Volume 4, No. 7, July 2013
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

AN EFFICIENT MODEL FOR PROVIDING SECURITY IN CLOUD COMPUTING ENVIRONMENT

[*1]Vikas Kumar , Sweta Pandey [1],

* Computer Science and Application, Thapar University, Patiala, India
Vikas735s@gmail.com[1]
[1]Information Technology, Banasthali University, Jaipur, India
Shwetapandey806@gmail.com[2]

Abstract: In this paper, we present an overview of existing cloud security algorithms. All these algorithms are described more or less on their own. Cloud security is a very popular task. We also explain the fundamentals of sequential rule mining. We describe today's approaches for cloud security. From the broad variety of efficient algorithms that have been developed we will compare the most important ones. We will systematize the algorithms and analyze their performance based on both their run time performance and theoretical considerations. Their strengths and weaknesses are also investigated. It turns out that the behaviour of the algorithms is much more similar as to be expected. A new model for cloud security is also proposed at the end. The results show that the new model is more efficient in comparison to the existing models.

INTRODUCTION

To achieve flexible and fine-grained access control, a number of schemes have been proposed more recently. Unfortunately, these schemes are only applicable to systems in which data owners and the service providers are within the same trusted domain. Since data owners and service providers are usually not in the same trusted domain in cloud computing, a new access control scheme employing attributed-based encryption is proposed, which adopts the so-called key-policy attribute-based encryption (KP-ABE) to enforce fine-grained access control. However, this scheme falls short of flexibility in attribute management and lacks scalability in dealing with multiple-levels of attribute authorities. This paper comprises of four sections including the present one which describes the goal of this paper. Section II shows research based papers which illustrates related work in cloud security. Section III gives a brief introduction regarding proposed model and experimental result. And at last section IV describe the conclusion and references

RELATED WORK

Nattakarn Phaphoom et al. [1] provide a comprehensive review on the building blocks of cloud computing and relevant technological aspects. It focuses on four key areas including architecture, virtualization, data management, and security issues.

Gaurav Dhiman et al. [2] present v Green, a multi-tiered software system for energy efficient computing in virtualized environments. It comprises of novel hierarchical metrics that capture power and performance characteristics of virtual and physical machines, and policies, which use it for energy efficient virtual machine scheduling across the whole deployment

Ramesh et al. [3] explains basic power management scheme in the general computing as well as grid computing. And this paper strongly performed an analysis on various categories of real time grid systems. The power consumption on various grid levels based on multiple volumes in the organization level is analysed. The conclusion is focused the future requirement of research direction in the energy efficient system design of grid computing.

Barroso et al. [4] describes energy-proportional designs which enable large energy savings in servers, potentially doubling their efficiency in real-life use. Achieving energy proportionality will require significant improvements in the energy usage profile of every system component, particularly the memory and disk subsystems.

Aman Kansal et al. [5] describe the challenges developers face in optimizing software for energy efficiency by exploiting application-level knowledge. To address these challenges, we propose the development of automated tools that profile the energy usage of various resource components used by an application and guide the design choices accordingly.

Henri Arjamaa et al. [6] present energy consumption estimates of ICT equipment in Finland and in three important industrial countries, namely the United States, Germany, and the United Kingdom. In addition, a worldwide estimate of the energy consumption of data centers is presented. The results are then analyzed, which

give answers to questions, such as how valid are the estimation methods used and are the estimation methods comparable with each other.

Christopher K. Lennard et al. [7] describe resynthesis procedures used for reducing power consumption in CMOS networks have produced poor results as they select nodes for resynthesis based upon local circuit properties. In this, a technique is presented for optimizing the choice of regions used in resynthesis. The cost function which is developed is able to predict the amount of global improvement in power expected through the resynthesis of network nodes under both zero as well as arbitrary delay assumptions.

Pinheiro et al. [8] have proposed a technique for managing a cluster of physical machines with the objective of minimizing the power consumption, while providing the required Quality of Service (QoS). The authors use the throughput and execution time of applications as constraints for ensuring the QoS. Here nodes are assumed to be homogeneous. The algorithm periodically monitors the load and decides which nodes should be turned on or off to minimize the power consumption by the system, while providing expected performance.

Srikantaiah et al. [9] have investigated the problem of dynamic consolidation of applications in virtualized heterogeneous systems in order to minimize energy consumption, while meeting performance requirements. The authors have explored the impact of the workload consolidation on the energy-per-application metric depending on both CPU and disk utilizations.

