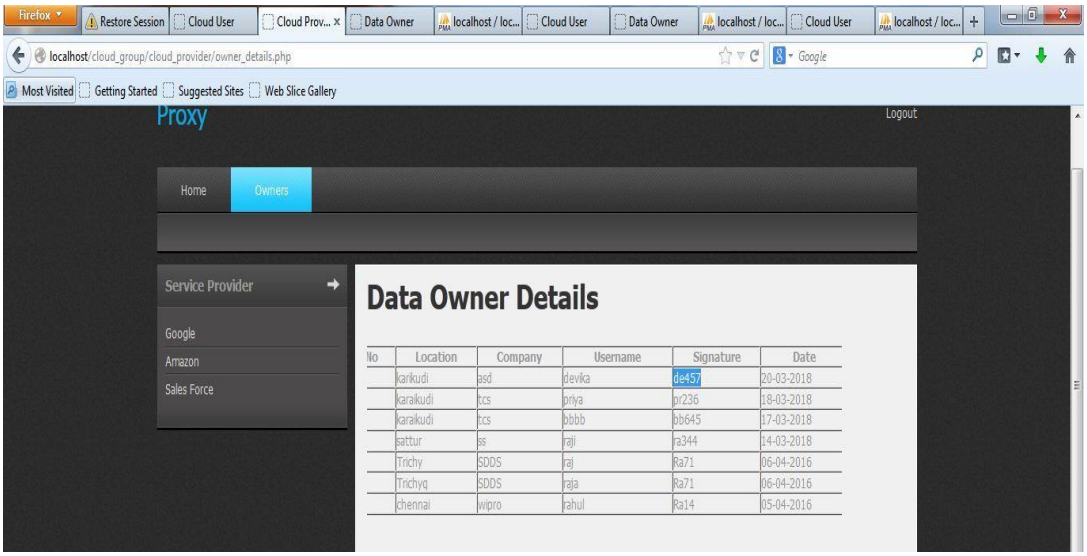

Fig 3: Signature details

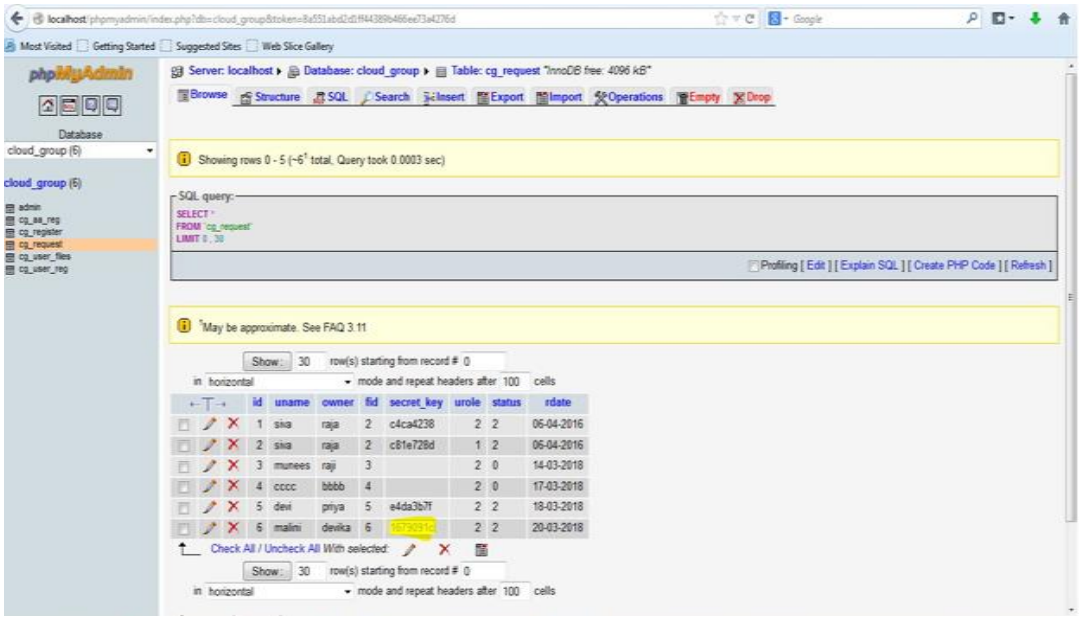

Fig 4: Group Manager registration Database

Field	Type	Null	Default
Id	int(11)	Yes	NULL
Name	varchar(30)	Yes	NULL
Contact	bigint(20)	Yes	NULL
Email	varchar(40)	Yes	NULL
Username	varchar(30)	Yes	NULL
Password	varchar(30)	Yes	NULL
Status	int(11)	Yes	NULL
Rdate	varchar(15)	Yes	NULL

