SAJET

South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 111–116

ISSN No: 2454-9614

Optimal Performance and Security for data in Grid using TDEA

S. Satheeshkumar[a], D. Venkateswaran[a*], N. Sengottiyan[a,b]

[a)] Department of Computer Science and Engineering, Nandha Engineering College
Erode, Tamilnadu, India.
[b)] Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology,
Coimbatore, Tamilnadu, India

*Corresponding Author: S. Satheeshkumar

E-mail: venkatnba@yahoo.com

Received: 10/11/2015, Revised: 13/12/2015 and Accepted: 04/03/2016

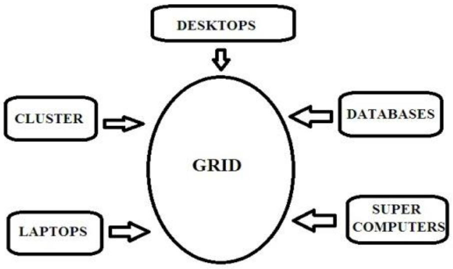
Abstract

Using Grid Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared network of configurable computing resources, without the burden of local data storage and maintenance. Grid computing offers dynamically scalable resources provisioned as a service over the Internet. The third-party, on-demand, self-service, pay-per-use, and seamlessly scalable computing resources and services offered by the Grid paradigm promise to reduce capital as well as operational expenditures for hardware and software. This thesis provides a survey on the achievable security merits by making use of multiple distinct Grids simultaneously. Various distinct architectures are introduced and discussed according to their security and privacy capabilities and prospects. It provides four distinct models in form of abstracted multi-Grid architectures. These developed multi-Grid architectures allow to categorize the available schemes and to analyze them according to their security benefits. An assessment of the different methods replication of applications, partition of application System into tiers, partition of application logic into fragments and partition of application data into fragments is given in particular. In addition, enabling public audit ability for Grid storage is of critical importance so that users can resort to an Integrity third party auditor to check the integrity of outsourced data and be worry-free. This thesis proposes a secure Grid storage system supporting privacy-preserving public auditing. It further extends the result to enable the ITPA to perform audits for multiple users simultaneously and efficiently.

Keywords: dynamic secret-based encryption, retransmission, security, wireless communication, zig-bee protocol, TDEA.
Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

Grid computing is the collection of shared computer resources from more than one location to reach a common goal. The grid can be thought of as a distributed system with not capable of acting on workloads that involve a large number of files. Grid computing is different from standard high performance computing systems such as cluster computing in that grid computers have each node set to carry out an action in different task/application. Grid computers also tend to be more heterogeneous and geographically distributed over a wide area than cluster computers. Although a single grid can be use entirely to a particular application, commonly a grid is used for a various purposes. Grids are often constructed with not limited in use of grid middleware software libraries. Grid sizes can be quite large.



2. Literature Survey

THOMES RISTANPERT, ERUN TROMAR, HOVEV SHACHEM and STEFAN SAVEGE **[1]** stated that third-party grid computing represents the promise of obtain service from outside as applied to computation. Services, such as Microsoft’s Azure and Amazon’s EC2, allow users to represent by an instance virtual machines (VMs) on demand and thus purchase precisely the capacity they require when they require it. The attacks they considered require two main steps: placement and extraction. Placement refers to the adversary arranging to place their harmful VM on the same physical machine as that of a target customer. Using the same platform they also demonstrated the existence of simple, low-overhead, “co-residence” checks to determine when such an advantage placement has taken place. While they focused on EC2, they believed that variants of our practical method are likely to generalize to other services, such as Microsoft’s Azure or Rack space’s Mosso **[11],** as they only utilized standard customer capabilities and do not require that grid providers disclose details of their infrastructure or assignment policies. Having managed to place a VM co-particular place with the target, the next step is to extract confidential information travelled through a cross-VM attack. While there are a number of lines of approach for such an attack, in this paper we focus on side-channels: cross-VM data leakage due to the sharing of physical resources. They showed preliminary results on VM side channel attacks, including a range of building blocks and coarse-grained attacks such as measuring activity burst timing .This point to the practicality of side-channel attacks in grid-computing surrounding conditions. Overall, their results indicated that there exist touchable dangers when distributing systematically sensitive tasks to third-party compute grids.