Elnozahy et al. [10] have investigated the problem of power-efficient resource management in a single web-application environment with fixed response time and load-balancing handled by the application. The two main power-saving techniques are switching power of computing nodes on or off and Dynamic Voltage and Frequency Scaling (DVFS).

Nathuji and Schwan et al. [11] have studied power management techniques in the context of virtualized data centers, which has not been done before. Besides hardware scaling and VMs consolidation, the authors have introduced and applied a new power management technique called “soft resource scaling.

Dodonov and De Mello et al. [12] have proposed an approach to scheduling distributed applications in Grids based on predictions of communication events. They have proposed the migration of communicating processes if the migration cost is lower than the cost of the predicted communication with the objective of minimizing the total execution time.

Guo et al. [13] have proposed and implemented a virtual cluster management system that allocates the resources in a way satisfying bandwidth guarantees. The allocation is determined by a heuristic that minimizes the total bandwidth utilization. The VM allocation is adapted i.e. migration is performed when some of the VMs are reallocated or power off but protocols for the migration are defined statically.

Berral et al. [14] presented a theoretical approach for handling energy-aware scheduling in data centers. Here, the authors propose a framework which provides an allocation methodology using techniques that include turning on or off machines, power-aware allocation algorithms and machine learning to deal with uncertain information while the expected QoS is maintained through the avoidance of SLA violations.

Song et al. [15] have proposed resource allocation to applications according to their priorities in multi-application virtualized cluster. The approach requires machine learning to obtain utility functions for the applications and define application priorities.

Sahai et al. [16] proposed Attribute-Based Encryption (ABE) Fuzzy Identity-Based Encryption, with the original goal of providing an error-tolerant identity-based encryption [12] scheme that uses biometric identities.

Pirretti et al [17] proposed an efficient construction of ABE under the Random Oracle model and demonstrated its application in large-scale systems. Goyal et al. enhanced the original ABE scheme by embedding a monotone access structure into user secret key.

Goyal et al. [18] proposed Key-Policy Attribute-Based Encryption (KP-ABE), a variant of ABE. In the same work, Goyal et al. also proposed the concept of Cipher text-Policy Attribute Based Encryption (CP-ABE) without presenting a concrete construction. CP-ABE is viewed as another variant of ABE in which cipher texts are associated with an access

Ostrovsky et al. [19] proposed an enhanced KP-ABE scheme which supports non-monotone access structures. Chaseet al. [16] enhanced Sahai-Waters ABE scheme and Goyal et al. KP-ABE scheme by supporting multiple authority. Further enhancements to multi-authority ABE can be found.

Bethencourt et al. [20] proposed the first CP-ABE construction with security under the Generic Group model. In Cheung et al. [18] presented a CCA-secure CP-ABE construction under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.

Waters et al. [21] proposed another CP-ABE scheme under various security assumptions. Aside from providing basic functionalities for ABE, there are also many works proposed to provide better security/privacy protection for ABE.

Goyal et al. [22] proposed a CP-ABE construction with an exponential complexity which can just be viewed as theoretic feasibility. For the same goal, these works include CP-ABE with hidden policy, ABE with user accountability, ABE with attribute hierarchy.

Table: Comparison between the existing cloud security models

Techniques/ Parameters	KP-ABE	EKP-ABE	CP-ABE	CP-ASBE	HIBE
Access Control	Low High if associated with re-encryption technique	Better than KP-ABE	Average Realization of complex Access Control	Better than CP-ABE	Comparatively low
Efficiency	Average High for broadcast type encryption	Higher thanKP-ABE Only allowconstant cipher text	Average Not efficient for modern enterprise environments	Better than CP-ABE Less collusion attacks	Better Lower when compared with ABE schemes
Computational overheads	High	Reduces the computations	Average	Lower than CP-ABE	Higher

PROPOSED SYSTEM

This proposed system addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to un-trusted cloud servers without disclosing the underlying data contents.
We propose a novel encryption scheme for access control in cloud computing. The proposed work is an extension of cipher text-policy attribute- set-based encryption (CP-ASBE, or ASBE for short) scheme.

New Scheme:

In new scheme, a data encrypted specifies an access structure for a cipher text which is referred to as the cipher text policy. Only users with decryption keys whose associated attributes, specified in their key structures, satisfy the access structure can decrypt the cipher text.

Basic Concepts Used

Key Structure: We use a recursive set based key structure as in [10] where each element of the set is either a set or an element corresponding to an attribute. The *depth* of the key structure is the level of recursions in the recursive set, similar to definition of depth for a tree. For a key structure

with depth 2, members of the set at depth 1 can either be attribute elements or sets but members of a set at depth 2 may only be attribute elements.

