Review in Cloud Computing Security

Anchal Pokharana,Shweta Meena

Research Scholar, School of Engineering & Technology, Poornima University, Jaipur, India

Abstract:*The cloud Computing provides an undemanding and Non ineffectual Solution for Daily Computing. 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 we attempt to solve this problem. In this we need to provide availability of data by overcoming many existing problems like Data Leakage , Data Integrity and Privacy Protection. To learn about cloud computing security, a review process involving 2 stage approaches has been undertaken for 20 research papers which were published in the period of year 2010 to year 2013. After an exhaustive review process, four key issue were found "Security and privacy, Data Leakage and weakness, Data integrity problem and Data Hiding in cloud Computing." which is mostly need to enhance of Cloud Security aspects to get better Data accessibility over network. Several solution approaches have been found in the 20 papers. The outcome of the review was in the form of various findings, found under various key issues. 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.*
Key words: *Data Security , Integrity , Privacy , CSP , Data Leakage , Data Hiding , CI, AES Encryption*

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 and maintenance, and increased scalability while providing services at different abstraction levels. Cloud Providers offer services that can be grouped into three categories:

1. Software as a Service (SaaS): In this model, a complete application is offered to the customer, as a service on demand A single instance of the service runs on the cloud & multiple end users are serviced. On the customers" side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

2. Platform as a Service (PaaS): Here, a layer of software, or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE, Ruby etc.

3.Infrastructure as a Service (IaaS): IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, GoGrid, 3 Tera, etc.

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.

II. REVIEW PROCESS ADOPTED

A literature review is necessary to know about the research area and what problem in that area has been solved and need to be solved in future. This review process approach was divided into five stages in order to make the process simple and adaptable. The stages were:-

Stage 0: Get a "feel"
This stage provides the details to be checked while starting literature survey with a broader domain and classifying them according to requirements.

Stage 1: Get the "big picture"
The groups of research papers are prepared according to common issues & application sub areas. It is necessary to find out the answers to certain questions by reading the Title, Abstract, introduction, conclusion and section and sub section headings.

Stage 2: Get the "details"
Stage 2 deals with going in depth of each research paper and understand the details of methodology used to justify the problem, justification to significance & novelty of the solution approach, precise question addressed, major contribution, scope & limitations of the work presented.
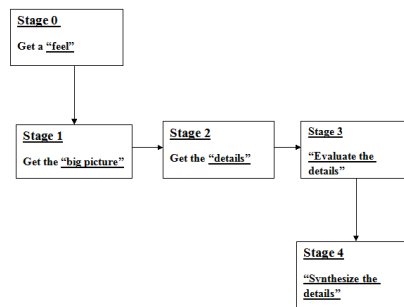
Fig: 2.1 Review Process Adopted

Stage 3: "Evaluate the details"
This stage evaluates the details in relation to significance of the problem, Novelty of the problem, significance of the solution, novelty in approach, validity of claims etc.

Stage 3+: "Synthesize the detail"
Stage 3+ deals with evaluation of the details presented and generalization to some extent. This stage deals with synthesis of the data, concept & the results presented by the authors.

III. VARIOUS ISSUES IN THE AREA

After reviewing 20 research papers on Cloud Computing Security we have found following issues, which has to be addressed, while the designing and implementation of the Cloud Computing these issues are:
1) **Security and privacy in cloud computing**
2) **Data Leakage and weakness in cloud computing**
3) **Data integrity problem in the cloud environment**
4) **Data hiding in cloud Computing**

IV. ISSUE WISE DISCUSSION

Issue 1:- Security and privacy in cloud computing
Security and Privacy in Cloud Computing is one of the issue, some approaches were used for this issue which is three way protection scheme. Diffie Hellman algorithm with digital signature and AES encryption algorithm,Digital Signature with RSA Encryption Algorithm, CI(Computational Intelligence) ,Enhanced Data Security Model, Private Face Recognition,key technologies in cloud are Virtualization technology, Programming model, Distributed data storage .Cloud Computing Background Key Exchange (CCBKE) scheme for security-aware scheduling in the background of cloud computing service providers. Provide experimental results or a proposed architecture and specific algorithm. By these solution approaches a secured cloud model is obtained [6].