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 11, November 2017

Table 1: Table structure for group manage registration

Field	Type	Null	Default
Id	int(11)	Yes	NULL
Aname	varchar(30)	Yes	NULL
Name	varchar(50)	Yes	NULL
Email	varchar(50)	Yes	NULL
Contact	bigint(20)	Yes	NULL
Location	varchar(50)	Yes	NULL
Company	varchar(30)	Yes	NULL
Design	varchar(30)	Yes	NULL
Signature	varchar(50)	Yes	NULL
public_key	varchar(20)	Yes	NULL
num_user	int(11)	Yes	NULL
Uname	varchar(50)	Yes	NULL
Pass	varchar(50)	Yes	NULL
Rdate	varchar(15)	Yes	NULL
Status	int(11)	Yes	NULL

Table 2: Table structure for user registration

Field	Type	Null	Default
Id	bigint(20)	Yes	NULL
Uname	varchar(50)	Yes	NULL
Owner	varchar(15)	Yes	NULL
Fid	varchar(45)	Yes	NULL
secret_key	varchar(50)	Yes	NULL
Urole	int(11)	Yes	NULL
Status	varchar(45)	Yes	NULL
Rdate	varchar(15)	Yes	NULL

Table 3: Table structure for user request

V. CONCLUSION

Cloud Computing is experiencing rapid growth and development. However, security concerns continue to pose challenges to its success. This paper examines various privacy threats and reviews techniques to mitigate them. While some methods employ traditional cryptographic techniques to ensure privacy, others explore alternative strategies. Additionally, the paper discusses methods for maintaining privacy during public auditing processes.

Ultimately, it is crucial for every cloud user to have confidence that their data is securely stored, processed, accessed, and audited at all times. Ensuring data freshness is vital to safeguard against intentional misconfigurations or rollbacks.

We propose the creation of an authenticated file system that facilitates the efficient, transparent, and scalable migration of an enterprise-level distributed file system to the cloud. This system allows enterprise tenants to verify the freshness of the data retrieved during file system operations, ensuring complete access control over the published data.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 11, November 2017

REFERENCES

[1] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.

[2] J. Li, Q. Huang, X. Chen, S. S. Chow, D. S. Wong, and D. Xie, "Multiauthority ciphertext-policy attribute-based encryption with accountability," in Proc. 6th ASIACCS, 2011, pp. 386–390.

[3] S. Müller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," Bull. Korean Math. Soc., vol. 46, no. 4, pp. 803–819, 2009.

[4] G. Ateniese, C. Blindo, A. De Santis and D.R. Stinson, Extended capabilities for visual cryptography, Theroretical computer science, Vol.250 (2001) 143-161.

[5] S. Droste, New results on visual cryptography, Advances in Cryptology-CRYPTO'96, Lecture notes in computer science, Vol.1109(1996) pp. 401-415

[6] M. Naor, A. Shamir, Visual cryptography, Advances in Cryptology – EUROCRYPT'94, Lecture notes in computer science, Vol.950, Springer, Berlin, 1995, pp. 1-12.

[7] S. Zhang, S. F. Zhang, X. B. Chen, and X. Z. Huo, "The Comparison between Cloud Computing and Grid Computing," 2010 International Conference on Computer Application and System Modeling (ICCASM), pp. V11-72 - V11-75,

[8] M. M. Alabbadi, "Cloud Computing for Education and Learning: Education and Learning as a Service (ELaaS)," 2011 14th International Conference on Interactive Collaborative Learning (ICL), pp. 589 – 594, DOI=21-23 Sept. 2011.

[9] P. Kalagiakos "Cloud Computing Learning," 2011 5th International Conference on Application of Information and Communication Technologies (AICT), Baku pp. 1 - 4, DOI=12-14 Oct. 2011.

[10] P. Mell and T. Grance, "Draft NIST working definition of cloud computing - vol. 21, Aug 2009, 2009.

[11] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a Service Security: Challenges and Solutions," 2010 7th International Conference on Informatics and System, pp. 1-8, March 2010.

[12] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," 2009 8th IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009, pp. 711-716.