International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 17 (2015)

An Innovative Adaptive Method for Reducing Vulnerability and Flaws in Cloud Computing Environment

S. Srinivasan[1], K. Raja[2]
[1]*Research Scholar, Research & Development Center, Bharathiar University,Coimbatore,Tamilnadu,India and Associate Professor, Department of M.C.A,K.C.G College of Technology, Chennai, Tamilnadu, India.*
[2]*Principal cum Dean Academics, Alpha College of Engineering, Chennai, Tamilnadu, India.*
effectivemail@yahoo.com, raja_koth@yahoo.co.in

***Abstract*—Cloud computing provides a large measurable distributing environment for growing huge amount of data, processes, storage that work on different services and applications by on-demand services. Although the probable growth attained from the cloud computing environment, the security and privacy of an open ended, relatively generously accessible resource is still uncertainty, which impacts the cloud implementation. The current renovation of information technology rapidly increases their pace in promising cloud computing security and privacy in real time applications and its services. This paper deals the security concern includes many of threats, vulnerability, security flaws and attacks to the information and data. It assesses the problem of data segregation, service availability, fault tolerance, data migration, confidentiality, data integrity from the innovative adaptive model with a user authentication structure in a cloud computing. The innovative versatile mechanism provides the integration of various models such as dispersed, availability, rearrangement, encryption models with different interfaces, protocols and user authentication mechanism. This paper verifies user validity identity management between cloud users and service providers. This capable method maintains the cloud environment with better performance evaluation. Furthermore, security and privacy analysis recognizes the viability of the proposed method for cloud computing and extent productive efficiency with secure cloud environments.**

Keywords- cloud security; vulnerabilities; flaws; data segregation; authentication; threats;

I. INTRODUCTION

Cloud computing is a combination of new creative business methods, technologies and controls by presenting Information Technology (IT) services, shared software, hardware and other resources, has granted to users as a metered service through the Internet [1]. It assures to give an elastic IT infrastructure, accessible via the internet for convenient devices [2]. The key features of cloud computing are scalability, elasticity, multi-tenancy, on-demand self-service and self-provisioning of resources [3].

The cloud computing has three major cloud delivery models are Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as Service (SaaS). The cloud deployment model provides public, private, community and hybrid cloud [4]. According to new revolution of business models and computer industry, the cloud computing request has been rapidly developed, the security and privacy are the major consideration for the consumer to adapt cloud computing in real world applications [5].

Cloud computing suggest build savings in Information Technology of computer industry related to cost, including smaller execution, maintenance cost, minimum hardware to buy, diminish in operating cost, floor space and storage as resources and other services provided by a cloud service provider as a metered service. As per International Data Corporation (IDC) survey in 2009, 74% Information Technology (IT) managers believed that the vital challenge in a cloud hinders information themselves using cloud services and its types [6].

In a cloud computing environment, security and privacy are shared between the cloud service provider and consumer. Although cloud providers, publicize the security and privacy of their services, real exploitation of cloud services is not as safe and reliable as they claim. Amazon's Simple Storage Service was interrupted twice in the year 2009. According to Garter in 2009, more than 70% Chief Technology Officers' (CTOs) supposed that main reason not to use cloud computing services and its types due to cloud security and privacy concerns. Cloud computing security [7] is a huge set of technologies, controls, policies, and methods prearranged to shield data, information and applications with the associated infrastructure of cloud computing environment. Strong cloud security and privacy policies to create the guarantee information, restricting the illegal access in both computer industry data centers and cloud computing based distributed servers. The security and privacy of the cloud computing environment are the key import crisis in the improvement of cloud computing.

The major multiple cloud security issues [7,8,9,10] are:

- Data confidentiality
- Data integrity
- Service availability
- Vulnerability
- Leakage and loss of control
- Insider threats and malicious attacks
- Data intrusion
- Regulatory compliance
- Service hijacking

- Repudiation of information
- Privileged user access

The rest of this paper is organized as follows: Section II discusses numerous security issues in terms of vulnerability, threats, flaws and attacks in cloud computing. In Section III, gives a detailed description of the proposed exciting innovative adaptive method for reducing vulnerability and flaws in cloud environment. Section IV shows performance of experimental results. Finally, Section V concludes the paper with future work directions.