ARI JUELS **[2]** details the construction of an access-driven side-channel attack by which a malicious VM is called as virtual machine that is used extracts the grained information from a VM running on the same physical computer. The attack first gives a symmetric multiprocessing system virtualized using a modern VMM (Xen). This gradually addresses these challenges and the attack that are used to extract an ElGamal decryption key using the most recent version of the libgcrypt cryptographic library. Specifically, they showed that the attacker

VM’s monitoring of a victim’s repeats it provide information’s that are used to reconstruct the victim’s 457-bit exponent of private accompanying a bit modulus with very high accuracy—so the attackers with high was then left to search fewer than that are so possible exponents which are the right one.

JURAJ SOMOROVSKY, MARIO HEIDERICH, NILS GRUSCHKA and LUIGI LO IACONO **[3]** stated that Grid Computing resources are handled through interfaces of control. If these interfaces are done with new machine images, it can be added and the ones which elitists can be modified. The grid computing has been hailed that is about t save the cost of the authors. In euphoria, the migration to the grid needs to be considered for the further. Even though the obstacles are there, the highest weight is assigned which has the high security. The authors refer to two distinct classes of attacks. They are Amazon EC2 and Eucalyptus grid control interfaces. The 1st attacks comply of the XML Signature Wrapping attacks. For this the knowledge of a single SOAP message is sufficient .The reason is easiness is that one can generate arbitrary .The messages is accepted for a valid signature. To do this things happen, in one attack variant, knowledge of the (public) X.509.The Eucalyptus Web is used as a front-end. Technically, the grid control interface can be realized either as a SOAP-based Web Service, or as a Web application. If the control interface is SOAP-based, then WS-Security **[21]** can be applied to provide security services. For the authentication, the security tokens and XML Signature can be used for the authentication method.

SVEN BUGIEL, STEFAN NÜRNBERGER, THOMAS PÖPPELMANNY, AHMAD-REZA SADEGHI and THOMAS SCHNEIDER**[4]** stated that grid Computing is an technique that are used in business opportunities. Much has been written about the risks and benefits of grid computing in the last years. The security and privacy aspects of real-life grid deployments, independently from malicious grid providers or customers. Grid computing offers IT resources. The high usability of today's grid computing platforms makes this rapidly emerging paradigm. The main goal of this paper is the investigation and evaluation of security and privacy threats caused by the unawareness of users in the grid. The methods and techniques described in this are applicable to arbitrary IaaS providers, they focused on one of the major grid providers, Amazon's Elastic Compute Grid (EC2) **[24]** and adapt their terminology accordingly. In the following, they described the players involved in the (Amazon) Grid App Store and the resulting security challenges.

3. Types of Gird

3.1 Computational Grid

3.2 Collaboration Grid

3.3 Utility Grid

3.4 Network Grid

3.5 Data Grid

3.1. Computational Grid

There are different types of grid that are about to provide secure access to computational resources, sufficient enough to perform treat of computational problems which otherwise would have required high computing power machines.

3.2. Collaboration Grid

With the boost in network hardware resources and internet services, demand for better collaboration has increased. Such craved collaboration is best possible with these kinds of grids.

3.3. Utility Grid

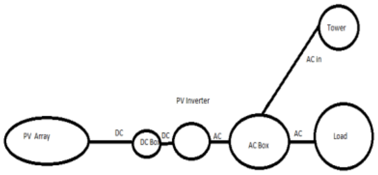
In this type of grid not only CPU cycles are shared, also to her software's and special central like sensors are also shared.

3.4. Network Grid

Even if we have computational machines with plenty computational power as a part of grid but with poor network communication one can't utilize those machines in desirable way. Network grid provides high performance communication using data caching between nodes there by quicken communication with each cache nodes acting as router.