Issue 2:- Data Leakage and weakness in cloud
Three proposed enhancements to that standard cloud service model: Virtual Private Storage Proxy, Remote Integrity Monitoring,Encrypted Computational Streams and 3 dimensional techniques for this issue [. Defend the solution by providing Methods to Remotely Augment and an Algorithm and Graphical representation of the 3 Dimensional Securities in cloud computing.

Issue 3:-Data integrity problem in the cloud environment.
Provide Data confidentiality and integrity verification using user authenticator scheme. Combine the encrypting mechanism along with the data integrity check mechanism [12]. The data are double wrapped to ensure no data leakage happens at the serve side. Cloud Storage Data Architecture, in this architecture, a data storage service involves three different entities. Cloud service provider(CSP) and Trusted Third Party(TTP).

Issue 4:-Data hiding in cloud Computing.
 Automatic DNA sequence generation MCDB with TMR techniques (Redundancy Technique)with sequential method .Result is secured cost effective multi-cloud storage (SCMCS) model in cloud computing, better addressing, data integrity, data confidentiality, and service availability. This model is more secured in protecting user's data. Mechanism in cloud for data hiding is two functions to create fake attributes Input function and Generating function that are periodic function .Research defend the solution by providing proposed architecture and graphical representation

V. ISSUE WISE SOLUTION APPROACHES USED

The solution approaches under the various issues have been shown in the **Table 6.1 to 6.4**, which includes additional information like hardware, software, variable/parameters usedalong with results obtained. The same table also describes the
Comparative analysis between various solution approaches.

VI. ISSUE WISE DISCUSSION ON RESULTS
ISSUE1:-SECURITY AND PRIVACY IN CLOUD COMPUTING

S.No.	Solution Approach	Results	Ref
1.	Digital Signature with Diffie Hellman Key Exchange and AES Encryption	Authentication, verification and encryption or decryption of data together	[1]
2.	Security service model with Key Realization Technology	A secured model involves standardization, supervision model, laws & regulations	[9]
3	CI(Computational Intelligence) with its Dynamic Application	Predict the incoming status and problems	[14]
4	Digital Signature with RSA Encryption Algorithm.	Low-cost supercomputing services.	[18]
5	Enhanced Data Security Model	Highest security, Least time to encrypt data and data retrieve faster.	[10]
6	Control mechanisms : 3 migration phases are classified. These are pre-migration, in operation and termination.	Create a trust environment between the client and the CSP	[13].
7	Private Face Recognition	Obtain correct result as under non-encrypted conditions.	[19]
8	Multi Tenancy model and pooled computing resource	Solve threats problems	[7]
9	Key technologies: Programming Model, Distributed Data storage,Virtualization Technology	High performance price ratio, Automatic upgrade, Strong adaptability Easy maintenance	[12]
10	Study on Data Security of Cloud Computing(Trusted access control, produce cipher text)	Secure data throughout the whole lifetime	[11]
11	Authenticated Key Exchange Scheme for Efficient Security with CCBKE	Improve efficiency by dramatically reducing time consumption and computation load	[17]

Table 6.1 Issue wise Solution Approaches & Result

Issue 2:- Data Leakage and weakness in cloud

S.No.	Solution Approach	Results	Ref.
12	3 Dimensional Security.CIA (Confidentiality, Integrity, and Availability)	Overcoming many existing problem like denial of services,Data leakage	[15]
13	Three proposed enhancements to that standard cloud service model which are Virtual Private Storage Proxy, Remote Integrity Monitoring and Encrypted Computational Streams.	Improve the adoption rate of the cloud for critical business services. Improve privacy, confidentiality, and integrity	[20]

Table 6.2 Issue wise Solution Approaches & Result

Issue 3:- Data integrity problem in the cloud environment

S.No.	Solution Approach	Results	Ref
14.	Data confidentiality and integrity verification using user authenticator scheme.	Solve integrity problem in the cloud environment	[5]
15.	Data confidentiality Approaches: Encryption and querying encrypted data and trusted Computing. Data accessing approaches are Private Information Retrieval[PIR]	Designing new protection techniques as well as building secures database services.	[2]
16	3)Provide a Cloud Storage Data Architecture,involves three different entities. Client, cloud service providers(CSP) and Trusted Third Party(TTP)	Reduce the data block access, and amount of computation on the server and client.	[3]
17.	Integrity layered architecture of a typical cloud based on MAS architecture consists of two main layers cloud resources layer and MAS architecture layer	Backup cloud data regularly that provide reconstruct the original cloud data by downloading the cloud data vectors from the cloud servers.	[16]
18	Create fake tuples with uniform distribution with no distinct pattern.	Very efficient in terms of query result analyzing.	[4]

Table 6.3 Issue wise Solution Approaches & Result

Issue 4:- Data hiding in cloud Computing.