II. SECURITY ISSUES IN A CLOUD

Security and privacy are considered a main feature for cloud computing consolidation as a robust and feasible multi-purpose solution[11]. Security and privacy concerns indicate in the implementation of cloud computing technologies for sharing of resources, cloud services and data storage. Security risk is a primary role in cloud computing environment. Protecting the cloud information such as sharing of data, resources, credit card detail from the malevolent insider is a serious significance in a network. An enormous information center involves security arguments such as vulnerability, threats, attacks, flaws, privacy and secret control issues related to clouding data, and information has accessed by the third-party cloud service providers and other users, that be deficient in integrity, data loss and confidentiality. A cloud security [12] is the most responding in percentage of challenge of nine issues recognized to cloud environment as shown in Fig 1.

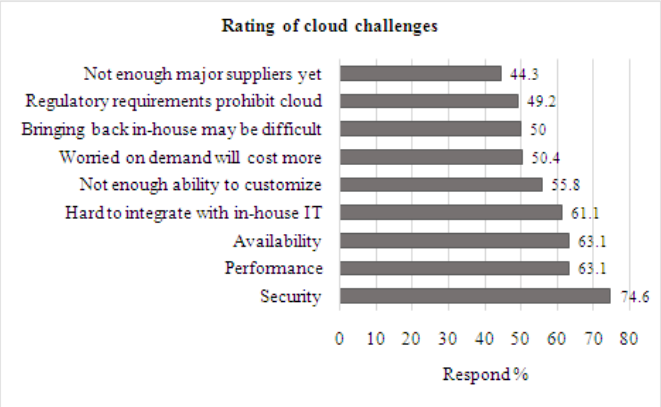

Fig 1. Rating of cloud computing challenges.

Garfinkel [13], identified data intrusion may happen with the cloud service providers, like Amazon cloud service, is hacked password or data intrusion. If any user capable to access an Amazon account password, then they are clever to access all the account's instances and other resources. Thus the hacker uses the stolen password to erase or modify all the information from the accounts or even disables its account's services. Service captures allow attackers to a concession the services such as, cookies, sessions, email profiles there by launching malicious inside attacks such as phishing, and exploitation of vulnerabilities.

The concept of privacy is very complex in various countries or jurisdictions. The definition adopted by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) in the Generally Accepted Privacy Principles (GAPP) standard is "The rights and obligations of persons and organizations with respect to the gathering, use, preservation, and disclosure of personal information" [7].

Gartner [14], explored regulatory compliance is a major security issue in cloud computing environment, which the clients are liable for the security and privacy of their solution, as users can select solution providers can be audited and authenticated by authentication method and third-party organizations.

According to Forrester [15], information operational integrity, vulnerability, attacks like DDoS attacks, data protection and threats are the top concerns of security and privacy issues for cloud computing environment. An attacker has access or altered data on the cloud storage, modify processing logic and functions of any component. More security and privacy occurrence in today's cloud environments is:

- A salesforce.com employee fell victim to a phishing attack and leaked the customer secret data, which produced further targeted phishing attacks in October 2007.
- In April 2011, Sony admitted that its Playstation network had intruded, leaving the user names, passwords and other information used to record accounts compromised. The stolen data may have payment-card data, security answers used to change passwords, which is the most important to the possibility of future recognize theft scams.

Bernd et al. [16], explored vulnerability is other major security concerns in a cloud. The control challenge is a matter of vulnerabilities, which explores some examples as listed below:

- Virtualized computer networks offer insufficient network based controls.
- Poor key management measures.

Data loss is another security issue raised by the consumers. When the organizations transfer their data to cloud, the cloud service provider not able to guarantee the data integrity and safety as they would in their premises, that

cause data leakage, loss of data and loss of control due to multi-tenant policy maintained in cloud environment [9].

Jensen et al. [17], describes an overview of security flaws and attacks on cloud computing infrastructures is specified. Some examples and current advances are shortly discussed in the following.