3.5. Data Grid

There are two things, data and computation over that information. Data grid provides the support for data storage other data related services like data discovery, handling, publication, etc



4. Related Work

4.1. Existing Method

The technique of public key based homomorphism linear appraiser which enables Third Party Auditor to perform the inspection without demanding the local copy of data and thus drastic manner reduces the communication and figuring overhead as compared to the straightforward data auditing approach. By incorporate the HLA with random screening, the protocol assure that the TPA could not learn any knowledge about the information content stored in the grid server during the efficient auditing process. The accumulation and algebraic properties of the authenticator further benefit our design for the batch inspection. Various prime numbers are appointed as tags for each segment of file which is stored in host. Each section is holding two prime numbers each of which belongs to a assorted prime order. The third party listener knows the prime numbers in a random manner. During confirmation, the third party auditor sends the numbers as undistinguished challenge and if the numbers are co-ordinate with tags then the file unity is said to be verified. All the nodes are treated equally and weak capable nodes also require huge computations. All the mirror nodes store the file with same encryption mechanism. Unwanted data leakage still remains a problem due to the potential exposure of decryption keys. Only single grid provider environment is considered.

4.2. Proposed Technique

The aimed system includes all the existing system approach which covers multiple grid service provider environments. In addition, size cube data are being processed with varying size nature in different grid locations having same copy of data. The data cubes is stored and retrieved in different grid locations based on the storage and computational capability. Thus the aimed system explores such issue to provide the support of variable-length block verification. Likewise, the privacy level for all grid providers is analyzed by trusted authority and security degree and performance is quantified for encryption algorithms. Partial data of files are taken from multiple mirror locations and send to preference client. Eligible for very large size files. Beside the point size cubes of data are handled among the multiple grid service providers based on their computational capableness. Varied trust level is set to different grid providers and encryption/decryption is varied based on the grids computational capability.

5. Conclusion

Through this project, the problem of secure communication is eliminated. In addition, the application required less working experience in systems to run the software. The application is tested well so that the end users use this software for their complete operations. It is trust that almost all the system objectives that have been planned at the commencement of the software development have been net with and the implementation process of the project is completed. A trial run of the system has been made and is giving good results the procedures for processing is simple and regular order. The process of preparing plans been missed out which might be considered for further modification of the application. The project effectively stores and retrieves the records from the grid space database server. The records are encrypted and decrypted whenever necessary so that they are secure. The application if developed as web services, then many applications can make use of the records. The data integrity in grid environment is not considered. The error situation can be recovered if there is any unsuitable match. The web site and database can be hosted in real grid place during the implementation

Reference

[1] Sushmita Ruj and Amiya Nayak,” A Decentralized Security Framework for Data Aggregation and Access Control in Smart Grids “,IEEE Transactions On Smart Grid, Vol. 4, No. 1, March 2013.

[2] Ting Liu, Member, IEEE,YangLiu,YashanMao,YaoSun,XiaohongGuan, Fellow, IEEE, Wei bo Gong, Fellow, IEEE,and ShengXiao, ” A Dynamic Secret-Based Encryption Scheme for Smart Grid Wireless Communication,” IEEE Transactions On Smart Grid, Vol. 5, No. 3, May 2014.

[3] Mostafa M. Fouda, Member, IEEE, Zubair Md. Fadlullah, Member, IEEE, Nei Kato, Senior Member, IEEE, Rongxing Lu, Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE” A Lightweight Message Authentication Scheme for Smart Grid Communications” IEEE Transactions On Smart Grid, Vol. 3, No. 3, September 2012.

[4] Sungwook Kim, Eun Young Kwon, Myungsun Kim, Jung Hee Cheon, Seong-ho Ju, Yong-hoon Lim, and Moon-seok Choi,” A Secure Smart-Metering Protocol Over Power-Line Communication ” IEEE Transactions On Power Delivery, Vol. 26, No. 4, October 2011.

[5] Kebina Manandhar, Xiaojun Cao, Member, IEEE,FeiHu,Member, IEEE,andYaoLiu ” Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter “,IEEE Transactions On Control Of Network Systems, Vol. 1, No. 4, December 2014.

[6] Amir-Hamed Mohsenian-Rad, Member, IEEE, and Alberto Leon-Garcia, Fellow, IEEE” Distributed Internet-Based Load Altering Attacks Against Smart Power Grids “, IEEE Transactions On Smart Grid, Vol. 2, No. 4, December 2011.