Access Structure

In our scheme, we use the same tree access structure as in [19]. In the tree access structure, leaf nodes are attributes and nonleaf nodes are threshold gates. Each nonleaf node is defined by its children and a threshold value. Let denote the number of children and the threshold value of node. An example of the access tree structure is shown in Fig., where the threshold values for "AND"and"OR"are2 and 1, respectively.

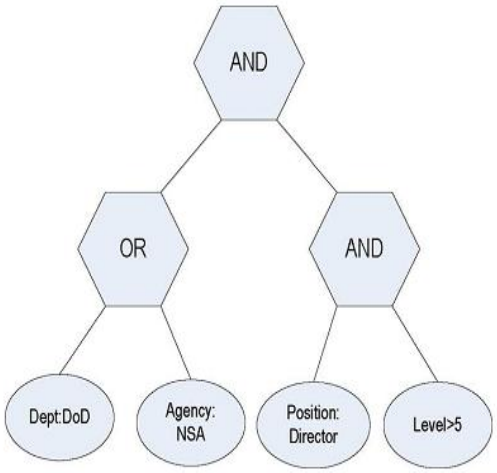

Fig1. Example access structure

The above access structure demands that only a director in DoD or NSA of level larger than 5 can access the data files protected by the access policy.

The Proposed Model:

In our proposed model, the client or user interacts with the third party auditor. The third party auditor is an authorized person appointed by the owner of the cloud. In our model, both data and auditor are present at the cloud servers site. It is responsible for performing functions at all the three layers.
The first layer is USER AUTHENTICATION
The second layer is DATA ENCRYPTION AND DATA PROTECTION
The third layer is DATA DECRYPTION

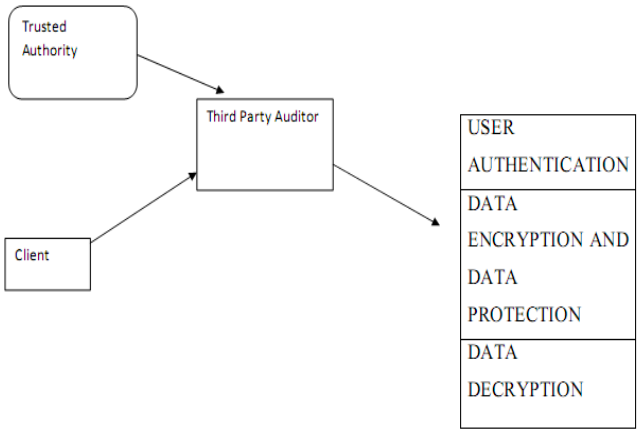

Fig2. The proposed Model

The Scheme

We propose a novel encryption scheme for access control in cloud computing. The proposed work is an extension of cipher text-policy attribute- set-based encryption (CP-ASBE, or ASBE for short) scheme.
Our scheme consists of a trusted authority, multiple domain authorities, and numerous users corresponding to data owners and data consumers. The trusted authority is responsible for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities. A domain authority is responsible for delegating keys to subordinate domain authorities at the next level or users in its domain. Each user in the system is assigned a key structure which specifies the attributes associated with the user's decryption key.

Our proposed scheme performs following operations

- System Setup
- Top-Level Domain Authority Grant
- New Third Party Auditors
- New File Creation
- User Revocation
- File Access, and File Deletion

CONLCUSION

In this paper, a novel approach has been introduced in which new scheme for realizing scalable, flexible, and fine-grained access control is there in cloud computing. The new scheme seamlessly incorporates a hierarchical structure of system users by applying a delegation algorithm to ASBE. New scheme not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes. We formally proved the security of new scheme based on the security of CP-ABE by Bethencourt *et al.* Finally, we implemented the proposed scheme, and conducted comprehensive performance analysis and evaluation, which showed its efficiency and advantages over existing schemes.