Ristenpart et al. [18],[19] presented some attack methods for virtualization of the Amazon EC2 IaaS service. In their method, the attacker assigns new virtual machines until someone runs on the same physical machine as the victim's machine, then the attacker can make cross-VM side channel attacks to study or alter the victim's information. The author's present strategies to reach the preferred victim machine with high probability, and show to use their position for extract secret information, eg., a cryptographic key, from the victim's VM. Finally, they suggest the usage of blinding procedures to fend cross-VM side-channel attacks.

Gruschka et al.[20], a flaw in the organization interface of Amazon's EC2 was found. The SOAP-based interface user's XML signature as clear in WS-Security for integrity safeguard and authenticity confirmation. The EC2 execution for signature confirmation is vulnerable to the signature wrapping attack [21].

User identity management maintaining digital identities, the semantic context of user's identity information using zero-knowledge proof-based methods. This method is used to protect user's privacy with delegation abilities to deal with identification and authentication problems in collected services [22]. The cloud service providers and consumers are taking care of security, privacy and protecting the cloud services, sharing of resources, information leakage from malicious attacks or hackers, data intruders in cloud computing.

III. INNOVATIVE ADAPTIVE METHOD FOR CLOUD

The innovative adaptive method reduces vulnerabilities, threats and flaws during sharing of resources by users in a cloud. Vulnerability is the chance that an asset will be not capable to oppose the actions when there is a dissimilarity between the force being applied by the hazard agent, and an object's ability to defy the force [16]. It appraises the problem of data separation, service accessibility, fault tolerance, data movement, data confidentiality and integrity. This innovative method resolves the crisis of security and privacy from the cloud plat-form security perspective, cloud service provider and cloud delivery model viewpoint. This method also validates user-authenticity, identity management between cloud computing users and cloud service providers is shown in Fig 2.

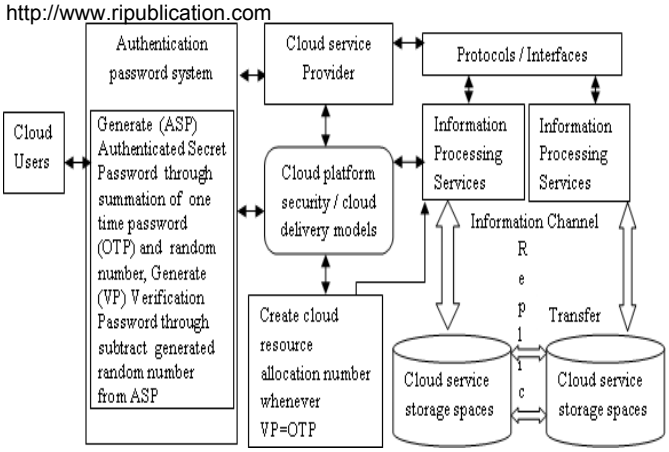

Fig 2. An innovative adaptive method for cloud environment

On the implementation of cloud, cloud users are putting their real time applications and information onto an isolated system that is not controlled by them. The major interior control systems, segregation of the task, which has two separate independent services responsible for information processing services and cloud data storage. It prevents scam, fault, and misuse of rights. The cloud service provider not able to provide services suddenly due to system breakdown, the cloud users will be seriously troubled about the service availability as per their requirement. It can be resolved by connecting information-processing services with other cloud storage services, hence information is copied and coordinated through duplication service. Moreover, cloud service provider's fix premium charges for their available services and resources, which might be extreme away from reasonable fees. The users able to transfer or movement of their information between two independent information-processing services or cloud storage services with affordable cloud service providers from one cloud to other clouds based on their user requirement. Even though the segregation of task mechanism splits the information processing from the storing of information about the reason of preventing frauds and threats. It is efficient with the statement that the two cloud service providers will not join. To ensure the statement, it is essential to separate the two cloud service providers by wounding all the direct communication between them. The need of filtering is enforced on the communication between the two cloud service providers. The information channel serves as a communication control between information-processing service and the cloud service storage space. It is the responsible for offering an interface for data processing services and cloud storage service to cooperate with each other, for maintaining, controlling and retrieving information in a secure way. The information channel service will invoke the cryptography service to perform a cryptographic operation on the data before handling the data over to the cloud. Thus, the information reserved by the cloud service storage space is cryptographically processed, or it can be expanded with digital certificates or signature or message authentication codes [23] based on security requirements.