S.No.	Solution Approach	Results	Ref
19	Automatic DNA sequence generation for secured Cost-Effective Multi-cloud Storage	Secured cost effective multi-cloud storage (SCMCS) model	[8]
20	MCDB which uses Shamir's secret sharing algorithm with multi-clouds. MCDB adopted TMR techniques	Better addressing, data integrity, data confidentiality, and service availability.	[6]

Table 6.4 Issue wise Solution Approaches & Result

VII.   COMMON FINDINGS

Issue 1:- Security and privacy in cloud computing
❖ The best solution Approach is "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption" because this solution provides authentication, verification and encryption or decryption of data together.

❖ The worst Approach is Key Technologies because by using this approach Network transmission problem, Standardization problems occur.

Issue 2:- Data Leakage and weakness in cloud
❖ The best approach is 3 Dimensional Security because provides availability of data by overcoming many existing problem like denial of services, Data leakage.
❖ The worst approach is cloud service model because it having some risks.

Issue 3:- Data integrity problem in the cloud environment
❖ In third Issue the best approach is Cloud Storage Data Architecture because it reduce the data block access, and amount of computation on the server and client.
❖ Worst approach is the mechanism to create fake tuples with uniform distribution because for small databases this is not good.

Issue 4:- Data Hiding in cloud Computing.
❖ In Fourth Issue the best approach is MCDB which uses Shamir's secret sharing algorithm with multi-clouds because of Better Addressing and data Availability
❖ The worst approach is DNA Sequence Because It is time consuming.

VIII. SCOPE FOR THE WORK IN AREA
❖ New combination of different method with cryptography technique enhance the security of cloud computing.
❖ 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. Because of this problem, raises many new security challenges which have not been well understood.
❖ Protect data through the unsecure networks like the Internet; using various types of data protection is necessary.Investigate new strategies to improve the efficiency of symmetric-key encryption towards more efficient security-aware scheduling.
❖ PCA algorithm for face recognition and algorithm having higher recognition rate appears due to the highercomplexity of these algorithms. It's difficult to apply to encrypted domain.

IX. CONCLUSION

The review of 20 research papers has been carried out in the area of Cloud Computing Security to investigate and find out current challenges and scope of work. After the review, we found issues were Data Hiding, Data Leakage which should be given proper concern, when the enhancement of security takes place. These papers are a survey of different security issues that affect the cloud environment and related work that carried out in the area of integrity. Propose of these models are to reduce the security risks that occurs in cloud computing and improve system reliability.

We were found many issues like data leakage, data hiding, Data integrity, data confidentiality can solved by Data confidentiality and integrity verification using user authenticator scheme, Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing, Implementing Digital Signature with RSA Encryption etc. which we review in 20 research papers.

The exhaustive review could finally lead to extract findings in the area of Cloud Computing Security, strengths and weaknesses and scope of work during M. Tech 1st semester Research work.

REFERENCES

[1]   Mr. PrashantRewagad&Ms.YogitaPawar, 2013, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", IEEE International Conference on Communication Systems and Network Technologies, 978-0-7695-4958-3/13, 978-1-4577-1964-6/12, pp. 437-439
[2]   DivyakantAgrawal, Amr El Abbadi, ShiyuanWang ,2013, "Secure and Privacy-Preserving Database Services in the Cloud",IEEEICDE Conference 2013, CNS-1053594 and IIS-1018637, 978-1-4673-4910-9/13, pp.1268-1271

[3]   RajkumarChalse, AshwinSelokar&ArunKatara, 2013, "A Nesw Technique of Data Integrity for Analysis of the Cloud Computing Security", 5th International Conference on Computational Intelligence and Communication Networks, 978-0-7695-5069-5/13, pp.469-473

