A Survey Paper on Designing Multi-Cloud Server for Scalable and Secure Sharing over Web

[1*] Shruti Timande, [2] Prof. Sulbha Patil

[1] Department of Wireless Communication and Computing, RTMNU University, TGPCET
Nagpur, Maharashtra, India

[2] Assistant Professor Computer Science and Engineering, RTMNU University, TGPCET
Nagpur, Maharashtra, India

ABSTRACT

With the internet getting so popular data sharing and security of personal data has gain much more importance than before. Cloud provides and efficient way to outsource the data either online or offline but data security becomes one of the major issues in unreliable multi-cloud environment. This paper addresses the issues in multi-cloud environment and also provides a way to provide better security in multi-cloud environment. Further it discusses the different encryption algorithms that can be used to maintain a design framework for cloud environment.

KEYWORDS:

Cloud Computing; IaaS; Encryption; SaaS; PaaS; Distributed; Security; Privacy

INTRODUCTION

Engineering development and its selection are two discriminating effective variables for any business/association. Cloud computing is a late innovation ideal model that empowers associations or people to impart different administrations in a consistent and practical way. Cloud computing exhibits an opportunity for pervasive frameworks to power computational and stockpiling assets to achieve assignments that would not typically be conceivable on such asset obliged gadgets. Distributed computing can empower programming and base planners to construct lighter frameworks that last more and are more convenient and versatile [1]. Regardless of the favorable circumstances distributed computing offers to the originators of pervasive frameworks, there are a few impediments and constraints of distributed computing that must be tended to [2].

1.1 CLOUD BASICS

Cloud computing, or "the cloud", concentrates on expanding the viability of the imparted assets. Cloud assets are typically imparted by numerous clients as well as progressively reallocated for every interest and pay for every utilization premise. This can work for dispensing assets to clients. For instance, a cloud machine that serves Indian clients amid Indian business hours with an application (e.g., email) may reallocate the same assets to serve China clients amid China's business hours with an alternate application (e.g., an application server). This methodology ought to build the utilization of processing power accordingly decreasing ecological harm which are needed for a mixed bag of capacities. With distributed computing, numerous clients can get to a solitary server to recover and access the information without purchasing licenses for diverse applications [4].

1.2 CLOUD SERVICES

A. Software as a Service (SAAS)

SaaS customers rent utilization of uses running inside the Clouds supplier base, for instance Salesforce. The applications are normally offered to the customers through the Internet and are overseen totally by the Cloud supplier. That implies that the organization of these administrations, for example, upgrading and fixing are in the supplier's obligation. The profit of SaaS is that all customers are running the same programming adaptation and new usefulness can be effortlessly coordinated by the supplier and is in this way accessible to all customers [7].

B. Platform as a Service (PAAS)

PaaS Cloud providers offer an application platform as a service, for example Google App Engine. This enables clients to deploy custom software using the tools and programming languages offered by the provider. Clients have control over the deployed applications and environment-related settings. As with SaaS, the management of the underlying infrastructure lies within the responsibility of the provider [4].

C. Infrastructure as a Service (IAAS)

IaaS conveys fittings assets, for example, CPU, plate space or system segments as an administration. These assets are generally conveyed as a virtualization stage by the Cloud supplier and might be gotten to over the Internet by the customer. The customer has full control of the virtualized stage and is not in charge of dealing with the underlying base [4].

D. Storage as a Service

Capacity as an administration (StaaS) is a plan of action in which an expansive administration supplier rents space in their stockpiling foundation on a membership premise. The economy of scale in the administration supplier's framework permits them to give stockpiling a great deal more cost adequately than most people or organizations can give their own particular stockpiling, when aggregate expense of possession is considered. Capacity as a Service is frequently used to illuminate offsite reinforcement challenges. Faultfinders of capacity as an administration point to the vast measure of system data transmission needed to direct their stockpiling using a web based administration [7].

