An Approach to Secure Run Time Environment under Untrusted Management OS

Anchal Pokharana[1], Asmita Singh[2], Rahul Hada[3]

[1]Department of CE, Poornima College of Engineering, Jaipur, India
[2,3]Department of CE, Poornima University, Jaipur, India

Abstract**—** *Cloud Computing is internet based computing, in which large groups of remote servers are networked so as to allow sharing of data processing tasks, centralized data storage, and online access to computer services or resources. The prevalent Problem Associated with Cloud Computing is the Cloud security and the appropriate Implementation of Cloud over the Network. Cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. Problem is that Clouds typically have single security architecture but have many customers with different demands and I attempt to solve this problem. In this I need to provide Integrity of data by overcoming many existing problems like Client Data Integrity, Cloud Storage Integrity ,Integrity Problem on Transmitted Data, Integrity Problem When Update the Client Data, Integrity among VM Instances and Integrity of Cloud Services . Which is mostly need to enhance of Integrity of Cloud Data to get better Data accessibility over network. To learn about Data Integrity in cloud computing, a review process involving 3 stage approaches has been undertaken for 40 research papers which were published in the period of year 2010 to year 2013. The outcome of the review was in the form of various findings, found under the key issue. The findings included algorithms and methodologies used to solve particular research problem, along with their strengths and weaknesses and the scope for the future work in the area.*

Keywords**— Data Integrity, Cloud Storage, Virtual Instances, Privacy, RSA**

I. INTRODUCTION

Cloud Computing simply means internet computing. It allows user to store large amount of data in cloud storage and use as and when required from any part of the world via any terminal equipment. Since cloud computing is rest on internet. It implies sharing of computing resources to handle applications. Cloud computing offers reduced capital expenditure, operational risks, complexity, maintenance and increased scalability while providing services at different abstraction levels [2].

Since cloud computing is a utility available on net so it brings about not only convenience and efficiency problems but also great challenges in the field of data security and privacy protection and many more like: data theft and leakage, Data confidentiality, Integrity Verification, authentication various hackers attacks are raised. Cloud computing is a great change of information system. Security becomes a bottleneck of cloud computing development ensuring the security has been regarded as one of the greatest problems in the development of cloud computing [4]. Cloud computing is a latest and fast growing technology that offers an innovative, efficient and scalable business model for organizations to adopt various information technology resources i.e. software, hardware, network, storage, bandwidth etc. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. It has the capability to incorporate multiple internal and external cloud services together to provide high interoperability there can be multiple accounts associated with a single or multiple service provider (SPs). So, Security in terms of integrity is most important aspects in cloud computing environment[1]

Data integrity refers to maintaining and assuring the accuracy and consistency of data over its entire life cycle. Data integrity can be compromised in a number of ways:

- Human errors when data is entered
- Errors that occur when data is transmitted from one computer to another
- Software bugs or viruses
- Hardware malfunctions, such as disk crashes
- Natural disasters, such as fires and floods

There are many ways to minimize these threats to data integrity. These include:

- Backing up data regularly
- Controlling access to data via security mechanisms
- Designing user interfaces that prevent the input of invalid data
- Using error detection and correction software when transmitting data

II. SOLUTION APPROACHES USED

Data Integrity among VM Instances

For issue A light Weight Centralized File Monitoring Approach (Cryptography) and A Fingerprinting System Call Approach are used to maintain data integrity among VM Instance. These approaches prevents malicious VM users to modify well known frequently executed programs. The solution approaches under this issues have been shown in the **Table 2.1**, which includes additional information like Data used along with results obtained. The same table also describes the Comparative analysis between various solution approaches.

