International Journal of Advanced and Innovative Research (2278-844)/

Volume 7 Issue 11

Secure Data Sharing In Cloud Computing Using Revocable-Storage IBE

[1]Sunita Palleti, [2]CH. Suresh Kumar

[1]Research Scholar, [2]Assistant Professor, Department of Computer Science & Engineering

KODADA Institute of Technology & Science For Women, Kodad

Abstract: ***Cloud computing is a distributed system which works with the multiple component to provide a processing of users input request. The input request can be of data storage, data access and utilizing the data in real time with different available model. Cloud computing consist of multiple layers and model of performing the processing of large amount of data. Different areas of research are available which includes the data security, authentication, accessibility and identity based data utilization. Data usage over the cloud helps in fast and scalable usage of data. Cloud data is accessible with various platform includes web and mobile units. Thus the availability of data and its accessibility increase the vulnerability over the data. This topic is required in further research to enhance the security over the cloud data and accessing them on secure channel. This research discuss about the algorithm which enhance the security with hybrid level of security model. An end to end communication protocol with enhances cryptography and data auditing approach is presented. Thus the algorithm shows the efficiency over the traditional security mechanism. The proposed algorithm works experimented over the java platform using Apache server. The Computation parameter which is taken for comparison is computation time, computation cost, and bandwidth and Energy consumption in data packet transmission. The experiment performed over the proposed security and reliable model shows the efficiency of proposed approach over the traditional solution of data processing in cloud computing distributed environment.***

Keywords:-Cloud Security, Energy Optimization, Data transmission, Distributed Solution, Data Accessing, Bandwidth Utilization.

1. INTRODUCTION

Cloud computing is an on-demand computing service in which various services and resources are provided to the user on on-demand basis. In that various internet base services are provided to the user, and user need to only for those services which he want to use. In cloud computing there is a shared pool of services in which user can access any service that he wants. But in cloud computing user's data resides in cloud server. This is vulnerable to risk and requires an efficient handling mechanism to maintain integrity of the data. Thus secure storage for the users data is required in cloud, there are various techniques are presented by the various researchers to provide secure storage mechanism for the cloud data, in that various cryptography based schemes are used to provide secure cloud storage for the data. Schemes like ABE (Attribute Based Encryption) are used to provide a secure storage for the clouds data.

In cloud a large amount of data is stored which contains confidential information. Data like PHR (personal health records) is generally stored at third party environment which contains confidential concerns, thus a secure handling for that data is required, and a secure cloud storage technique for the PHR data is presented in this dissertation which provides an enhanced functionality to the user's data.

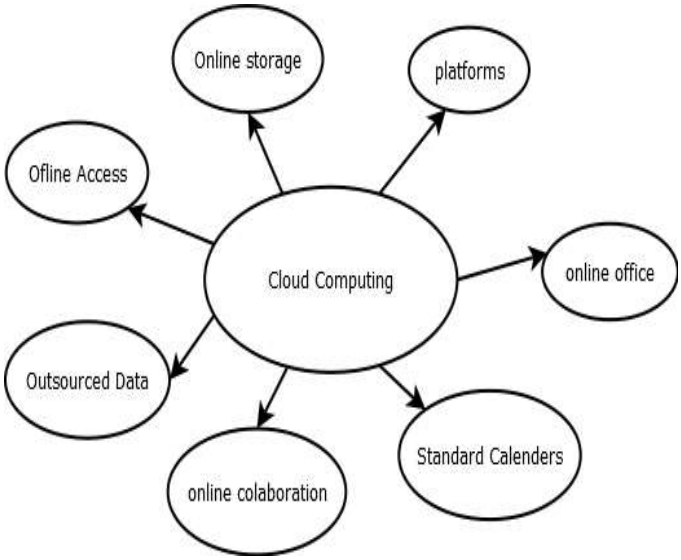

Figure 1.1: Cloud Computing Environment.

Cloud Security

In cloud computing data introduced from the various fields like medical.