BRIEF LITERATURE SURVEY:

There are many issues with current cloud and their architectures. Some of them are users are often tied with one cloud provider, computing components are tightly coupled, lack of SLA supports, lack of Multi-tenancy supports, Lack of Flexibility for User Interface. [4]

One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider. Cachinet al. give examples of the risk of attacks from both inside and outside the cloud provider, such as the recently attacked Red Hat Linux's distribution servers. Another example of breached data occurred in 2009 in Google Docs, which triggered the Electronic Privacy Information Centre for the Federal Trade Commission to open an investigation into Google's Cloud Computing Services. Another example of a risk to data integrity recently occurred in Amazon S3 where users suffered from data corruption[1].

One of the results that they propose is to utilize a Byzantine flaw tolerant replication convention inside the cloud. Hendricks et al. express that this result can evade information defilement created by a few parts in the cloud. Then again, Cachinet al. assert that utilizing the Byzantine flaw tolerant replication convention inside the cloud is unsatisfactory because of the way that the servers having a place with cloud suppliers utilize the same framework establishments and are physically placed in the same spot [1]. As per Garfunkel, an alternate security hazard that may happen with a cloud supplier, for example, the Amazon cloud administration is a hacked secret key or information interruption. In the event that somebody gets access to an Amazon account secret key, they will have the capacity to get to the majority of the account's occasions and assets [1].

Despite the fact that cloud suppliers are mindful of the malevolent insider threat, they expect that they have basic answers for assuage the issue [1]. Rocha and Correia [1] focus conceivable assailants for Iaas cloud suppliers. For illustration, Grosse et al. [1] propose one result is to keep any physical access to the servers. Notwithstanding, Rocha and Correia [1] contend that the aggressors delineated in their work have remote get to and needn't bother with any physical access to the servers. Grosse et al. [1] propose an alternate result is to screen all right to gain entrance to the servers in a cloud where the client's information is put away. Be that as it may, Rocha and Correia [1] assert that this component is gainful for observing worker's conduct as far as whether they are after the protection arrangement of the organization or not, however it is not successful in light of the fact that it identifies the issue after it has happened.

An alternate methodology to secure distributed computing is for the information holder to store scrambled information in the cloud, and issue decoding keys to approved clients. At that point, when a client is renounced, the information manager will issue re-encryption orders to the cloud to re-scramble the information, to keep the disavowed client from decoding the information, and to produce new unscrambling keys to substantial clients, so they can keep on getting to the information. Then again, since a distributed computing environment is involved numerous cloud servers, such summons may not be gotten and executed by the majority of the cloud servers because of problematic system correspondences [3].

An alternate approach to secure the information utilizing diverse squeezing and encryption calculations and to conceal its area from the clients that stores and recovers it. The main contrast is that the framework introduced by Olfa Nasraoui [2] is an application based framework like which will run on the customers own framework. This application will permit clients to transfer record of diverse organizations with security peculiarities including Encryption and Compression. The transferred records might be gotten to from anyplace utilizing the application which is given.

The security of the Olfa Nasraoui [2] model has been investigation on the premise of their encryption calculation and the key administration. It has been watched that the encryption calculation have their own particular attributes; one calculation gives security at the expense of fittings, other is solid however utilizes more number of keys, one takes additionally handling time. This area demonstrates the different parameters which assume a paramount part while selecting the cryptographic calculation. The Algorithm discovered most guaranteeing is AES Algorithm with 256 bit key size (256k) [2].

A principle gimmick of cloud is information offering. Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng [5] demonstrate to safely, effectively, and adaptably impart information to others in distributed storage. We portray new open key cryptosystems which deliver steady size figure messages such that proficient assignment of unscrambling rights for any set of figure writings is conceivable. The curiosity is that one can total any set of mystery keys and make them as minimized as a solitary key, yet enveloping the force of every last one of keys being accumulated. At the end of the day, the mystery key holder can discharge a consistent size total key for adaptable decisions of figure content set in distributed storage, however the other encoded documents outside the set stay secret [5].