Table 2.1 Data Integrity among VM Instances

S. No	Solution Approach	Data used	Results
1	A light Weight Centralized File Monitoring Approach (Cryptography	Hash database	Avoiding the need of external database to store the checksum of files. Minimum resources needed Requires minimal and lightweight Standalone utility application, transparent and platform independent
2	A Fingerprinting System Call Approach	Synthetic dataset	Prevents malicious VM users to modify well known frequently executed programs
3	Virtualization Architecture	Synthetic dataset	A secure VM execution environment under an untrusted management OS
4	An architecture for dynamic management and monitoring of virtual machines	Real dataset	Improvement on the secure policy by adding a flexible access control.
5	TVMCM, Trusted VM Clone Model	Spatial Dataset	Identities verification of involved servers Attestation of source VM and destination VM Protection of integrity of transmitted data. Capable of working with the Xen hypervisor

In this issue the best approach is Fingerprinting System Call Approach for Intrusion Detection because it creates individual array for each system call and Low Complex, Scalability and adaptability are the advantages .The worst Approach is light Weight Centralized File Monitoring Scheme because this scheme is not deployed yet.

III. TECHNOLOGIES USED BY RESEARCHERS

Hardware specification:

Researchers used various types of hardware specifications according to the requirement of their work. These are following

1. Pentium Core.
2. Intel Core i3
3. RAM Size 128mb, 2GB.
4. Processor 1.2GHz, 2.4GHz

Software specification:

Researches used the following software for their proposed work

1. Supporting OS: Windows XP, VISTA, LINUX: Red Hat, Ubuntu, Fedora.
2. Java Development Kit - jdk1.6.0_02.
3. Java Runtime Environment - jre1.6.0_06.
4. Web Browser like Google chrome with Java Plug-in installed.
5. Wireless connectivity driver.
6. XEN and KVM Hypervisor

Technology Specific Tools used:

Researchers used the following technology tools for their experimentation part:

1. Java Development Kit - jdk1.6.0_02.
2. Java Runtime Environment - jre1.6.0_06.
3. Java. awt package for layout of the applet.
4. Java.net package for connection settings and message passing.

IV. DATA USED

Researchers used many types of data for their experimentation, some of these are

- Hash database
- Synthetic dataset
- Real dataset
- Spatial Dataset

V. ADVANTAGES

- A light Weight Centralized File Monitoring Approach , is standalone utility application and is transparent and platform independent
- A new data integrity check scheme, based on the well-known RSA security assumption the advantage of this scheme is that the client did not need to keep the copy data in the client. So it indeed relieves the storage burden in client.
- The performances measures such as encryption time and time taken to detect corruption are reduced by a conceptual cloud architecture by adopting an encryption algorithm with dynamic small size key.
- Virtualization Architecture provides A secure VM execution environment under an untrusted management OS

VI. DISADVANTAGES

- On-demand logical resource (file) replication scheme, The Limitation of the proposed system is that FRS is a single point of failure in a group.
- A Dynamic Proof of Retrievability (PoR) Scheme detect only static data corruption. And security issues has limitations that are Data losses / leakage, Difficult to assess the reliability of suppliers, Authentication mechanisms are not so strong.

VII. PROPOSED SOLUTION

In this section, threat model is defined, analyze the security requirements, outline the design of the proposed secure virtualization architecture and then present the relevant details.

Threat Model:

In this threat model we consider the scenario of a client executing a security-critical VM on the remote virtualized computing environment. In this scenario the hypervisor layer is verified and integrity of the hypervisor layer is assured using Trusted Computing techniques However, the management VM Dom0 is a complete OS and managed by the administrator.

The security threats may come from several ways:

- Attackers from outside of the cloud computing environment. An attacker may access the management OS and control root, memory,Input/Output, CPU and other privileged access rights.
- Attackers who are clients of the cloud computing environment, a client that runs a DomU in the cloud computing environment can control Dom0, access all the privileges and break into another client's VM.
- Attackers from inside the cloud computing environment. The hypervisor layer is verified from hardware but Dom0 is controlled by the system administrator. A careless or malicious administrator may leak or change sensitive information of the client. A compromised Dom0 can control the network I/O and secondary storage, but have no access to the hypervisor memory address space.