Cloud computing security or simply cloud security is field in cloud computing which deals with all the security issues in cloud computing. In cloud computing user's data resides in third party cloud servers which vulnerable for various online threats. In that scenario all the auditing tasks are performed by the third party auditor (TPA). But there various types of attacks are performed by the unauthorized users or intruders to access that data. That contains confidential, private information of the users. Thus security of that data is the biggest concern. There are various cryptography based techniques like ABE, CP-ABE; KP-ABE etc. are used to provide security for that data

Cloud computing security or, more simply, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centres. Organizations use the Cloud in a variety of different service models SAAS IAAS & PAAS and deployment models (Private, Public, Hybrid, and Community). There are various security issues concerns related with distributed computing however these issues fall into two general classes: security issues looked by cloud suppliers (associations giving programming , stage , or framework as-a-benefit through the cloud) and security issues looked by their clients (organizations or associations who have applications or store information on the cloud).

2. LITERATURE REVIEW

Soumya Parvatikar, Puja Prakash, Richa Prakash, Pragati Dhawale, S.B. Jadhav [1]

Private well-being document (PHR) is in most cases noticeable as a patient-pushed model of sharing well-being related expertise. But protection is the prime concern while storing data in an outsourced atmosphere. If the full entry of the PHR information is supplied to the patients that simply waste for him to preserving that knowledge. However there are disorders like dangers of the security introduction scalability in the key management and many others are the difficulties in delivering a nice-grained service to the consumer and provide a cryptographically approved provider. To provide a great-grained and comfortable access manage, an ABE (Attribute founded Encryption) service is used to encrypt sufferers knowledge. In that no longer handiest a at ease mechanism is provided but additionally provide a high-quality grained carrier and partition the patients data into various protection domains. That reduces the complexity in the administration. A cozy framework to share sufferer's information over the outsourcing environment is furnished, that helps to share patients PHR knowledge over the internet, which can be used within the therapy of the various ailments. A comfortable world access is furnished to the opposite users like doctors to uses this data for the remedy of the illnesses.

Saipavan Konda, Niranjan Reddy P [2]

Personal wellness report (PHR) is sufferer pushed model of individual wellbeing records sharing, which is commonly outsourced and put into the 0.33 occasion server, for example, cloud provider. There is among the biggest safety considerations, in view that personal health documents are saved in 13 occasion server in the untrusted atmosphere. Consequently there may be various cryptography strategies can be used to encrypt that information before outsourcing it. That provides patients a manage over the access of their

information. A sufferer driven mannequin and an entry control framework to preclude unauthorized entry for the PHR knowledge. An Attribute based encryption process and a One Time Password (OTP) centred technique is used to furnish better performance to relaxed outsourcing of the information. Dynamic entry manipulate framework is provided to the patient for secure outsourcing to their knowledge.

A.Yoshitaka,S.Chujyou,H.Kato [4]

Japan is likely one of the countries where way forward for nation is probably the most raised in the world. Not handiest bettering the social medication services but additionally improving in social wellbeing care protection framework, person actions within the social services and many others. Thus PHR (individual wellness record) of the every sufferer can be used to provide expertise about the diseases which used to medication or in treatment of those ailments. Wellness knowledge evaluation is performed to furnish higher information in regards to the health care data. That digital health care data can be used through the general population to and the medical authorities to fortify the wellness care offerings. But when put that knowledge available to the general population can be cause serious protection difficulty for the patients personal data. A appropriate administration and management is required to furnish a secure entry for that information.