There are different examination challenges likewise there for embracing distributed computing, for example, generally oversaw administration level assertion (SLA), security, interoperability and dependability. This examination paper diagrams what distributed computing is, the different cloud models and the principle security dangers and issues that are at present inside the distributed computing industry. This exploration paper additionally investigates the key research and difficulties that shows in distributed computing and offers best practices to administration suppliers and also endeavors planning to power cloud administration to enhance their end result in this serious financial atmosphere [7].

Cloud based data storage systems have many complexities regarding critical/confidential/sensitive data of client. The trust required on Cloud storage is so far had been limited by users. The role of the paper is to grow confidence in Users towards Cloud based data storage. The paper handles key questions of the User about how data is uploaded on Cloud, maintained on cloud so that there is no data loss; data is available to only authorized User(s) as per Client/User requirement and advanced concepts like data recovery on disaster is applied [8].

Cloud computing is an adaptable, financially savvy, and demonstrated conveyance stage for giving business or shopper IT benefits over the Internet. Then again, distributed computing shows an included level of danger on the grounds that key administrations are frequently outsourced to an outsider, which makes it harder to keep up information security and protection, help information and administration accessibility, and show agreeability. Distributed computing powers numerous advances (SOA, virtualization, Web 2.0); it additionally inherits their security issues, which we talk about here, recognizing the fundamental vulnerabilities in this sort of frameworks and the most paramount dangers found in the writing identified with Cloud Computing and its surroundings and also to distinguish and relate vulnerabilities and dangers with conceivable arrangements[10].

Gehana Booth, Andrew Soknacki, and Anil Somayaji introduced an abnormal state characterization of momentum research in distributed computing security. Dissimilar to past work, this characterization is composed around assault systems and relating resistances. Particularly, they plot a few risk models for distributed computing frameworks, talk about particular assault systems, and order proposed protections by how they address these models and counter these components. This examination highlights that, while there has been significant exploration to date, there are still real dangers to distributed computing frameworks, for example, potential base trade off, that need to be better addressed [11].

Brent Lagesse talk about a pervasive framework using distributed computing assets and issues that must be tended to in such a framework. In this framework, the client's cell phone can't generally have system access to influence assets from the cloud, so it must settle on canny choices about what information ought to be put away by regional standards and what courses of action ought to be run mainly. As an issue of these choices, the client gets to be defenseless against assaults while interfacing with the pervasive framework [12]

Wayne A. Jansen talked about Security and protection issues in cloud. In meteorology, the most ruinous additional tropical violent winds advance with the arrangement of a bowed back front and cloud head differentiated from the fundamental polar-front, making a snare that totally surrounds a pocket of warm air with colder air. The most harming winds happen close to the tip of the snare. The cloud snare development gives a helpful relationship to distributed computing, in which the most intense deterrents with outsourced administrations (i.e., the cloud snare) are security and protection issues. This paper distinguishes key issues, which are accepted to have long haul centrality in distributed computing security and protection, in view of archived issues and showed shortcomings [13].

Mukesh Singhal and Santosh Chandrasekhar proposed intermediary based multi-distributed computing schema permits alert, on the fly coordinated efforts and asset imparting among cloud-based administrations, tending to trust, strategy, and security issues without pre-established cooperation understandings or institutionalized interfaces [14].

Sushmita Ruj, Milos Stojmenovic, Amiya Nayak propose another decentralized access control plan for secure information stockpiling in mists, that backings nameless confirmation. In the proposed plan, the cloud confirms the genuineness of the without knowing the client's character before putting away information. Their plan likewise has the included gimmick of access control in which just substantial clients have the capacity decode the put away data. The plan averts replay assaults and backings creation, alteration, and perusing information put away in the cloud. We additionally address client disavowal. Besides, our confirmation and access control plan is decentralized and hearty, dissimilar to different access control plans intended for mists which are unified. The correspondence, calculation, and capacity overheads are tantamount to unified methodologies [15].

