# DIVISION AND REPLICATION OF DATA IN GRID FOR OPTIMAL PERFORMANCE AND SECURITY

Venkateswaran.D[1] and Satheeshkumar.S[2]

[1]M.E.Scholar, Department of Computer Science & Engineering Nandha Engineering College, Erode, Tamil Nadu, India
[2]Assistant Professor, Department of Computer Science & Engineering, Nandha Engineering College, Erode, Tamil Nadu, India

## ABSTRACT

*Using Grid Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared networks of configurable computing resources, without the burden of local data storage and maintenance. In this project based on the dynamic secrets proposed design an encryption scheme for SG wireless communication, named as dynamic secret-based encryption (DSE). Dynamic encryption key (DEK) is updated by XOR the previous DEK with current DS. In this project based on the dynamic secrets proposed design an encryption scheme for SG wireless communication, named as dynamic secret-based encryption (DSE). The basic idea of dynamic secrets is to generate a series of secrets from unavoidable transmission errors and other random factors in wireless communications In DSE, the previous packets are coded as binary values 0 and 1 according to whether they are retransmitted due to channel error. This 0/1 sequence is called as retransmission sequence (RS) which is applied to generate dynamic secret (DS). Dynamic encryption key (DEK) is updated by XOR the previous DEK with current DS.*

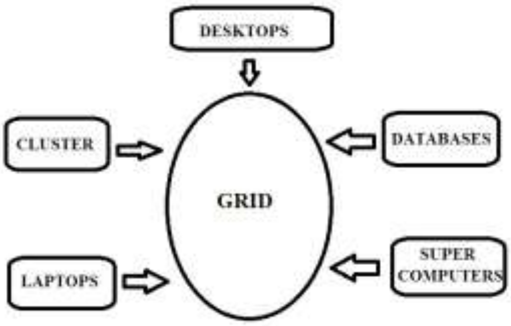
## KEYWORDS

*Dynamic secret-based encryption, retransmission, security, smart grid, wireless communication, ZigBee protocol.*

## 1. INTRODUCTION

Grid computing is defined as the bunch of computer resources that are shared to reach a common goal from more than one locations. The grid computing is like to a distributed system with not having ability of acting on workloads that involve a huge number of files. Grid computing is different from other computing systems such as cluster computing. In grid computing the computers have separate node set to carry out an action in different task/application. Grid computers are 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.

DOI:10.5121/ijgca.2016.7101



## 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 form outside as applied to computation. There are two services allow users to represent an instant virtual machine they are Microsoft’s Azure and Amazon’s EC 2. Placement and Extraction are the two main steps considered by the attacks. The adversary placed the harmful VM to the targeted customer machine with the reference of Placement. 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 Rackspace’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. The preliminary results on VM side channel attacks shows measuring activity burst timing (coarse – grained attack) and building block range.Overall, their results indicated that there exist touchable dangers when distributing systematically sensitive tasks to third-party compute grids.

ARI JUELS explains the building of as access driven side channel attack by a venomous VM is called as Virtual Machine. The VM gets the grained information by a physical computer where the same VM runs on it. The attack first gives a symmetric multiprocessing system virtualized using a modern VMM (Xen). This will addresses the attacks and the challenges that helps to extract an ElGamal decryption key which are using the recent version of 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 GRID

Computational grids: 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.

Collaboration grid: Collaboration has been increased by boosting the internet services and network hardware devices. Such craved collaboration is best possible with these kinds of grids.

Utility Grid: In Utility grid the shared resources are CPU cycles, software’s and peculiar sensors.

Network grid: We have more number of computational machines with plenty computational power but the result is poor network communication, we can’t utilize it properly. By using data caching between the nodes the network grid provide high performance communication. The communication is quicker because each nodes are acting as a router.

Data grid: There are two important things in grid they are data and computation. Data grid offers the support for storage of data and other data related services such as data handling, data publication, discovering the data as like data mining, etc

## 4. EXISTING TECHNIQUE

The technique of public key based homomorphic 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. At the time of auditing process the TPA couldn’t learn any information about the data that are stored in the grid server. This has been done by incorporating the HLA with random screening. For batch inspection the algebraic properties and accumulation of the authenticator is the additional benefit. The files that are stored in the host are allotted with various prime numbers. By the assorted prime order each section is holding two various prime numbers. 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-ordinated 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. Due to exposure of decryption keys the problem is unwanted data leakage. Only single grid provider environment is considered.

## 5. 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. The aimed system provides the support of variable – length block verification to avoid such kind of issues. The encryption algorithm checks the performance of all grid and the trusted authority and security degree checks the level of privacy. From mirror locations the partial data's are taken and send to the requested client on the grid. 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.

## 6.CONCLUSION

Through this project, the problem of secure communication is eliminated. To run the software the application doesn't need more working experience. The application is tested well so that the end users use this software for their complete operations. The system objectives and software development of the process is completed. It obtains good result during the sample run of the application. For further modification and application the plan missed out will be considered. The project effectively stores and retrieves the records from the grid space database server. The records in the server are secure because that are encrypted and decrypted whenever it is necessary. If the application is developed as a web service many sub application may use of records. The data integrity in grid environment is not considered. If any unsuitable match found the situation may occur error, instantly it will be recovered. The web site and database can be hosted in real grid place during the implementation.

## REFERENCES

1] Sushmita Ruj and Amiya Nayak," A Decentralized Security Framework for DataAggregation 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, March 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.

## AUTHORS

Venkateswaran.D, received the B.E. degree in Computer science and Engineering from Knowledge Institute of Technology in 2013.He is currently doing his M.E Computer science and Engineering in Nandha engineering college, Erode, India.

Satheeshkumar.S, (AP/CSE) working as Assistant Professor in Nandha Engineering College. He  has published many national and international research papers. He has very depth knowledge of her research areas.