C. J. Wang, X. L. Xu , D. Y. Shi , W. L. Lin [5]

As a rising patient-driven mannequin of wellness information sharing, cloud-centered individual health file (PHR) framework holds top notch assurance for enticing patients and guaranteeing more compelling conveyance of medicinal offerings. A novel sufferer-driven cloud-based comfy PHR framework, which allows patients to soundly retailer their PHR information on the 13 get together cloud server, and above all share their PHR information to an broad form of customers, together with medical services supplier like doctors and attendants, loved ones or companions. To cut back the important thing administration multifaceted nature for doctors and purchasers, we partition the customers within the cloud-based PHR framework into two safety areas named open space and individual area. Now not the identical as past Cloud-based PHR framework, PHR owners scramble their PHR knowledge for common society space utilizing determine content procedure property situated encryption plan, even as they encode their PHR expertise for the man or woman area making use of mysterious multi-recipient personality centered encryption plan. Simply approved purchasers whose qualifications fulfil the predefined figure content material procedure or whose personalities fit in with committed characters can decode the encoded PHR understanding, where figure content material association or committed personalities are inserted within the scrambled PHR understanding. Vast investigative and exploratory results are exhibited which show the patient-driven cloud-based comfortable PHR framework is comfortable, versatile and productive

P. Van Gorp , M. Comuzzi [6]

Individual well-being records (PHRs) have to stay the lengthy lasting property of sufferers and must be showable to the licensed customers or like doctors and different healthcare authorities. In present situation PHR makes a speciality of the ordinary information sharing corporations and provide international healthcare framework. My PHR computing device, a sufferer- pushed mannequin is provided, that presents a more desirable framework wellbeing records sharing. In that procedure not most effective the scientific understanding but in addition related expertise to that programming of PHR is also shared. In that procedure knowledge shared over the cloud which can be utilized with the aid of the various customers. Sufferers can access the information by the use of faraway virtual desktop. Deep rooted PHR information is offered to the patients, medical professionals, coverage businesses and many others. To get viable options for the illnesses.

WB Lober, B Zierler,AHerbaugh, SE Shinstrom, A Stolyar, EH Kim, And Y Kim [7]

Personal wellness documents (PHRs) are methodology to make patient centric health offerings. There is some work is required to furnish better wellness care offerings to the patients at house and difficulties in work procedure like have an effect on of the access of these records, psychological influence, physical have an impact on etc. The results of these healthy evaluation is used by the quite a lot of companies to furnish better health care offerings to the sufferers. That help in growth of the healthcare offerings and get to the bottom of the issues of the sufferers related to the well-being care services.

3. PROBLEM IDENTIFICATION

- In Existing system, there are following associate problems which are worked on our proposed work :
- AES-256 is quite common and easily available for hacker activity in case it desire to break.
- Existing accessing and storage scheme is slow in terms of computation time and process.
- Thus it exhibit high cost while storage of data, providing its availability to access.
- The existing algorithm use model which is still extension is required for proper loose coupling.
- Previous approach having limitation of accessing data from large structure of dataset.
- Highly indexed data structure is not taken in the base paper, which further need analysis of high end access.

4. PROPOSED METHODOLOGY

In order to computer the enhanced work from the study of previous algorithm here a proposed algorithm name EECC algorithm is proposed by us which is efficient while comparing with the existing ECC and MAC algorithm for the encryption and data storage security.

- The proposed work can be done in accordance of working with security and storage over the various available components. Data optimization over the network and to work on reducing better resource management and CRM investigation can be done in further proposed methodology.
- An advance accessing mechanism with process security is going to process in proposed approach with lexical storage and HECC security approach.
- The above algorithm pseudo code is executed at our implementation end and further the modules and sub algorithm which is being implemented at server end is discussed here.

Algorithm Pseudo Code

Input: User, File medical Data, Algorithm inputs, Apache framework.

Output: Cloud data storage, indexing, Algorithm parameter, Permission entity.

Steps:

Begin :

Initiate all the framework{

Loadall DataConfiguration();

Load userDB();

Load Server Scenario();

}

If(user input is valid?)

{

user input=key, input data & credentials

process Storage();

}else exit 0;

processStorage()

{

CompressiveSensing(Uinput);

Perform Lexical indexing OCs File();

Storage Order Gen();

FAccess();

}

FAccess()

{

Input string S;

Process DB indexing (S);

Process Indexing();

Storage Order();

OptResult();

}

The above algorithm Pseudo code is executed at our implementation end and further the modules and sub algorithm which is being implemented at server end is discussed here. Below are the detail description of various module and scenario presented in our work.

