Enhanced Secured Multi cloud using Technical Environment and Regulatory Framework

Sri Vidya CH
Student, M.Tech CSE Dept,
Institute of Aeronautical Engineering,
Hyderabad, AP, India.

N. Chandra Sekhar Reddy, Ph.D
Professor, CSE Dept.,
Institute of Aeronautical Engineering,
Hyderabad, AP, India.

G. Praveen Babu
Associate Professor,
Dept., of CSE School of Information Technology,JNTU
Hyderabad, Andhra Pradesh , India

ABSTRACT
Cloud Computing is the rising generation key platform for sharing the resources like software as a service, infrastructure as a service, and platform as a service. In future all IT enterprises migrate into cloud platform. Cloud server exchanges the messages for remote location users with the help of multi cloud architectures. Security issues are generated in data transmission. Day by day new vulnerabilities are discovered in cloud computing. Previous cloud development provides the security in limited dimensions with the help of application logic. It not sufficient for control the all different attackers. This is not efficient and scalable environment. It's not optimal approach [1].

Increase the range of cloud computing security and detect the attacks in deep degree manner. It provides highly safe results with good data protection. Here we concentrate on two dimensions. Those dimensions are application logic view and regulatory framework. Its have excellent security properties. This approach provides the excellent security compare to previous approaches. We proved different properties like good integrity and confidentiality compare to previous approaches [1][2].

General Terms
Multi cloud, Privacy, Confidentiality

Keywords
Cloud Computing, Multi cloud architectures, Security constraints, Data Protection model

1. INTRODUCTION
Cloud is the category of parallel and distributed computing. It is the collection of interconnected and dynamical virtualized system. Many number of cloud service providers are available in market. Those service providers are Amazon [4], IBM and HP. Different number of consumers are access the different number of clouds services. This paper concerned with Software as a service. Previous cloud data storage security solutions identified with the help of technical environment. That is called application logic. It controls the less number of attackers. New different weak spots are available. In those weak spots attackers it may chance to enter and create the risks and problems. It's not possible to control the all dimensions of attackers [2][3].

Some more number of security properties we add in technical solution environment and increases the detection of attacker's in cloud data storage areas. Newly we add the homomorphic encryption procedures for increasing the security. This procedure performs based on two concepts. Those concepts are technical perspective and secure multi party computation verification perspective. These two provides the good excellent security compare to previous approaches [1][2].

2. RELATED WORK
Field of Cloud computing is in early childhood stage related to implementation and usage. Cloud computing can provide the assurance to reduce the investment and expenditure of hardware and software. Cloud computing provide the services to the users over the internet. Cloud computing related services already used different applications of databases. Those databases are e-commerce and medical records. Now here we take the concern related security constraints in cloud environment [1].

Different categories of security concerns are available. Those security concerns are traditional security, availability and third party control. Previously trusted computing technology was introduced for providing the security. It works based on integrity measurements. It enables the process of trusted execution. It does not provide the reliable data delivery solutions. Trusted computing mechanism is not efficient. It is not accurate approach for total data delivery [4].

After some days new approach is came into market. That is called Cryptographic co-processors. It's provided the advantages like high security and tamper resistant execution environment. This is related hardware security approach. It executes the programs effectively. It does provide the services to execute limited storage and memory programs with high expensive cost services. It takes more time for providing the response. This is not scalable cloud computing infrastructure [6]. Next another new approach secure cloud computing provide the file downloading services. Two parties of people mutually communicated without third party start the distribution of the services implementation process. Encrypted data formats provide the secure solution in data transmission environment. It provides the distrustful solutions [1] [2].

Increase the security services with the help of homomorphic encryption techniques in cloud. Original file was encrypted then we perform additionally multiplication with some noisy data. Whenever starts the outsourcing file add the signature and start the data transmission process. After deliver the file of information performs the verifiability operation. Data is corrupted total file is not deliver accurately in destination. Fully Homomorphic encryption approach also is not sufficient for providing the guaranteed data transmission results [3][4].

Increases the data delivery solutions then we add the new technology. It consists of multiple data owners. Multiple owners are works as a multiple parties. Verifies the data in

different locations of environment provide the perfect results with the help of third parties implementation process. This is completely generalized verification process. It controls the number of attackers are more compare to previous approaches here in implementation. Then present cloud works as a trusted cloud [4][3].

Apply the Advanced Encrypted standard increase the complexity in encryption process. Start the outsourcing operation applies the SPED technology. It enables the homomorphic encryption process in transmission and verifiability follows the boolean circuits. It generates the result like true or false. In verification time new middleware is added in our implementation process. It expands the communication process with parallel computing environment [1]. Parallel process verification generate with the help of co-processors. It is not sufficient we add the virtualization process detect the attackers efficiently. It's also expensive.

Now we enter multi cloud environment for increases the service distribution as a quality with reduced cost. Tamper proof software configure into multiple cloud servers. One cloud server works as a un-trusted server then we collect the remaining packets from other neighbor cloud server. New protocols concentrate on multiple clouds for downloading the original file of information. These two clouds also sometimes it does not provide the efficient solution [1] [2].