[7] Yichi Zhang, Lingfeng Wang, Weiqing Sun, Robert C. Green II, and Mansoor Alam,” Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids” ,IEEE Transactions On Smart Grid, Vol. 2, No. 4, December 2011.

[8] Husheng Li, Member, IEEE, Shuping Gong, Lifeng Lai,Member,IEEE,ZhuHan, Senior Member, IEEE, Robert C. Qiu, Senior Member, IEEE, and Depeng Yang” Efficient and Secure Wireless Communications for Advanced Metering Infrastructure in Smart Grids” IEEE Transactions On Smart Grid, Vol. 3, No. 3, September 2012.

[9] Hasen Nicanfar, Student Member, IEEE, Paria Jokar, Student Member, IEEE, Konstantin Beznosov, Member, IEEE, and Victor C. M. Leung, Fellow, IEEE, ” Efficient Authentication and Key Management Mechanisms for Smart Grid Communications” IEEE Systems Journal, Vol. 8, No. 2, June 2014

[10] Thoshitha T. Gamage, Member, IEEE, Thomas P. Roth,StudentMember,IEEE, Bruce M. McMillin, Senior Member, IEEE, and Mariesa L. Crow, Fellow, IEEE,” Mitigating Event Confidentiality Violations in Smart Grids: An Information Flow Security-Based Approach “,IEEE Transactions On Smart Grid, Vol. 4, No. 3, September 2013.

[11] Kin Cheong Sou, Henrik Sandberg, and Karl Henrik Johansson,” On the Exact Solution to a Smart Grid Cyber-Security Analysis Problem “,IEEE Transactions On Smart Grid, Vol. 4, No. 2, June 2013.

[12] Gaojie Chen, Member, IEEE, Yu Gong, Pei Xiao, Senior Member, IEEE, and Jonathon A. Chambers, Fellow, IEEE” Physical Layer Network Security in the Full-Duplex Relay System” IEEE Transactions On Information Forensics And Security, Vol. 10, No. 3, Mar. 2015.

[13] Jinyue Xia and Yongge Wang” Secure Key Distribution for the Smart Grid” IEEE Transactions On Smart Grid, Vol. 3, No. 3, September 2012.

[14] Xudong Wang, Senior Member, IEEE, and Ping Yi,” Security Framework for Wireless Communications in Smart Distribution Grid ” IEEE Transactions On Smart Grid, Vol. 2, No. 4, December 2011.

[15] Anthony R. Metke and Randy L. Ekl, IEEE” Security Technology for Smart Grid Networks” IEEE Transactions On Smart Grid, Vol. 1, No. 1, June 2010.

[16] Zhiguo Wan, Member, IEEE, Guilin Wang, Yanjiang Yang, and Shenxing Shi” SKM: Scalable Key Management for Advanced Metering Infrastructure in Smart Grids “,IEEE Transactions On Control Of Network Systems, Vol. 1, No. 4, December 2014.

[17] Bin Hu, Senior Member, IEEE, and Hamid Gharavi, Life Fellow, IEEE, ” Smart Grid Mesh Network Security Using Dynamic Key Distribution With Merkle Tree 4-Way Handshaking,” IEEE Transactions On Smart Grid, Vol. 5, No. 2, March 2014

[18] RohitMoghe,StudentMember,IEEE,FrankC.Lambert, Senior Member, IEEE, and Deepak Divan, Fellow, IEEE,” Smart “Stick-on” Sensors for the Smart Grid” , IEEE Transactions On Smart Grid, Vol. 3, No. 1, March 2012.

[19] Vinod Namboodiri, Member, IEEE, Visvakumar Aravinthan, Member, IEEE, Surya Narayan Mohapatra, Babak Karimi, Student Member, IEEE, and Ward Jewell, Fellow, IEEE” Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids ” IEEE Systems Journal, Vol. 8, No. 2, June 2014.

[20] Keith J. Ross, Member, IEEE, Kenneth Mark Hopkinson, Senior Member, IEEE, and Meir Pachter, Fellow, IEEE,” Using a Distributed Agent-Based Communication Enabled Special Protection System to Enhance Smart Grid Security “,IEEE Transactions On Smart Grid, Vol. 4, No. 2, June 2013