5. RESULT ANALYSIS

In this section, different observed result which is performed is presented. A statically analysis and graphical analysis using the existing as well as proposed technique is presented.

Experimental Setup

In order to evaluate the complete scenario and execution. The experiment is performed over the net beans using the cloudsim API with the planet lab workload. The workload is processed through the simulation environment with multiple VM and cloudlet data scenario.

The experiment scenarios get performed using the Java programming language over the multiple algorithm and proposed solution using the over utilized scenario of VM and given host.

Computing Parameter

There are mainly three parameter, which is taken for the comparison analysis is taken. Computing parameter such as computation time, computation cost and bandwidth consumption is observed.

Computation Time

Computing time is the time difference which is observed by subtracting final executing time to initial loading time. A time difference between both the times is observed and call as computation time.

Computing Time = Final Execution Time – Initial Time;

Ct=Fet-It;

Computation Cost

Computing cost is the total cost which can be observed by monitoring different usage resources and aspects such as bandwidth, data consumption, resources etc.

Bandwidth consumption

It is the total data consumption per unit of time which is taken by the token and complete access monitoring.

Bandwidth Consumption = Total Data Consumption/ Unit Time;

Bc = Tdc/Ut;

Statistical Analysis

In this section we will explain about the several calculations Performed over different algorithms.

Table 1.1: Comparison Computation Between Existing And Proposed Computation Time At Server End.

ALGORITHM NAME DATA SIZE	EXISTING ECC (SERVER END)	ENHANCE ECC (SERVER END)
5 MB	5654 ms	5654 ms
10 MB	4555 ms	4555 ms
15 MB	11890 ms	11890 ms

In the above table the computation over different files has been shown.

Table 1.2: Comparison Computation Between Existing And Proposed Computation Time At TPA End.

ALGORITHM NAME DATA SIZE	EXISTING ECC (TPA END)	ENHANCE ECC (TPA END)
5 MB	2311 ms	2311 ms
10 MB	1980 ms	1980 ms
15 MB	7123 ms	7123 ms

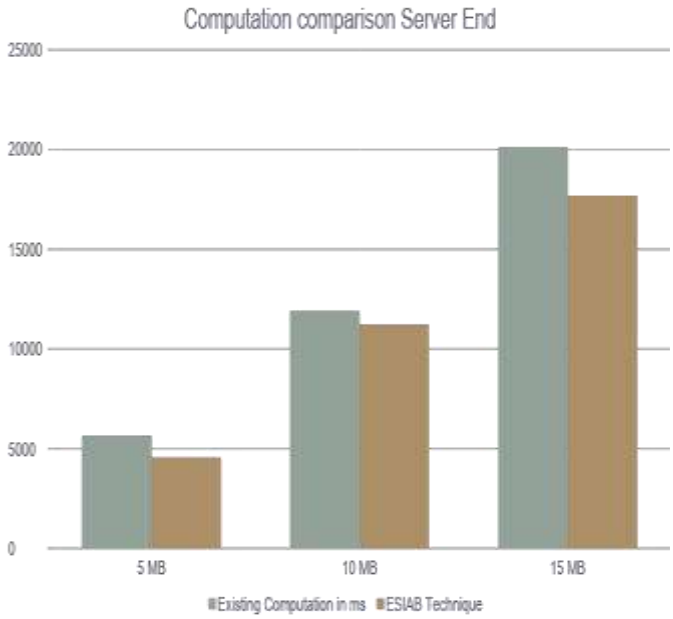

Figure 1.2: Graph Of Computation Time Over Different Files.

The above figure which represents the comparison analysis part in between the Existing ECC based encryption algorithm and the proposed ECC being proposed in our implemented work, the graph shows the efficiency while working at server side.