VIII. SYSTEM BLOCK DIAGRAM

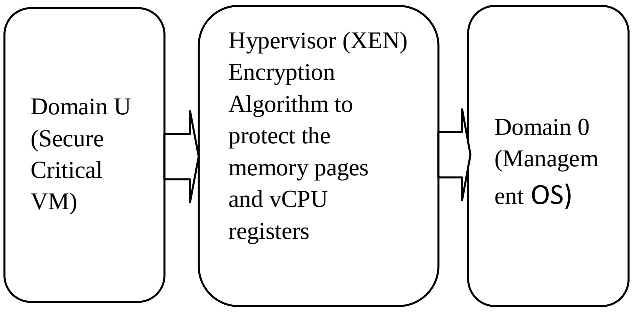

Figure 8.1 System Block Diagram

Design of a Secure Runtime Environment

- Dom 0 communicate with Dom U by using shared memory
- The shared memory use the grant table method, in which Dom U initiates the granting and Dom 0 asks for access through Hypercalls.
- Hypervisor monitors every memory and vCPU access from Dom 0 to Dom U
- Encrypt all the memory pages and vCPU registers if they involve any private information of Dom U.
- Dom 0 is provided with an encrypted view of memory pages and vCPU registers for the purpose of saving or restoring state.
- The contents of these pages and registers remain secret from Dom0

IX. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, the basic experiments have been conducted to give the detailed analysis of Native Vs Xen Hypervisor on CPU performance.

Experiment 1: Detailed analysis of Native Vs XEN Hypervisor on CPU performance Benchmark:

Benchmarking is the performance measurement of Virtual machine in term of CPU Bound, I/O Bound, and Memory Bound. Based on micro benchmarks, which compare the impact on basic primitive operation, and extending to real life situations by prediction. The benchmarking is also measure the workloads of similar life cycle. In this experiment sysbench benchmarking tool is used. The sysbench can test single-threaded and multi-threaded performance by calculating prime numbers.

Installation command of sysbench in Ubuntu14.04 is

#apt-get install sysbench

Open Terminal:

For XEN:

Step-1 **Xen start** (For XEN start)

Step-2 **Sysbench --test=cpu –-cpu–max–prime =2000 run** (command for run 2000 prime no)

Step-3 **Xend stop**(For XEN end)

Result:

Test Execution summary:

Total time: 1.7896ms

Total no of events :10000

Total time taken by event execution:1.7857

per-request statistics

Minimum	: 0.17ms
Average	: 0.18ms
Maximum	: 4.08ms

Approx .95 percentile .17ms

"Total execution time for 2000 prime no , on XEN Hypervisor is 1.7896 ms ."

For NATIVE

Step-1 **Sysbench --test=cpu –-cpu–max–prime =2000 run**

Result:

Test Execution summary:

Total time:1.7796ms

Total no of events :10000

Total time taken by event execution: 1.7857

per-request statistics

Minimum : 0.17ms

Average : 0.18ms

Maximum : 4.08ms

Approx .95 percentile .17ms

"Total execution time for 2000 prime no. on Native is 1.7796 ms."

An experiment for detailed analysis of the CPU performance on XEN and Native have been conducted. In this experiment CPU performance was checked on different prime numbers for XEN Hypervisor and Native. The execution time for different prime numbers are shown in table 9.1.

Table 9.1 Execution Time for XEN and Native

Reading on Prime No.	**XEN Reading (Total Execution time)**	**Native Reading (Total Execution time)**
2000	1.78ms	1.77ms
4000	4.11ms	4.09ms
6000	6.821ms	6.807ms
10000	12.956ms	12.9327ms
20,000	31.597ms	31.565ms
40,000	78.193ms	78.140ms
45,000	91.494ms	91.504ms

Results shows that CPU performance on XEN and Native is almost same because the Execution time of XEN and Native was close to each other.

X. CONCLUSION

The review of 41 research papers has been carried out in the area of Data Integrity in Cloud Computing to investigate and find out current challenges and scope of work

After this review I focused on the issue that is data integrity among VM instances and Cloud storage integrity, many of the solution approaches are used to maintain integrity of cloud.

The exhaustive review has finally led to extract findings, issue wise findings and common findings in the area of Data Integrity in Cloud Computing, strengths and weaknesses and also the gaps in the published research work.

Virtualization is the core of Cloud Computing, to maintain the integrity of Cloud Storage we can provide the integrity on Virtual Machines and it would be a big effect on cloud storage integrity.