The compatibility could be assured by providing consistent interfaces and protocols between cloud services such as data access interface, data duplication interface, data replication interface, hypertext transfer protocol and so on.

This modern creative method allows verifies the user authentication, acquire user request resources or services,

Cloud security Implementation	Reduces attack surface (lines of code)	Malware detection	Mitigates zero-day threats	Added overhead (%)
Malware	> 725 K	Yes	No	No data
Virtual snort	> 300 K	Yes	No	No data
Hybrid IDS	> 300 K	Yes	No	~4-36%
VMwall	~1,600 K	Yes	No	1-7%
Shype	~11 k	No	No	<1%
CReW	>270 K	Yes	Yes	~48-347%
Hypervisor-based Proactive recovery	~1,600 K	Yes	Yes	~8-12.7%

confirms the availability of resources or services with cloud service providers and cloud delivery models, after that allocate cloud resource allocation number to user requested specified resources, then it can be processed by Information-processing service and cloud storage service via interfaces and protocols. This process leads to reduce hijacking and several attacks like DDoS, HTTP Get flood attack, SYN flood attack, Cross Site Scripting (XXS) attacks, Hypervisor attacks and other attacks in cloud environment.

Table 1 [24] shows a summary comparison, of the approaches based on reduction at the attack surface, prevention of zero-day threats, and overhead.

Table 1 indicates comparison summary of cloud security implementation with attacks, malware and threats.

This novel method passes the three stages of information security in cloud computing, as first stage is information in transmission, second stage is information in storage, and final stage is processing information.

The improved creative method uses computational protective cloud architecture with different layers. Layer one specifies user request and authentication process, layer two shows cloud delivery models with cloud platform security, which includes software security, platform security, infrastructure security and layer three show strong cloud security framework. This cost saving hierarchical layered approach preserve privacy, reducing information and data leakage in cloud environment as shown in Fig 3.

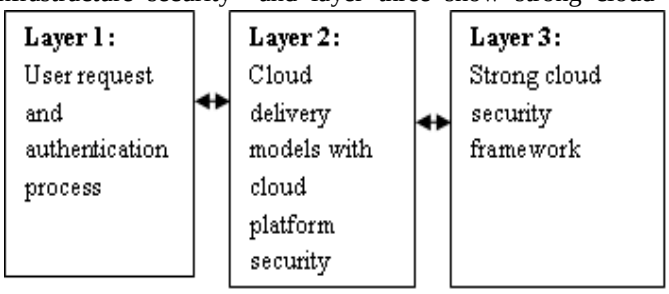

Fig 3. Layers and stages of innovative adaptive method.

This modern new method describes a secure authentication framework is proposed. The basic idea of this authentication framework as follows :-

1. The user has to register their proper identification details at the server.
2. The server generates random number for each user resource request after the user entered (login) into the system.
3. The user has received the one-time password from the server.
4. Generate Authentication Secret Password (ASP), which is the sum of step 2 and step 3.
5. Create Verification Password (VP) internally by the server, which is the subtraction of step 4 and step 2.
6. Allocate the Resource Allocation Number (RAN) for each user resource request when step 3 and step 5 are equal.

The complete operation process of an innovative adaptive method security framework as shown in Fig 4.

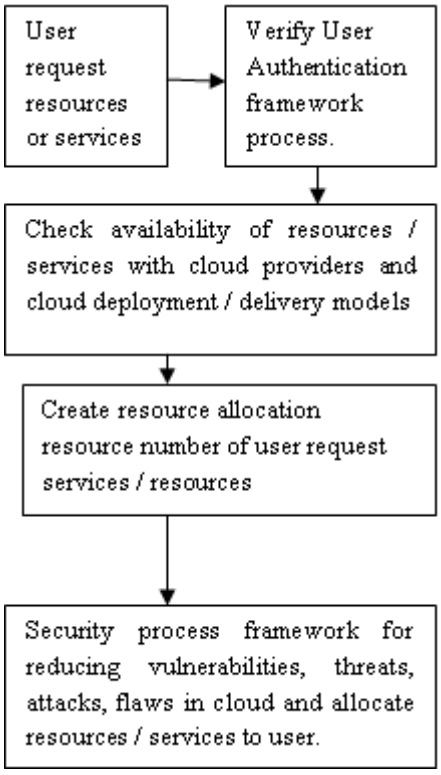

Fig 4. Operation process of Innovative adaptive security framework.