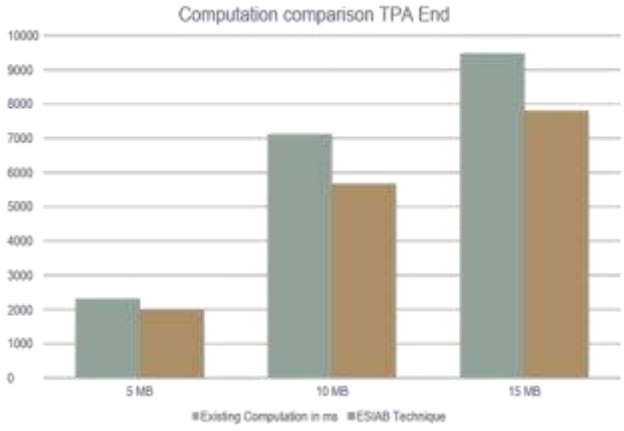

Figure 1.3: Bar Graph Comparison Analysis In Between Implemented Algorithm TPA Side.

The figure above demonstrate the computation time which is being taken while communication performed by the TPA, the operation such as data integrity verification and correctness of data computation data is performed at TPA side , the result comparison given high performance which is shown in above bar graph.

5. CONCLUSION & FUTURE WORK

As per discussed and algorithm performed by us in the area of cloud commutating. The considered work from the traditional algorithm taken as ECC and MAC for the encryption purpose and the key exchange and data distribution among the range of data. The proposed work performed by us is enhancing ECC where the SHA-2 takes part for the key generation and hash tag generation process. Our work also simplify the modules take part in complete process and finally the data is stored in encrypted form and hash tag for the same file id stored, further the integrity verification and proof generation is performed by us. The proposed work is conducted at configured cloud server accessed from remote location using static IP driven. The result we computed using the computation time and key exchange system given by the proposed system outperform better in proposed work. As per analysis the proposed work compute the low time at TPA side as well as server side to process the data store at server side as well as manage and proof generation.

As per discussion the proposed algorithm outperforms best in its field where both the encryption and hashing perform best among. Our further work will be implementing the system and algorithm with multiple authority system and also to perform them in parallel to get our result in heavy traffic cloud environment.

REFERENCES

1 .Soumya Parvatikar, Puja Prakash , Richa Prakash, Pragati Dhawale, S. B. Jadhav Secure Sharing of Personal Health Records utilizing Multi Authority Attribute based Encryption in Cloud Computing, IEEE Transactions On Parallel And Distributed Systems Volume : II, Issue : X, October - 2013.

2. Saipavan Konda,Niranjan Reddy Enhanced Scalable and Secured Sharing of Personal Health Records in Cloud Computing Based on Attribute Based Encryption with Integrity Proof Volume 3, Issue 9, September 2013.

3.Price M, Bellwood P, Kitson N, Davies I, Weber J, Lau F. Conditions conceivably touchy to a Personal Health Record (PHR) intercession, a methodical audit. BMC Med Inform Decis Mak [Internet]. ; 2015:

4. Yoshitaka,S.Chujyou,H.Kato Translation between HL7 v2.5 and CCR message designs (For correspondence among clinic and individual wellbeing record frameworks). Open Systems (ICOS), IEEE Conference on, September 2011.

5 C. J. Wang, X. L. Xu , D. Y. Shi , W. L. Lin Prevalence and pattern of hepatitis C infection disease among blood contributors in Chinese territory: an efficient survey and meta-investigation Published online 2011 Apr 9.

6 P. Van Gorp , M. Comuzzi, An open stage for individual wellbeing record applications with stage level security assurance, Volume 51, August, 2014.

7 M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, Above the Clouds: A Berkeley View of Cloud Computing, Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.

8 Abdulrahman Jabour,JosetteF.Jones, Facilitators and Barriers to Patients Engagements with Personal Health Records: Systematic Review, UAHCI 2013.

9 Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wan, Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE Transactions on Computers (Volume: 62, Issue: 2, Feb. 2013).

10 RachnaArora, AnshuParashar, Maintaining Data Confidentiality and Security over Cloud: An Overview.