REFERENCES

[1] Agrawal, D.; Abbadi, A.E.; Shiyuan Wang, "Secure and privacy-preserving database services in the cloud," Data Engineering (ICDE), 2013 IEEE 29th International Conference on , vol., no., pp.1268,1271, 8-12 April 2013 doi: 10.1109/ICDE.2013.6544921

[2] Bajpai, D.; Vardhan, M.; Kushwaha, D.S., "Ensuring Security in On-demand File Replication System," Computer and Communication Technology (ICCCT), 2012 Third International Conference on , vol., no., pp.315,320, 23-25 Nov. 2012 doi: 10.1109/ICCCT.2012.70

[3] Bendahmane, A.; Essaaidi, M.; El Moussaoui, A.; Younes, A., "Result verification mechanism for MapReduce computation integrity in cloud computing," Complex Systems (ICCS), 2012 International Conference on , vol., no., pp.1,6, 5-6 Nov. 2012 doi: 10.1109/ICoCS.2012.6458583

[4] Chalse, R.; Selokar, A.; Katara, A., "A New Technique of Data Integrity for Analysis of the Cloud Computing Security," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on , vol., no., pp.469,473, 27-29 Sept. 2013 doi: 10.1109/CICN.2013.103

[5] Chunxiao Li; Raghunathan, A.; Jha, N.K., "Secure Virtual Machine Execution under an Untrusted Management OS," Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on , vol., no., pp.172,179, 5-10 July 2010 doi: 10.1109/CLOUD.2010.29

[6] George, R.S.; Sabitha, S., "Data anonymization and integrity checking in cloud computing," Computing, Communications and Networking Technologies (ICCCNT),2013 Fourth International Conference on , vol., no., pp.1,5, 4-6 July 2013 doi: 10.1109/ICCCNT.2013.6726813

[7] Ghazizadeh, P.; Mukkamala, R.; Olariu, S., "Data Integrity Evaluation in Cloud Database-as-a-Service," Services (SERVICES), 2013 IEEE Ninth World Congress on , vol., no., pp.280,285, June 28 2013-July 3 2013 doi: 10.1109/SERVICES.2013.40

[8] Gupta, S.; Kumar, P.; Sardana, A.; Abraham, A., "A fingerprinting system calls approach for intrusion detection in a cloud environment," Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on , vol., no., pp.309,314, 21-23 Nov. 2012 doi: 10.1109/CASoN.2012.6412420

[9] Gupta, S.; Sardana, A.; Kumar, P., "A light weight centralized file monitoring approach for securing files in Cloud environment," Internet Technology And Secured Transactions, 2012 International Conference for , vol., no., pp.382,387, 10-12 Dec. 2012

[10] Hossain, A.-A.; Seung-Jin Lee; Young-Rok Shin; Islam, M.M.; Cheol-Su Lim; Eui-Nam Huh, "Shear-based spatial transformation to protect proximity attack of cloud data," ICT for Smart Society (ICISS), 2013 International Conference on , vol., no., pp.1,5, 13-14 June 2013 doi: 10.1109/ICTSS.2013.6588071

[11] Huifeng Wang; Zhanhuai Li; Xiaonan Zhao; Chanying Qi; Qinlu He; Jian Sun, "A scheme to ensure data security of cloud storage," Service Operations and Logistics, and Informatics (SOLI), 2013 IEEE International Conference on , vol., no., pp.79,82, 28-30 July 2013 doi: 10.1109/SOLI.2013.6611386

[12] Islam, M.R.; Habiba, M., "Agent based framework for providing security to data storage in cloud," Computer and Information Technology (ICCIT), 2012 15th International Conference on , vol., no., pp.446,451, 22-24 Dec. 2012 doi: 10.1109/ICCITechn.2012.6509712

[13] Itani, W.; Kayssi, A.; Chehab, A., "Energy-efficient incremental integrity for securing storage in mobile cloud computing," Energy Aware Computing (ICEAC), 2010 International Conference on , vol., no., pp.1,2, 16-18 Dec. 2010 doi: 10.1109/ICEAC.2010.5702296