The allocation of resources to cloud user by the remarkable strong cloud security framework and cloud service provider to consumer. The resource allocation process as follows :-

1. While user get the Resource Allocation Number (RAN), it can appended with one time password as a plain text and it allows for the cryptographic substitution cipher method and send the resultant text (key) to step 2.
2. The strong cloud security framework receive the text (key) from step 1 and allocate the requested resources to cloud user with the help of cloud computing service provider and pass it to step 3.
3. Apply decryption method, verify the one time password again the decrypted text, if both are same, then allocate the resources to user. This is another way of Proof of Identity (POI), which verified the integrity and data confidentiality of cloud computing. It shows the way to avoid vulnerability and threats in cloud environment.

The above authentication framework and allocation of resources to cloud user by the remarkable strong cloud security framework and cloud service provider to consumer in cloud environment can be represented mathematically in form of finite automata. A finite automata is represented formally by a 5-tuple (Q,Σ,δ,q_0,F), where: Q is a finite set of states, Σ is a finite set of symbols, δ is the transition function, that is, $\delta: Q \times \Sigma \rightarrow Q$. q_0 is the start state, that is, the state of the automaton before any input has been processed, where $q_0 \in Q$. F is a set of states of Q (i.e. $F \subseteq Q$) called accept states.

The following Finite Automata state diagram represents the strong security authentication framework with the allocation of resources to cloud user as shown in Figure 5.

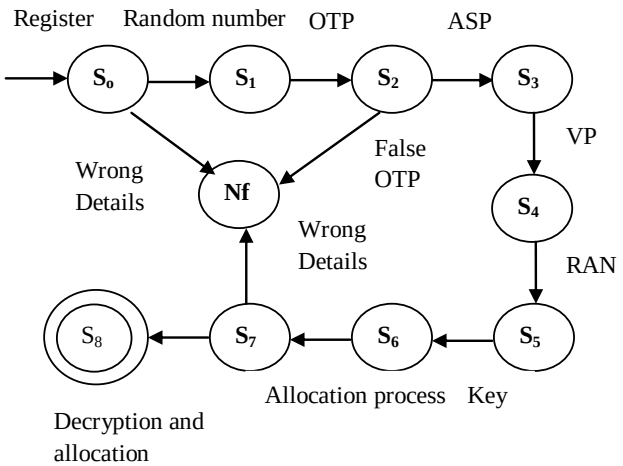

Figure 5. Finite Automata state diagram for the strong security authentication framework with the allocation of resources.

where S_o : Start state - Register user identification details.
S_1 : Generate Random number (as input symbol)
S_2 : Generate One Time Password (OTP as input symbol) from server
S_3 : Generate Authentication Secret Password (ASP)
S_4 : Generate Verification Password (VP as input)
S_5 : Create Resource Allocation Number (RAN as input symbol)
S_6 : Generate Key (encryption process as input)
S_7 : Resource Allocation process
S_8 : Final State - Decryption method and Resource allocation
N_f : Dead State - Wrong Details (or) OTP (or) key.

The third-party service provider make definite information security and privacy in cloud environment [25]. The cloud user should choose any services of the cloud delivery models and select any type of cloud deployment models based on their user requirements with the concerned security stages of cloud computing environment.

This method integrated cloud deployment models (private cloud, public cloud, hybrid cloud), cloud delivery models (platform as a service, software as a service and infrastructure as a service) with third-party service providers and vendors [26, 27].

