

Security Issues in Cloud Computing

Anchal Pokharana, Chandigarh University, Punjab, India anchalpokharana258@gmail.com

Asmita Singh, Govt College of Engineering & Technology, Bikaner, India, asmita.singh49@yahoo.com

Hema Shekhawat, Chandigarh University, Punjab, India hemashekhawat.cse@cumail.in

Abstract—cloud computing is a internet computing, a worldview, intended to outfit the intensity of systems of PCs and correspondences in a savvy way. Cloud computing gives a versatile ability to serve a wide and always extending scope of data preparing needs, including business, government, training and that's only the tip of the iceberg. The fundamental Problem with Cloud Computing is the Cloud information protection, information security and the viable Implementation of Cloud on the Network. Distributed computing forward the application programming and databases to the tremendous server farms, where the administrations on the information and information administration may not be completely dependable. Issue in this is essentially Clouds have single engineering for security concern yet have a huge number of clients with various requests and In this we have to expand accessibility of information on request by conquering these current issues like Data Leakage, Data Integrity and information Privacy Protection. To comprehend about distributed computing security, a survey procedure is received in this paper to audit 20 look into paper around there. After audit process, four essential key issue were discovered "Security and protection, Leakage of information and shortcoming, Data honesty issue and Data Hiding in distributed computing," which need to upgrade the Security in mists to show signs of improvement Data openness over cloud organize. A few arrangement approaches have been found in these exploration papers. The result of the audit was as different discoveries, found under different key issues. calculations and techniques used to take care of specific research issue are incorporated into discoveries, alongside their qualities and shortcomings and the extension for the future work in the territory.

Key words: Security issue, Data Integrity, Privacy, CSP, Data Leakage, Data Hiding, CI, AES Encryption, IaaS, PaaS, SaaS

I. INTRODUCTION

Cloud computing is a worldview in which data is for all time available in servers on the web and can be accessible from anywhere. Cloud processing lessened capital consumption, operational dangers, many-sided

quality and upkeep, and expanded scalability. Virtualization is the heart of cloud computing. Virtualization is a structure or procedure of separating the assets of a PC into numerous execution conditions. By vitalizing the machine, we can run a few working frameworks (and the majority of their applications) in the meantime.:

1. Software as a Service (SaaS): Foundation as an administration (IaaS) is a type of distributed computing that gives virtualized registering assets over the web. IaaS is one of the three primary classes of distributed computing administrations, nearby programming as an administration (SaaS) and stage as an administration (PaaS). The IaaS supplier additionally supplies a scope of administrations to go with those foundation segments. These can incorporate itemized charging, observing, log get to, security, stack adjusting and bunching, and in addition stockpiling flexibility, for example, reinforcement, replication and recuperation.

2. Platform as a Service (PaaS): Stage as an administration (PaaS) is a total improvement and arrangement condition in the cloud, with assets that empower you to convey everything from basic cloud-based applications to complex, cloud-empowered endeavor applications. You buy the assets you require from a cloud specialist co-op on a compensation as-you-go premise and access them over a protected Internet association.

3. Infrastructure as a Service (IaaS): Framework as an administration is a moment figuring foundation, it is overseen over the Internet. It rapidly scale here and there as indicated by request and pay just for what we use. IaaS maintains a strategic distance from the cost. It diminish many-sided quality of purchasing and dealing

with our own physical servers and other datacenter infrastructure. It gives essential stockpiling and figuring abilities as institutionalized administrations over the system.

Since cloud computing is an utility accessible on net, so it realizes comfort and productivity issues, as well as extraordinary difficulties in the field of information security and security insurance and numerous more like: information robbery and spillage, Data secrecy, Integrity Verification, validation different programmers assaults are raised. Cloud registering is an incredible difference in data framework, Security turns into a bottleneck of distributed computing advancement, guaranteeing the security has been viewed as one of the best issues in the improvement of distributed computing.

II. REVIEW PROCESS

A literature review is very important for the depth knowledge about the research area. We have used five stage review process which includes all the detailed version of work. These stages are designed to make the process simple and under stable. The stages were:-

Stage 1 : “feel” of work

The details to be checked before starting literature. Review briefly and classify them according to requirements. this phase is not providing the big picture of work.

Stage 2: Get the “big picture” of work

Selected research papers are divided into groups according to common problem, issues & sub areas. By reading the Title, Abstract, introduction, conclusion and section and sub section headings, It is required to find out the answers to specific questions.

Stage 3: Get the “details” of work

Stage 3 manages going top to bottom of each research paper and comprehend the subtle elements of procedure used to legitimize the issue, legitimization to criticalness and curiosity of the arrangement approach, exact inquiry tended to, real commitment, scope and restrictions of the work displayed.

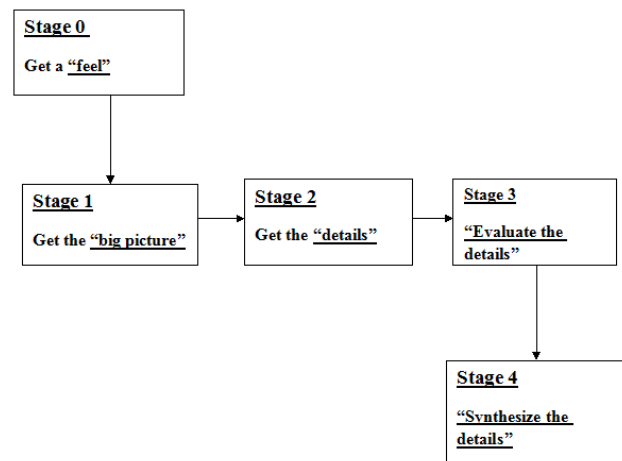


Fig: 2.1 Review Process used

Stage 4: “Evaluate the details” of work

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 5 : “Synthesize the detail”

Stage 5 deals with evaluation of the details presented and generalization to some extent. This stage deals with the concepts and the results given and evaluated by authors. this stage provides synthesis of the data.