Lukas Malina and Jan Hajny present a novel security protecting security answer for cloud administrations. They manage client unnamed access to cloud benefits and imparted stockpiling servers. Their answer furnishes enrolled clients with nameless access to cloud administrations. Our answer offers nameless verification. This implies that clients' close to home qualities (age, legitimate enrollment, effective installment) can be demonstrated without uncovering clients' personality. In this manner, clients can utilize administrations without any risk of profiling their conduct. Then again, if clients break supplier's manages, their right to gain entrance rights are repudiated. They dissect current protection protecting answers for cloud administrations and framework our answer focused around progressive cryptographic segments. Their answer offers unacknowledged access, un-join capacity and the privacy of transmitted information. In addition, we actualize our answer and we yield the test comes about and contrast the execution and related arrangements [16].

Morgan, Lorraine Conboy, Kieran study help the current cloud innovations writing that does not address the unpredictable and multifaceted nature of reception. The discoveries are examined utilizing the reception of development writing as an issue to uncover how mechanical, authoritative and natural components effect cloud appropriation. Their decisions uncover that components affecting cloud selection have a tendency to be mental and in addition specialized, and a few proposals are advanced for future examination [17].

Sarita Motghare, P.s.mohod address the development of a proficient CPDP plan and element review administration for dispersed distributed storage too checking the uprightness insurance of a depended and outsourced stockpiling which help the versatility of administration and information relocation [18].

Bryan Ford talked about on alternate issues of distributed computing like iceburgs in cloud. Distributed computing is engaging from administration and productivity viewpoints, however brings dangers both known and obscure. Well-known and hotly-discussed data security dangers, because of programming vulnerabilities, insider assaults, and side-channels for instance, may be just the "tip of the ice sheet." As various, freely created cloud administrations impart perpetually smoothly and forcefully multiplexed equipment asset pools, eccentric connections between burden adjusting and other sensitive instruments could prompt element insecurities or "meltdowns." Non-straightforward layering structures, where option cloud administrations may seem autonomous yet impart profound, concealed asset conditions, may make startling and conceivably disastrous disappointment relationships, reminiscent of budgetary industry crashes. At last, distributed computing compounds effectively troublesome advanced conservation challenges, in light of the fact that just the supplier of a cloud-based application or administration can chronicle a "live," utilitarian duplicate of a cloud curio and its information for long haul social safeguarding. This paper investigates these generally un-perceived dangers, presenting the defense that we ought to study them before our financial fabric gets to be inseparably reliant on an advantageous however conceivably insecure processing model [19].

Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng describe new public-key cryptosystems which produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. We provide formal security analysis of our schemes in the standard model. We also describe other application of our schemes. In particular, our schemes give the first public-key patient-controlled encryption for flexible hierarchy, which was yet to be known [20].

Abhinandan P Shirahatti, P S Khanagoudar proposed a framework for uprightness of open evaluating of distributed storage. To securely exhibit an influential pariah evaluator (TPA), the going hand in hand with two noteworthy essentials must be met: 1) TPA should have the ability to gainfully survey the cloud data stockpiling without asking for the close-by copy of data, and present no additional on-line burden to the cloud customer; 2) he outcast assessing system should get no new vulnerabilities towards customer data security. In this framework, they utilize and remarkably solidify the overall public key based homomorphism authenticator with self-assertive covering to achieve the security shielding open cloud data assessing structure, which meets all above essentials. To help compelling treatment of different looking at errands, they further explore the technique for bilinear aggregate signature to enhance our essential result into a multi-customer setting, where TPA can perform diverse investigating assignments in the meantime. Expansive security and execution examination shows the proposed arrangements are provably secure and significantly viable [21].

Allan A. Friedman and Darrell M. West investigates how to contemplate security and security on the cloud. It is not expected to be a list of cloud dangers (see ENISA (2009) for a sample of thorough investigation of the dangers of cloud appropriation to particular gatherings). They outline the set of attentiveness toward the cloud and highlight what is new and what is most certainly not. We examine a set of arrangement issues that speak to precise concerns meriting the consideration of approach producers. We contend that the frail connection in security by and large is the human element and encompassing organizations and motivators matter more than the stage itself [22].