Attacker identifies the access activities from cloud data storage. Multiple times monitor the same process by attackers. It may chance to get the logic and perform the different operations like alter. Honest user's activities are not control in cloud server with the help of present cryptographic techniques. New risks are generated in cloud server environment [1] [2].

New Cross channel attackers are entered in virtual machines. Through cross channel attackers also it possible to accesses the original user data. All authorized users of confidential data accessed by the attackers. This approach is not efficient for detection of all attackers.

Existing System:
In Different number of cloud servers deploy the different number of application logics. Train the cloud servers application logics identifies the measures. Select the best application logic from n cloud server's logics and spread into remaining cloud servers. Automatically security related enhancements we produce here. This is technical solution.

Drawbacks:
In cloud server different numbers of flaws are generated here. Those flaws are internal and external threats. The above all proposals are related different detection approaches flaws. The above all proposals are not provide the perfect solution. Now in this paper we create the new proposal for better security solution.

3. PROBLEM STATEMENT

Previous enhancement of cloud security and privacy solutions considers technical requirements specification that is called application logic. It does not provide the security in all dimensions. It's have the less attacker detection skills. This present perspective is not sufficient for provide the integrity and confidentiality solutions. This perspective is difficult to detect the attackers. After implementation of technical perspective also in cloud some weak areas are available. It does not provide perfect security guarantee [1].

Now In this paper we add the technical and regulatory requirements for increasing the cloud security. Two combined requirements provide the integrity results in downloading files of content. First perspective is effective application logic preparation. Second perspective is homomorphic encryption techniques implementation. This is related multiparty verification compilation approach. Combined two requirements related compilation approaches we configure and increase the security complexity[4][5].

4. PROPOSED SYSTEM:

Now here we concentrate on two kinds of functionalities in new architecture. This is we call as a co trusted model. Two different functionalities follow the two different processors. Identify the reports from different processors separately. All functionalities are trust then this platform is trusted platform. This kind of software prevents the all interferences problems in our implementation process. Here we prevent the interferences in two phases. Those phases are storage and execution also. Diagram fig:1 shows the new cloud security architecture. It provides confidentiality and integrity solution to users. This is the new enhancement we show with the help of implementation process. It is the future multi cloud security infrastructure. It provides the excellent security features with the help two combined requirements compliance [6] [7].

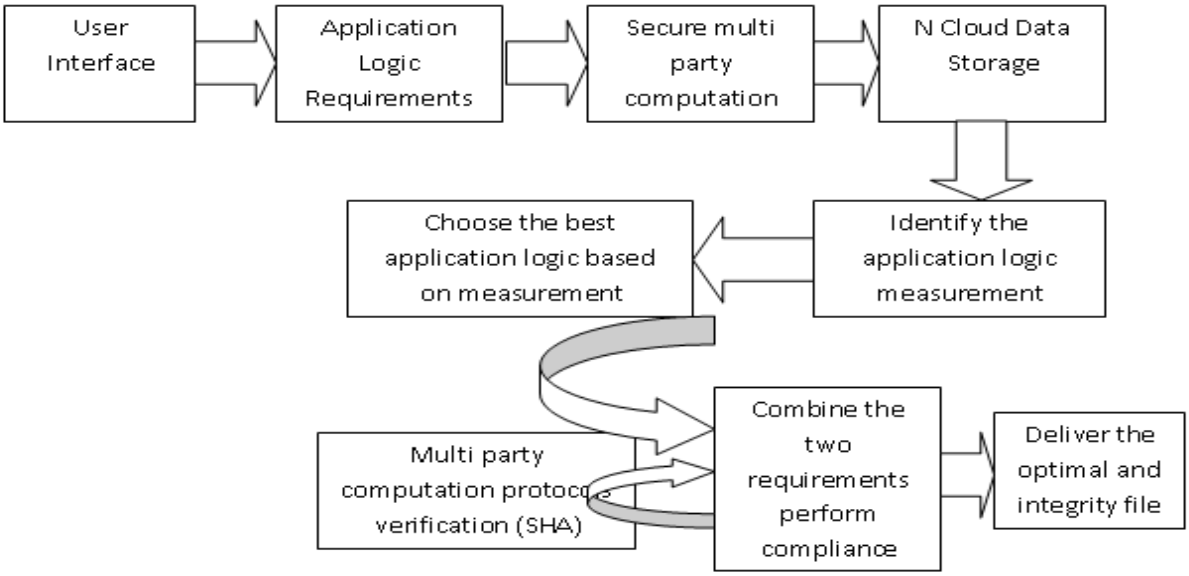

Fig 1: New cloud security architecture

Security cloud architecture contains different elements. Those individual elements working procedure we call modules.

Those modules are

1. System Model
2. Create the user interface for N cloud data storage servers.
3. Identify the application logic measurement
4. Multi Party protocol verification procedure
5. Combined two requirements compliance

4.1 System Model

We design the new cloud computing architecture with different requirements. Those requirements are perfect application logic and secure multi party verification. These two requirements provide the integrity file downloading purpose only. This kind of new compliance approach provides the efficient results [5] [7].