[4]   PuyaGhazizadeh, Ravi Mukkamala& Stephan Olariu, 2013, "Data Integrity Evaluation in Cloud Database-as-a-Service", IEEE Ninth World Congress on Services, 978-0-7695-5024-4/13, DOI 10.1109/SERVICES.2013.40, pp.280-285

[5]   V.Nirmala, R.K.Sivanandhan& Dr. R.Shanmugalakshmi, 2013, "Proceedings of 2013 International Conference on Green High Performance Computing", India, 978-1-4673-2594-3/13

[6]   Mohammed A. AlZain& Ben Soh and Eric Pardede, 2013, "A New Approach Using Redundancy Technique to Improve Security in Cloud Computing", pp. 230-235

[7]   GurudattKulkarni ,JayantGambhirGurudattKulkarni , JayantGambhir, TejswiniPatil&AmrutaDongare, 2012, "A Security Aspects in Cloud Computing", Journal of Engineering Science and Technology (IJEST), pp.447-450

[8]   D.Sureshraj&Dr.V.MuraliBhaskaran, 2012, "AUTOMATIC DNA SEQUENCE GENERATION FOR SECURED COST-EFFECTIVE MULTI -CLOUD STORAGE", IEEE.

[9]   Su Qinggang& Wang Fu, 2012, "Study of Cloud Computing Security Service Model" , IEEE the information security industrialization project, National Development and and m Commission, No. [2010] 3044.

[10]   EmanM.Mohamed ,SherifEI-Etriby&Hatem S. Abdelkader, 2012, "Enhanced Data Security Model for Cloud Computing" , IEEE The 8th International Conference on Informatics and Systems (INFOS2012) - 14-16 May Cloud and Mobile Computing Track, pp. cc-12 – cc-17

[11]   Zhongbin Tang, Xiaoling Wang, Li Jia, XinZhang,Wenhui Man, 2012, "*Study on Data Security of Cloud Computing*", 978-1-4577-1964-6/12

[12]   Ling Lang & Lin wang, 2012, "Research on cloud computing and key technologies", IEEE International Conference on Computer Science and Information Processing (CSIP), 978-1-4673-1411-4/12, pp.863-866

[13]   SubaSurianarayanan&T.Santhanam, 2012, "Security Issues and Control Mechanisms in Cloud", Proceedings of 2012 International Conference on Cloud Computing, Technologies, Applications & Management 97 8-1-4673-4416-6 /12, pp.74-76

[14]   GebeyehuBelayGerbremeskel, ChenglingWang&Zhongshi He, 2012, "The Paradigm Integration of Computation Intelligence Performance in Cloud Computing Towards Data Security", IEEE 2012 Fifth International Conference on Information and Computing Science, 2160-7443/12, pp.19-22

[15]   Parikshit Prasad, BadrinathOjha, Rajeev Ranjanshahi&AbhishekVaish, 2011, "3 Dimensional Security in Cloud Computing", 978-1-61284-840-2/11, pp. 198-201

[16]   Amir Mohamed Talib, RodziahAtan, Rusli Abdullah &MasrahAzrifah, 2011, "CloudZone: Towards an Integrity Layer of Cloud Data Storage Based on Multi Agent SystemArchitecture", IEEE Conference on Open Systems (ICOS2011), September 25 - 28, 2011, Langkawi, Malaysia, 978-1-61284-931-7/11, pp. 127-132

[17]   Chang Liu, Xuyun Zhang, Jinjun Chen & Chi Yang, 2011, "An Authenticated Key Exchange Scheme for Efficient Security-Aware Scheduling of Scientific Applications in Cloud Computing", Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, 978-0-7695-4612-4/11, pp.372-379

[18]   Uma Somani, KanikaLakhani, Manish Mundra , 2010,"Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC) ,pp.211-216

[19]   Chenguang Wang &Huaizhi Yan, 2010 , "Study of Cloud Computing Security Based on Private Face Recognition", IEEE *Basic Research Program of Beijing Institute of Technology* ,978-1-4244-5392-4/10 ,

[20]   Robert E. Johnson, 2010, "Cloud Computing Security Challenges and Methods to Remotely Augment A Cloud's Security Posture" , 978-0-9564263-8/3 , pp. 179-181