Mohamed Nabeel, Elisa Bertino propose a methodology, in view of two layers of encryption, that addresses such necessity. Under our methodology, the information manager performs a coarse-grained encryption, though the cloud performs a fine-grained encryption on top of the holder scrambled information. A testing issue is the manner by which to disintegrate access control arrangements (ACPs) such that the two layer encryption can be performed. We demonstrate that this issue is NP-finish and propose novel enhancement calculations. We use a productive gathering key administration plot that backings expressive ACPs. Our framework guarantees the privacy of the information and jelly the security of clients from the cloud while assigning the vast majority of the right to gain entrance control implementation to the cloud [23].

Myrto Arapinis, Sergiu Bursuc, and Mark Ryan concentrate on the specific distributed computing application of meeting administration. They distinguish the particular security and protection hazards that current frameworks like Easychair and EDAS stance, and location them with a convention hidden Confichair, a novel cloud-based meeting administration framework that offers solid security and security ensures [24].

Darko Andročec give diagram of existing writing on Cloud Computing matters in profit making (estimating of Cloud administrations, expenses, advantages and danger of Clouds, ROI and expense/advantages models) and propose some new research challenges. Probably the most fascinating future themes are a complete expense advantage investigation system advancement, utilizing reproductions to distinguish unmistakable expense lessening, supportability of current costs of Cloud administrations and framework organization cost in a Cloud environment [25].

Abhinay B.angadi, Akshata B.angadi, Karuna C.gull talk about security issues, protection and control issues, openness issues, secrecy, respectability of information and a lot of people more for distributed computing. Current answers for these security dangers are likewise talked about. Furthermore, we make a rundown of security things that all clients ought to be mindful of before picking to utilize cloud based administrations and examine routines for permitting the client to choose particular security levels of security for things [26].

PROPOSED SYSTEM

The proposed work is planned to be carried out in the following manner.

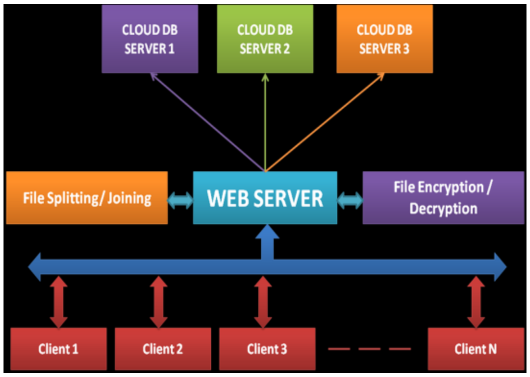

Fig: Basic Proposed System Architecture

The system will provide load balancing in terms of database as the file to be uploaded will be splitted into n parts and each part will be stored in a different cloud server. Consider an example where a file is splitted into two part out of which one is stored in google IaaS and other in Yahoo IaaS [25].

CONCLUSION

IaaS is the establishment layers of the Cloud Computing conveyance demonstrate that comprises of numerous segments and innovations. Every segment in Cloud framework has its helplessness which may affect the entire Cloud's Computing security. Cloud computing business develops quickly notwithstanding security concerns, so coordinated efforts between Cloud gatherings would aid in overcoming security difficulties and push secure Cloud Computing administrations.

In this paper we said a percentage of the security worries about cloud computing furthermore proposed a framework that can help enhance the security of cloud IaaS administrations. Our methodology is intended to be executed in a multi nature.

REFERENCES

1. Cloud Computing Security: From Single To Multi-Clouds Mohammed A. Alzain , Eric Pardede , Ben Soh , James A. Thom 2012 45th Hawaii International Conference On System Sciences.

2. Ensuring Data Integrity And Security In Cloud Storage Olfa Nasraoui, Member, IEEE, Maha Soliman, Member, IEEE, Esin Saka, Member, IEEE, Antonio Badia, Member, IEEE, And Richard Germain IEEE TRANSACTIONS ON CLOUD AND DATA ENGINEERING, VOL. 20, No. 2, February 2013.

3. Reliable Re-Encryption In Unreliable Clouds Qin Liu ,Chiu C.Tan ,Jiewu, And Guojun Wang IEEE Communications Society Subject Matter Experts For Publication In The IEEE Globecom 2011 Proceedings.