IV. PERFORMANCE AND EVALUATION

It is observable that large number of attacks, threats are crashed the information or reducing file size, diminishing sharing of resources, that would further increase the computational and communication overheads of recovering services in cloud environment. The experiment results and analysis of the innovative adaptive method for reducing vulnerabilities, threats, attacks and flaws in cloud computing environment have described as:

The basic goal is to reduce threats and vulnerabilities in cloud computing and it should maintain a tradeoff between operating expense and standard reliable accuracy, which helps us to improve the high performance of cloud security systems. First, we compute the performance of our cloud security under different parameters, such as resource request size or file size *sz*, sample measurement ratio *w*,and resource request number or sector number per resource pooling or block *s*. Our analysis illustrates that the value of *s* should raise with the increase of *sz* to decrease computational and communication costs. Thus the experiments were carried out as follows: the requested resources or stored files were chosen from 100 KB to 1000 MB, the sector number or resource request number were changed from 50 to 1000 in terms of resource request size or file size, and the sample measurement

ratios were changed from 20 to 50 percent. The experimental results are shown in Fig 6. These indicates that computational and communication costs increase gradually with growth of request resource or file size and sample measurement ratio.

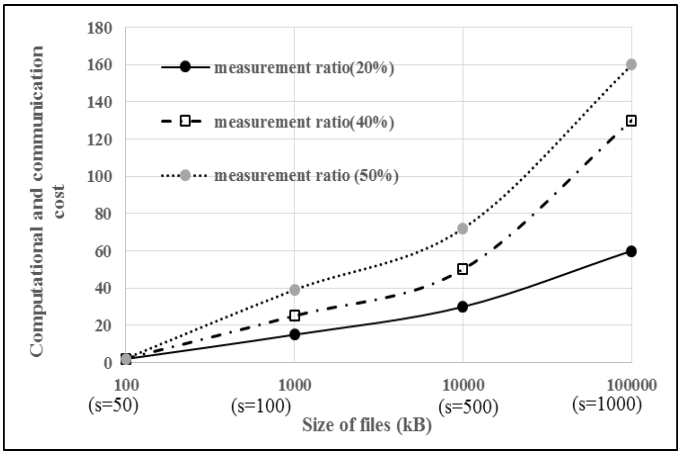

Fig 6. Cost and measurement ratio on various size of files

Proposed innovative method has admirable secured cloud architecture, which highly protect the information or resources or file size, allocation and sharing of requested resources or file size. More than 85 percent of threats, vulnerability, flaws and attacks were reduced on requested resources with better response in the cloud computing as shown in Fig 7.

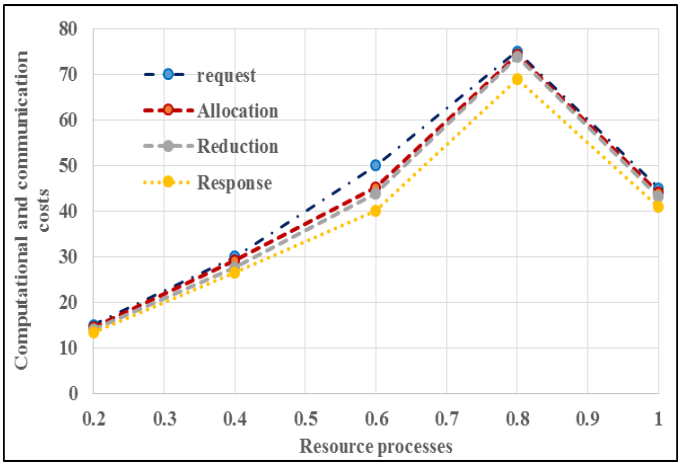

Fig 7. Reduction of high percent of vulnerability, threats and flaws on file size or resource allocation process in cloud.

It is easy to derive theoretically that the overheads of requested allocation resources or file size and reduction of security threats, attacks on allotted resources or different file sizes resemble one another. Fig 6 shows the experiment results, in which the computational and communication costs of allocation and reduction of threats and attacks on cloud are slightly changed for measurement resource processes, but those for reduction and response grow with the increase of sampling resources processes. Compare with Table 1, this proposed innovative method has reduced 85 percent of attack surface (lines of code), various types of threats, different overheads with higher response in cloud computing environment.