[14] Iuon-Chang Lin; Hsing-Lei Wang, "An Improved Digital Signature Scheme with Fault Tolerance in RSA," Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on , vol., no., pp.9,12, 15-17 Oct. 2010Sdoi: 10.1109/IIHMSP.2010.10

[15] Junfeng Tian; Zhijie Wu, "A Trusted Control Model of Cloud Storage," Computer Distributed Control and Intelligent Environmental Monitoring (CDCIEM), 2012 International Conference on , vol., no., pp.78,81, 5-6 March 2012 doi: 10.1109/CDCIEM.2012.25

[16] Khatri, T.S.; Jethava, G.B., "Improving dynamic data integrity verification in cloud computing," Computing, Communications and Networking Technologies (ICCCNT),2013 Fourth International Conference on , vol., no., pp.1,6, 4-6 July 2013 doi: 10.1109/ICCCNT.2013.6726483

[17] [17]Kouril, D.; Rebok, T.; Jirsík, T.; Čegan, J.; Drašar, M.; Vizváry, M.; Vykopal, J., "Cloud-based testbed for simulation of cyber attacks," Network Operations and Management Symposium (NOMS), 2014 IEEE , vol., no., pp.1,6, 5-9 May 2014 doi: 10.1109/NOMS.2014.683829

[18] Kulkarni, G.; Gambhir, J.; Patil, T.; Dongare, A., "A security aspects in cloud computing," Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference on , vol., no., pp.547,550, 22-24 June 2012 doi: 10.1109/ICSESS.2012.6269525

[19] Naruchitparames, J.; Giine, M.H., "Enhancing data privacy and integrity in the cloud," High Performance Computing and Simulation (HPCS), 2011 International Conference on , vol., no., pp.427,434, 4-8 July 2011 doi: 10.1109/HPCSim.2011.5999856

[20] Nepal, S.; Friedrich, C.; Henry, L.; Shiping Chen, "A Secure Storage Service in the Hybrid Cloud," Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on , vol., no., pp.334,335, 5-8 Dec. 2011 doi: 10.1109/UCC.2011.55

[21] Rewagad, P.; Pawar, Y., "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing," Communication Systems and Network Technologies (CSNT), 2013 International Conference on , vol., no., pp.437,439, 6-8 April 2013 doi: 10.1109/CSNT.2013.97

[22] Salma, T.J., "A flexible distributed storage integrity auditing mechanism in Cloud Computing," Information Communication and Embedded Systems (ICICES), 2013 International Conference on , vol., no., pp.283,287, 21-22 Feb. 2013 doi: 10.1109/ICICES.2013.6508269

[23] Sureshraj, D.; Bhaskaran, V.M., "Automatic DNA sequence generation for secured cost-effective multi -cloud storage," Software Engineering and Mobile Application Modelling and Development (ICSEMA 2012), International Conference on , vol., no., pp.1,6, 19-21 Dec. 2012 doi: 10.1049/ic.2012.0139

[24] Surianarayanan, S.; Santhanam, T., "Security issues and control mechanisms in Cloud," Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on , vol., no., pp.74,76, 8-10 Dec. 2012 doi: 10.1109/ICCCTAM.2012.6488075

[25] Talib, A.M.; Atan, R.; Abdullah, R.; Azrifah, M., "CloudZone: Towards an integrity layer of cloud data storage based on multi agent system architecture," Open Systems (ICOS), 2011 IEEE

Conference on , vol., no., pp.127,132, 25-28 Sept. 2011 doi: 10.1109/ICOS.2011.6079311

[26] Thanh Cuong Nguyen; Wenfeng Shen; Zhou Lei; Weimin Xu; Wencong Yuan; Chenwei Song, "A probabilistic integrity checking approach for dynamic data in untrusted cloud storage," Computer and Information Science (ICIS), 2013 IEEE/ACIS 12th International Conference on , vol., no., pp.179,183, 16-20 June 2013 doi: 10.1109/ICIS.2013.6607837

[27] Varalakshmi, P.; Deventhiran, H., "Integrity checking for cloud environment using encryption algorithm," Recent Trends In Information Technology (ICRTIT), 2012 International Conference on , vol., no., pp.228,232, 19-21 April 2012 doi: 10.1109/ICRTIT.2012.6206833