4. Service-Oriented Cloud Computing Architecture Wei-Tek Tsai, Xin Sun, Janaka Balasooriya 2010 Seventh International Conference On Information Technology

5. Key-Aggregate Cryptosystem For Scalable Data Sharing In Cloud Storage Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, And Robert H. Deng, Senior Member, IEEE, IEEE Transactions On Parallel And Distributed Systems. Volume: 25, Issue: 2. Year: 2014

6. Mell-Peter, Grance-Timothy. September 2011. The NIST Definition Of Cloud Computing.

7. C. Cachin, I. Keidar And A. Shraer, "Trusting The Cloud", ACM SIGACT News, 40, 2009, Pp. 81-86. Clavister, "Security in The Cloud", Clavister White Paper, 2008.

8. H.Mei, J. Dawei, L. Guoliang And Z. Yuan, "Supporting Database Applications As A Service", ICDE'09:Proc. 25thintl.Conf. On Data Engineering, 2009, Pp. 832-843.

9. C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring Data Storage Security In Cloud Computing", ARTCOM'10: Proc. Intl. Conf. On Advances In Recent Technologies In Communication And Computing, 2010, Pp. 1-9.

10. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina And Eduardo B Fernandez An Analysis Of Security Issues For Cloud Computing Hashizume Et Al. Journal Of Internet Services And Applications 2013.

11. Gehana Booth, Andrew Soknacki, and Anil Somayaji Cloud Security: Attacks and Current Defenses 8th ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE (ASIA'13), JUNE 4-5, 2013, ALBANY, NY.

12. Brent Lagesse Challenges In Securing The Interface Between The Cloud And Pervasive Systems IEEE Pervasive Computing, Vol. 8, Pp. 14–23, October 2009. [Online].

13. Wayne A. Jansen Cloud Hooks: Security And Privacy Issues In Cloud Computing Proceedings Of The 44th Hawaii International Conference On System Sciences – 2011.

14. Mukesh Singhal And Santosh Chandrasekhar Collaboration In Multicloud Computing Environments: Framework And Security Issues Published By The IEEE Computer Society 0018-9162/13/$31.00 © 2013 IEEE

15. Sushmita Ruj, Milos Stojmenovic, Amiya Nayak Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL:25 NO:2 YEAR 2014.

16. Lukas Malina and Jan Hajny Efficient Security Solution for Privacy-Preserving Cloud Services 6TH INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS SIGNAL PROCESSING YEAR 2013

17. Morgan, Lorraine Conboy, Kieran FACTORS AFFECTING THE ADOPTION OF CLOUD COMPUTING: AN EXPLORATORY STUDY Proceedings of the 21st European Conference on Information Systems 2012

18. Sarita Motghare, P.S.Mohod International Journal of Advanced Research In Computer Science Volume 4, No. 4, March-April 2013

19. Bryan Ford Icebergs in the Clouds: The Other Risks Of Cloud Computing SIGCOMM, August 2010

20. Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, And Robert H. Deng Key-Aggregate Cryptosystem For Scalable Data Sharing In Cloud Storage IEEE Transactions On Parallel And Distributed Systems. Volume: 25, Issue: 2. Year: 2014.

21. Abhinandan P Shirahatti, P S Khanagoudar Preserving Integrity of Data and Public Auditing For Data Storage Security In Cloud Computing IMACST: VOLUME 3 NUMBER 3 JUNE 2012

22. Allan A. Friedman and Darrell M. West Privacy and Security in Cloud Computing Number 3 October 2010

23. Mohamed Nabeel, Elisa Bertino Privacy Preserving Delegated Access Control in Public Clouds PUBLISHING YEAR 2012

24. Myrto Arapinis, Sergiu Bursuc, and Mark Ryan Privacy Supporting Cloud Computing: Confichair, A Case Study University Of Birmingham Nov. 2012

25. Darko Andročec Research Challenges For Cloud Computing Economics Nov. 2011

26. Abhinay B.Angadi, Akshata B.Angadi, Karuna C.Gull Security Issues with Possible Solutions In Cloud Computing-A Survey International Journal Of Advanced Research In Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013