REFERENCES

[1] Phaphoom.N, Wang. X, Abrahamson.P." Foundations and Technological Landscape of Cloud Computing" (ISRN Software Engineering Volume 2013 (2013), Article ID 782174, 31 pages)
[2] Dhiman.G, Marchetti.G, Rosing.T "v: Green: a system for energy efficient computing in virtualized environments" (Proceedings of the 14th ACM/IEEE international symposium on Low power electronics and design, page 243-248, published in ACM, 2009)
[3] D. Ramesh, A. Krishnan "An Analysis on Energy Efficient System Design in Grid Computing"(Second International Conference, CCSIT 2012, Bangalore, India, January 2-4, 2012. Proceedings, pp 421-428)
[4] Barroso, L.A. Holzle, U. "The Case for Energy-Proportional Computing" (IEEE computer society, Volume: 40, Issue: 12, Dec. 2007 Page:33 – 37, ISSN :0018-9162)
[5] Kansa.A, Zhao.F. "Fine-Grained Energy Profiling for Power-Aware Application Design" (http://research.microsoft.com/en-us/um/people/zhao/pubs/hotmetrics08joulemeter.pdf)
[6] Arjamaa.H, "Energy Consumption Estimates of Information and Communication Technology: synthesis and analysis" (http://www.cse.tkk.fi/en/publications/B/5/papers/Arjamaa_final.pdf)
[7] Christopher K. Lennard A. Richard Newton," An Estimation Technique to Guide Low Power Resynthesis" (http://pdf.aminer.org/000/436/871/an_estimation_technique_to_guide_low_power_resynthesis_algorithms.pdf)
[8] E. Pinheiro, R. Bianchini, E. V. Carrera, and T. Heath, "Load Balancing and Unbalancing for Power and Performance in Cluster-Based Systems" (Workshop on Compilers and Operating Systems for Low Power, pp: 182–195, 2009.)
[9]S. Srikantaiah, A. Kansal, and F. Zhao, "Energy Aware Consolidation for Cloud Computing", (Cluster Computing, Vol. 12, pp: 1–15, 2009.)
[10]E. Elnozahy, M. Kistler, R. Rajamony, "Energy-Efficient Server Clusters" (Power-Aware Computer Systems, pp: 179-197, 2003)
[11] R. Nathuji and K. Schwan, "Virtualpower: Coordinated Power Management in Virtualized Enterprise Systems" (ACM SIGOPS Operating Systems Review, Vol. 41, pp: 256-278, 2007.)
[12] E. Dodonov, R. de Mell, "A Novel Approach for Distributed Application Scheduling Based on Prediction of Communication Events" (Future Generation Computer Systems, Vol. 5, pp: 740-752, 2010.)
[13]C. Guo, G. Lu, H. Wang, S. Yang, C. Kong, P. Sun, W. Wu,Y. Zhang, "Secondnet: A Data Center Network Virtualization Architecture with Bandwidth Guarantees", (6th International Conference on emerging Networking Experiments and Technologies, USA, 2010.)
[14] J. L. Berral, R. Nou, F. Julia, "Towards Energy-Aware Scheduling in Data Centers using Machine Learning" (1st International Conference on Energy-Efficient Computing and Networking, Passau, Germany, 2010.)
[15]Y. Song, H. Wang, Y. Li, B. Feng, Y. Sun, "Multi-Tiered On-Demand Resource Scheduling for VM-Based Data Center"(9th IEEE/ACM International Symposium on Cluster Computing and the Grid, China, pp: 148–155, 2009.)
[16] A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In Proc. of EUROCRYPT'05, Aarhus, Denmark, 2005.
[17] D. Boneh and M. Franklin. Identity-Based Encryption from The Weil Pairing. In Proc. of CRYPTO'01, Santa Barbara, California, USA, 2001.
[18] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure Atrribute-Based Systems. In Proc. of CCS'06, New York, NY, USA, 2006.

[19] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data. In Proc. of CCS'06, Alexandria, Virginia, USA, 2006.
[20] R. Ostrovsky, A. Sahai, and B. Waters. "Attribute-based encryption with non-monotonic access structures". In Proc. of CCS'06, New York, NY, 2007.
[21] M. Chase. "Multi-authority attribute based encryption". In Proc. of TCC'07, Amsterdam, Netherlands, 2007.
[22] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In Proc. of SP'07, Washington, DC, USA, 2007.
[23] L. Cheung and C. Newport. Provably Secure Ciphertext Policy ABE. In Proc. of CCS'07, New York, NY, USA, 2007.
[24] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization", http://eprint.iacr.org/2008/290.
[25] V. Goyal, A. Jain, O. Pandey and A. Sahai, "Bounded Ciphertext-Policy Attribute based Encryption", In Proc. of ICALP'08, Reykjavik, Iceland, 2008
[26] M. J. Hinek, S. Jiang, R. Safavi-Naini, and S. F. Shahandashti, "Attribute-Based Encryption with Key Cloning Protection", http://eprint.iacr.org/2008/478
[27] Jin Li, Qian Wang, Cong Wang, and Kui Ren, "Enhancing Attribute-based Encryption with Attribute Hierarchy," In Proc. of ChinaCom'09, Xi'an, China, 2009.