[28] V.Nirmala, R.K.Sivanandhan & Dr. R.Shanmuga lakshmi, 2013, “Proceedings of 2013 International Conference on Green High Performance Computing”, India, 978-1-4673-2594-3/13

[29] Wei Chen; Qiaoyan Wen, "An architecture for dynamic management and monitoring of virtual machines," Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on , vol.01, no., pp.444,448, Oct. 30 2012-Nov. 1 2012doi: 10.1109/CCIS.2012.6664445

[30] Wei Ma; Xiaoyong Li; Yong Shi; Yu Guo, "TVMCM: A trusted VM clone model in cloud computing," Information Science and Service Science and Data Mining (ISSDM), 2012 6th International Conference on New Trends in , vol., no., pp.607,611, 23-25 Oct. 2012

[31] Wenjun Luo; Guojing Bai, "Ensuring the data integrity in cloud data storage," Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on , vol., no., pp.240,243, 15-17 Sept. 2011 doi: 10.1109/CCIS.2011.6045067

[32] Xiangtao Yan; Yifa Li, "A wew remote data integrity checking scheme for cloud storage with privacy preserving," Communication Technology (ICCT), 2012 IEEE 14th International Conference on , vol., no., pp.704,708, 9-11 Nov. 2012doi: 10.1109/ICCT.2012.6511296

[33] Yanfei Liu; Lunzhen Tan; Qiaolin Yi, "A trusted network platform architecture scheme on clouding computing model," Computer Science and Information Processing (CSIP), 2012 International Conference on , vol., no., pp.890,892, 24-26 Aug. 2012doi: 10.1109/CSIP.2012.6308997

[34] Yongkang Fu; Bin Sun, "A scheme of data confidentiality and fault-tolerance in cloud storage," Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on , vol.01, no., pp.228,233, Oct. 30 2012-Nov. 1 2012doi: 10.1109/CCIS.2012.6664402

[35] Yongzhi Wang; Jinpeng Wei; Srivatsa, M., "Result Integrity Check for MapReduce Computation on Hybrid Clouds," Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on , vol., no., pp.847,854, June 28 2013-July 3 2013 doi: 10.1109/CLOUD.2013.118.

[36] Yulong Ren; Wen Tang, "A service integrity assurance framework for cloud computing based on MapReduce," Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on , vol.01, no., pp.240,244, Oct. 30 2012-Nov. 1 2012doi: 10.1109/CCIS.2012.6664404

[37] Zhang Jianhong; Chen Hua, "Secuirty storage in the Cloud Computing: A RSA-based assumption data integrity check without original data," Educational and Information Technology (ICEIT), 2010 International Conference on , vol.2, no., pp.V2-143,V2-147, 17-19 Sept. 2010 doi: 10.1109/ICEIT.2010.5607505

[38] Zhen Mo; Yian Zhou; Shigang Chen, "A dynamic Proof of Retrievability (PoR) scheme with O(logn) complexity," Communications (ICC), 2012 IEEE International Conference on , vol., no., pp.912,916, 10-15 June 2012 doi: 10.1109/ICC.2012.6364056

[39] Zhongbin Tang; Xiaoling Wang; Li Jia; Xin Zhang; Wenhui Man, "Study on Data Security of Cloud Computing," Engineering and Technology (S-CET), 2012 Spring Congress on , vol., no., pp.1,3, 27-30 May 2012 doi: 10.1109/SCET.2012.6341932

[40] Zhang, Z.H.; Chai, X.D.; Hou, B.C., "System security approach for web-enabled HLA/RTI in the cloud simulation environment," Industrial Electronics and Applications (ICIEA), 2011 6th IEEE Conference on , vol., no., pp.245,248, 21-23 June 2011doi: 10.1109/ICIEA.2011.5975588

[41] Iuon-Chang Lin,Hsing-Lei Wang, 2010, “An Improved Digital Signature Scheme with Fault Tolerance in RSA”, 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 978-0-7695-4222-5/10, pp.9-12 may be presented after the conclusion, if desired.