4.2 Create the user interface for N cloud data storage servers:

Identify the different dimensions of functionality and develop the new security cloud interface logic. Different cloud data storage servers have different cloud interface logics in our implementation.

4.3 Identify the application logic measurement:

Start the training process based on downloading operation. Identify the cloud measures based on interface logics. Different application logics have different measures. Verify the different measures choose the best measurement of cloud data storage. Its control the attackers without corrupt. Every time cloud satisfies availability property using cloud data storage application logic [6] [7].

4.4 Multi Party protocol verification procedure

Every user is verified by the multi party protocols in downloading time. Multi party protocols verification follows the homomorphic encryption schemes. It controls the more number of attackers. It is complex procedure to enter the any kind of attacker. It contains excellent properties for detection of attackers. Compile the properties one by one sequentially. This approach provides in-depth of verification results implementation process [8] [3].

4.5 Combined two requirements compliance

Measurement of different application logics choose the best application logic (4.3) and perform the sequential compilation approach (4.4).

Two processes at a time we perform and control the attackers efficiently. It gives the accurate solution for detection of attackers [2] [6].

Compilation procedure decides status of user, whether we need to allow or deny the request for access the file content. We distribute the services efficiently as a quality of service mechanism approach representation process. This is best way to increase the security and privacy environment process in our implementation [7][8][9].

5. ELLIPTIC CURVE VERIFICATION ALGORITHM:

Input: The following inputs are needed:

1. A's authentic public key PA and the domain parameters (p;a;b;G;n;h).

2. The signed message M

3. The ECDSA Signature (r,s)

Output: True if signature is valid and False otherwise

Actions: 1. Verify that r, s € { 1,2,……n-1}

2. If check fails output false and terminate

3. Sinv=S-1 mod n
4. U1= H(hash code is generated)
5. Signature is verified
6. True
7. Otherwise
8. False

6. PERFORMANCE EVOLUTION GRAPH

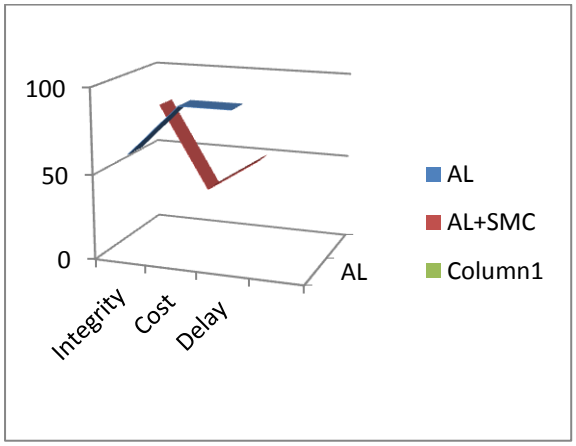

Fig 2: Result

Graph fig:2 explains about cloud with different QoS parameters. Those parameters are Integrity, cost and delay. Existing system performance levels are less compare to proposed system.

7. CONCLUSION

We use the multiple cloud architectures for increasing the security and privacy results. Previous multi cloud architectures we consider the single dimension only. It not provides the significant security services information. Security properties are missing some difficulties and issues are available.

In this new multi cloud architectures added the some more dimensions automatically increases the security features. It provides the integrity features implementation. Application logic features and security multi party protocol environment increases the security features. It provides the excellent security environment compare to previous approaches.

8. FUTURE WORK

Next for multi cloud security we offer one time passwords content. Security enhancement its possible with of firewalls also.

9. REFERENCES

[1] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, and Ninja Marnau, Security and Privacy-Enhancing Multi cloud Architectures, 2013

[2] Sven Bugiel, Stefan N□urnberger, Ahmad-Reza Sadeghi, Thomas Schneider ,Twin Clouds: Secure Cloud Computing with Low Latency, 2009

[3] Meiko Jensen, J¨org Schwenk, Jens-Matthias Bohli, Nils Gruschka, Luigi LoIacono Security Prospects through Cloud Computing by Adopting Multiple Clouds, 2011

[4] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, Jesus Molina ,Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control, 2009

[5] Hassan Takabi and James B.D.Joshi, Gail-JoonAhn Security and Privacy Challenges in loud Computing Environments, 2010

[6] Jeff Naruchitparames and Mehmet Hadi G¨unes, Enhancing Data Privacy and Integrity in the Cloud, 2011

[7] R. Thandeeswaran1, S. Subhashini1, N. Jeyanthi1, M. A. Saleem Durai, Secured Multi-Cloud Virtual Infrastructure with Improved Performance, 2012

[8] Mr.K.Saravanan #1, M.Lakshmi Kantham #2 , An enhanced QoS Architecture based Framework for Ranking of Cloud Services, 2013.

[9] Michael Smit, Mark Shtern, Bradley Simmons, and Marin Litoiu, Enabling an Enhanced Data-as-a-Service Ecosystem, 2011