VI. CONCLUSION AND FUTURE WORK

Noticeably, although the use of cloud computing has rapidly developed. Cloud security threats, attacks and privacy are still measured and it has been the significant concern in the cloud computing. To protect information and sharing of resources in cloud environment against vulnerability, attacks and flaws, a safer cloud environment is required, therefore proposed a proper innovative adaptive method should be enforced. This paper deals the numerous security issues in terms of threats, vulnerability, flaws and cloud attacks to the data. It deeply assesses the difficulty of data separation, service availability, fault tolerance, data movement, information confidentiality, data integrity in cloud. This paper provides the integration of various mechansim such as dispersed, accessibility, reorganization, encryption models with interfaces, protocols, user authentication mechanism and resources allocation process with the assistance of cryptographic mechanism of cloud computing environment. This paper verifies user validity identity proof management between cloud users and cloud providers. This proposed method, reduces the vulnerability, threats, flaws and attacks in cloud comuting environment.

Future research on this work will include to develop a better cryptographic method and algorithm with specific standard protocols that can support high confidentiality, integrity and to meet more privacy and secure cloud computing environment. To welcome the coming cloud computing era, solving the cloud computing security and privacy issues becomes magnificent urgency, that show the way of cloud computing environment has a clear and bright future.

REFERENCES

[1] Xuyun Zhang, Chang Liu, Surya Nepal, Suraj Pandey, and Jinjun Chen, “A Privacy Leakage Upper Bound Constraint-Based Approach for Cost-Effective Privacy Preserving of Intermediate Data Sets in Cloud”, IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 6, pp.1192-1202, June 2013.

[2] Mohamed Hamdi, ”Security of Cloud Computing, Storage, and Networking”, ISBN: 978-1-4673-1382-7/12, 2012 IEEE, pp.1-5,2012.

[3] Eman M.Mohamed, Hatem S. Abdelkader,”Enhanced Data Security Model for Cloud Computing”,The 8th International Conference on INFOrmatics and Systems

(INFOS2012) - 14-16 May 2012, Cloud and Mobile Computing Track, pp.cc-12-cc19,2012.

[4] Mohammed A.AlZain,Eric Pardede,Ben Soh,James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", IEEE Transactions on cloud computing, vol. 9, no. 4, ISBN: 978-0-7695-4525-7, July/August 2012, pp.5490-5499, 2012

[5] Guoman Lin, "Research on Electronic Data Security Strategy Based on Cloud Computing", 2012 IEEE second International conference on Consumer Electronics,ISBN: 978-1-4577-1415-3, 2012, pp.1228-1231, 2012

[6] Sun Cloud Architecture Introduction White Paper (in Chinese),http://developers.sun.com.cn/blog/functionalca/resource/sun_353cloudcomputing_chinese.pdf

[7] Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing",2012 IEEE proceedings of International Conference on Computer Science and Electronics Engineering, ISBN: 978-0-7695-4647-6,pp.647-651, 2012.

[8] Gansen Zhao,Chunming Rong,Martin Gilje Jaatun, Frode Eika Sandnes, , "Reference deployment models for eliminating user concerns on cloud security", Springer, June 2010, DOI 10.1007/s11227-010-0460-9,pp.105-112, 2010.

[9] Akhil Behl, "Emerging Security Challenges in Cloud Computing", 2011 IEEE, ISBN: 978-1-4673-0126-8, pp.217-222,2011.

[10] Akhil Behl and Kanika Behl, "Security Paradigms for Cloud Computing",IEEE,ISBN: 978-0-7695-4821-0,pp.200-205, 2012.

[11] Nelson Gonzalez, Charles Miers, Fernando Redígolo, Tereza Carvalho, Marcos Simplicio,Mats Naslund and Makan Pourzandi," A quantitative analysis of current security concerns and solutions for cloud computing" , 2011 Third IEEE International Conference on Cloud Computing Technology and Science, 978-0-7695-4622-3/11 $26.00 © 2011 IEEE,pp.231-238,2011.