III. VARIOUS ISSUES IN THE AREA

20 research papers have been reviewed on Cloud Computing Security. Some of the common issues are found in the area of cloud security. which are listed below.

- 1) **cloud computing Data privacy and security**
- 2) **cloud computing Data Leakage and weakness**
- 3) **Data integrity in cloud environment**
- 4) **Data hiding problem in cloud Computing**

IV. ISSUE WISE DISCUSSION

Issue 1:- Data privacy and security in cloud computing

Security and Privacy in Cloud Computing is one of the issue, some approaches have been used to over come with this issue. These are 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

This is another issue in cloud computing. 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.

In this Provide Data privacy and respectability check utilizing client authenticator plot. Join the information honesty check system alongside scrambling component [12]. The private information are enveloped twice to guarantee security by information spillage occurs at the serve side. In Cloud Storage Data Architecture, an information stockpiling administration includes three distinct elements. Cloud specialist organization (CSP) and Trusted Third Party (TTP).

Issue 4:-Data hiding in cloud Computing.

Programmed DNA succession age MCDB with TMR strategies (Redundancy Technique)with consecutive strategy .Result is anchored financially savvy multi-distributed storage (SCMCS) show in distributed computing, better tending to, information uprightness, information secrecy, and administration accessibility. This model is more anchored in securing client's information. System in cloud for information stowing away is two capacities to make counterfeit traits Input capacity and Generating capacity that are occasional capacity .Research protect the arrangement by giving proposed engineering and graphical portrayal

V. ISSUE WISE SOLUTION APPROACHES USED

The solution approaches under these four issues have been described in the tables which includes all the basic information like hardware, software, parameters and variables used in papers, along with quantitative results obtained. The Comparative analysis between various solution approaches are shown in tables.

VI. ISSUE WISE DISCUSSION ON RESULTS

Issue1:-Data privacy and security in cloud computing

S.No.	Solution Approach	Results	Ref
1.	Enhanced Data Security Model with efficient feathers'	Provides Highest security, Less time to encrypt data. Retrieval of data become faster.	[1]
2.	Private Face Recognition	Technique provides correct result under non-encrypted conditions.	[9]
3	Computational Intelligence (CI) with its Dynamic Application	Prediction of problem and the incoming status	[14]
4	Digital Signature with RSA Encryption Algorithm.	Super computing services on low cost.	[18]
5	Enhanced Data Security Model Digital Signature with Diffie Hellman Key Exchange and AES Encryption	Encryption, decryption of data Authentication, verification of the data all together	[10]
6	Control mechanisms : 3 migration phases are classified. These are pre-migration, in operation and termination.	Trustful environment developed between the client and the CSP	[13]
7	Security service model with Key Realization Technology	A secured model involves standardization, supervision model, laws & regulations	[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:	Designing new protection	[2]

	Encryption and querying encrypted data and trusted Computing. Data accessing approaches are Private Information Retrieval[PIR]	techniques as well as building secures database services.	
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 methodology is Cloud Storage Data Architecture since it decrease the information square access, and measure of calculation on the server and customer.
- ❖ Worst approach is the system to make counterfeit tuples with uniform circulation in light of the fact that for little databases this isn't great.

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 blend of various strategy with cryptography procedure improve the security of distributed computing.
- ❖ Cloud figuring moves the application programming and databases to the substantial server farms, where the administration of the information and administrations may not be completely reliable. In light of this issue, raises numerous new security challenges which have not been surely knew.
- ❖ Protect information through the unbound systems like the Internet; utilizing different kinds of information assurance is necessary. Investigate new techniques to enhance the effectiveness of symmetric-key encryption towards more proficient security-mindful planning.

- ❖ PCA calculation for confront acknowledgment and calculation having higher acknowledgment rate shows up because of the higher complexity of these calculations. It's hard to apply to scrambled area.

IX. CONCLUSION

The survey of 20 research papers has been completed in the territory of Cloud Computing Security to research and discover ebb and flow difficulties and extent of work. After the survey, we discovered issues were Data Hiding, Data Leakage which ought to be given appropriate concern, when the upgrade of security happens. These papers are an overview of various security issues that influence the cloud condition and related work that did in the region of trustworthiness. Propose of these models are to decrease the security hazards that happens in distributed computing and enhance framework unwavering quality.

We were discovered numerous issues like information spillage, information concealing, Data respectability, information privacy can illuminated by Data secrecy and honesty confirmation utilizing client authenticator plot, 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 and so forth which we audit in 20 look into papers.

XI.REFERENCES

- [1] Sumit Kumar, Nishant Sharma, Gagan Sharma "Li-Fi Technology in Wireless Communication" Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, Volume-4 | Issue-3 , June 2017, URL: <http://www.ijtrd.com/papers/IJTRD8584.pdf>
- [2] Kumari Neha et al. "Using Reconfigurable Directional Antenna in MANET." *Procedia Computer Science* 125 (2018): 194-200.
- [3] Kumai, Neha, et al. "Mobile ad hoc networks and energy efficiency using directional antennas: A Review." *Intelligent Computing and Control Systems (ICICCS), 2017 International Conference on*. IEEE, 2017.
- [4] Singh, VK, Kumar, R. "Multichannel MAC Scheme to Deliver Real-Time Safety Packets in Dense VANET". *Procedia computerscience* ISSN 1877-0509, 2018.
- [5] S. Kapil et al, et al. "Analysing the Role of Risk Mitigation and Monitoring in Software Development (2018).