[12] Minqi Zhou and Rong Zang , "Security and Privacy in Cloud Computing",2010 IEEE Sixth International Conference on Semantics,Knowledge and Grids", published in IEEE Computer Society, ISBN: 978-0-7695-4189-1,pp.105-112,2010.

[13] S.L. Garfinkel, "An evaluation of amazon's grid computing services: EC2, S3, and SQS", Technical Report TR-08-07, Computer Science Group, Harvard University, Citeseer, 2007, pp.1-15.

[14] Gartner: Seven cloud computing security risks. Infoworld,2008-07-02, http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

[15] C.Wang,"Forrester: A Closer look at cloud computing securityissues,"http://www.forrester.com/securityforum 2009,2009.

[16] Bernd,Grobaur and Tobias,"Understanding Cloud Computing Vulnerabilities" Co published by IEEE Computer and Reliabilities Societies" IEEE April 2011,pp.50-57, 2011.

[17] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "On Technical Security Issues in Cloud Computing", *Proc. IEEE Int'l Conf. Cloud Computing* (CLOUD-II),2009.

[18] T. Ristenpart, E.Tromer, H.Shacham, and S.Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third Party Compute Clouds, " *Proc. 16th ACM Conf. Computer and Comm. Security* (CCS'09), pp. 199-212,2009.

[19] Y.Zhang, A.Juels, M.K.M. Reiter, and T.Ristenpart, "Cross-VM Side Channels and Their Use to Extract Private Keys", Proc. ACM Conf. Computer and Comm. Security (CCS'12), pp.305-316, 2012.

[20] N. Gruschka and L. Lo Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited", *Proc. IEEE Int'l Conf. Web Services* (ICWS'09), 2009.

[21] M. McIntosh and P. Austel, "XML Signature Element Wrapping Attacks and Countermeasures",*Proc. Workshop Secure Web Services*, pp.20-27,2005.

[22] Saleem-ullah Lar, Xiaofeng Liao and Syed Ali Abbas, "Cloud Computing Privacy & Security Global Issues, Challenges, & Mechanisms 2011 IEEE", 6th International ICST Conference on Communications and Networking in China (CHINACOM),pp.1240-1245,2011.

[23] Ramya.D, Dr.Raja.K, and Srinivasan.S, "An analysis of third party auditing techniques in cloud computing", International Journal of Advanced Research in Computer and Communication Engineering,, Vol. 3, Issue No.11, November 2014.

[24] Robert Denz and Stephen Taylor," A survey on securing the virtual cloud", Journal of Cloud Computing: Advances, Systems and Applications, Vol. 2, No.17, 2013.

[25] Srinivasan.S, Raja.K, "Dynamic Group Audit Control Mechanism for Cloud Computing Using *k*-means Inter-Batch Cluster Method", International Journal of Applied Engineering Research, ISSN 0973-4562, Vol.9 No.22, December 2014 Issue, pp.16821-16835, 2014.

[26] Srinivasan.S, Raja.K, "Secure Auditing Method for Cloud Computing", International Journal of Networking and Communication Engineering, ISSN 0974-9616, Vol.6 No.7, September 2014 Issue, pp.274-278, 2014.

[27] Srinivasan.S, Raja.K, "Security Challenges In Cloud Computing",International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459,Vol.4 Special Issue 4, April 2014, pp-01-06, 2014.

AUTHOR'S PROFILE

Srinivasan.S is currently pursuing research at the Bharathiar University, Coimbatore, Tamilnadu, India and also working as Associate Professor at KCG College of Technology, Tamilnadu, India. He received the MCA degree from Bharathiadasan University, India, in 1997 and M.E degree from Sathyabama University, India, in 2009. His research interests include cloud computing. He is a member of CSI, ISTE and IAENG.

Raja. K received the Ph.D degree from Sathyabama University, India, in 2006 and M.E Degree from Madras University, India, in 2001. Presently he is a Principal cum Dean (Academics) at Alpha College of Engineering, Tamilnadu, India. He is a member of CSI, IEEE, ISTE, IETE and IAENG. He has published 25 International Journals, 3 National Journals and 54 National & International conferences. He is a reviewer in National & International Journals. His research interests include cloud computing, knowledge management.