© 2018 IJSRST | Volume 4 | Issue 3 | Print ISSN : 2395-6011 | Online ISSN: 2395-602X

National Conference on Advances in Engineering and Applied Science (NCAEAS)
29th January 2018
Organized by : Anjuman College of Engineering and Technology (ACET) Nagpur, Maharashtra, India, In association with
International Journal of Scientific Research in Science and Technology

Review Article on Cloud Drops

Dr.Leena Gahane[1] , Ibrahim Abizar Rampurawala[2], Chetan Ganesh Mahurkar[2]

[1]Professor , Dpett of Physics , Anjuman College Of Engineering And Technology, Sadar, Nagpur, Maharashtra, India

[2]BE.II Sem Anjuman College Of Engineering And Technology, Sadar, Nagpur, Maharashtra, India

ABSTRACT

Cloud computing means storing and accessing data and programs over the internet instead of your computer's hard drive.

Drops is division and replication of data in the cloud for optimal performance and security.

Cloud drops is a pervasive awareness platform that integrates virtual information from the web more closely with the contextually rich physical spaces in which we live and work. Clouddrops technology is about securing data over the cloud. Clouddrops consists of many interactive stamp sized displays, each showing a tiny bit of digital information. The large number of displays and their small size allows the user to flexibly instrument, orchestrate and reconfigure her personal information environment. We show different form factors for stamp-sized displays, provide a device concept and a first implementation. Clouddrops represent dynamic digital content, such as websites and documents or contacts. Thereby, each individual content is represented as a separate clouddrop. This allows the user to flexible attach each item on a physical place. In the other direction, it makes a physical place accessible remotely to provide situated messaging and communication.

In the present article we are trying to understand the threats and suggesting new strategy for security aspects.

Keywords : Cloud computing, data, Cloud drops, stamp sized ,security(DATA FRAGMENTATION) , strategy.

I. INTRODUCTION

People intensively use physical space for accessing and remembering paper-bound information. The cloud computing paradigm has reformed the usage and management of the information technology infrastructure. Access to shared resources in a pay-as-you-go mode cuts the management effort of the user to a minimal level. Cloud computing is characterized by on-demand self-services, ubiquitous network accesses, resource pooling, elasticity, and measured services. The aforementioned characteristics of cloud computing make it a striking candidate for businesses, organizations, and individual users for adoption. However, the benefits of low-cost, negligible management (from a users perspective), and greater flexibility come with increased security concerns.

We present Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that judicially fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a file into fragments is performed based on a given user

criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes (we use the term node to represent computing, storage, physical, and virtual machines) contains a distinct fragment to increase the data security. However, there is always a possibility of a successful attack on any node. A successful attack on a single node must not reveal the locations of other fragments within the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security, we select the nodes in a manner that they are not adjacent and are at certain distance from each other. The node separation is ensured by the means of the Tcoloring. To improve data retrieval time, the nodes are selected based on the centrality measures that ensure an improved access time. To further improve the retrieval time, we judicially replicate fragments over the nodes that generate the highest read/write requests. The selection of the nodes is performed in two phases. In the first phase, the nodes are selected for the initial placement of the fragments based on the centrality measures. In the second phase, the nodes are selected for replication. The proposed DROPS methodology does not use traditional cryptographic techniques for data security that improves the performance. The working of the DROPS methodology is shown as a high-level work flow in Figure 1.

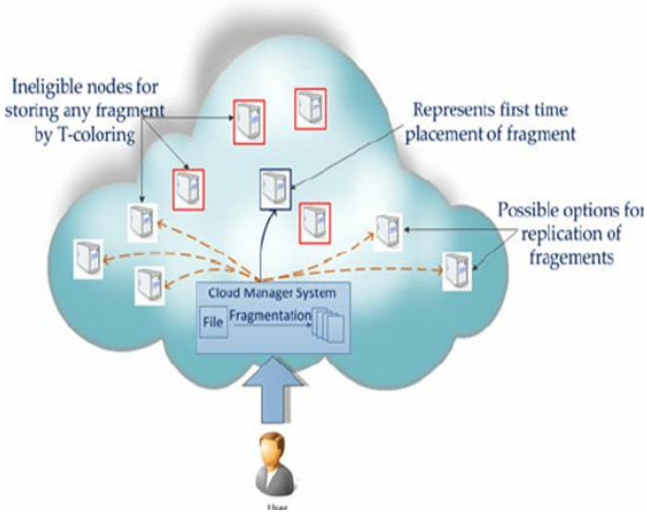

Figure 1. Cloud Drops Methodology

The utilized security procedure should likewise consider the improvement of the information recovery time .Cloud Security Using DROPS (Division and Replication of Data in the Cloud for Optimal Performance and Security) Technique that aggregately approaches the security and performance issues. In the DROPS technique, we separate a document into sections, and duplicate the divided information over the cloud nodes. Security is one of the most crucial aspects among those prohibiting the widespread adoption of cloud computing. Cloud security issues may stem due to the core technology's implementation (virtual machine (VM) escape, session riding, etc.), cloud service offerings (structured query language injection, weak authentication schemes, etc.), and arising from cloud characteristics (data recovery vulnerability, Internet protocol vulnerability, etc.). For a cloud to be secure, all of the participating entities must be secure. In any given system with multiple units, the highest level of the system's security is equal to the security level of the weakest entity. Therefore, in a cloud, the security benefit does not solely depend on an individual's security measures. The neighbouring entities may provide

an opportunity to an attacker to bypass the users defences. The off-site data storage cloud utility requires users to move data in cloud's virtualized and shared environment that may result in various security concerns. Pooling and elasticity of a cloud, allows the physical resources to be shared among many users. Furthermore, the shared resources may be reassigned to other users at some instance of time that may result in data compromise through data recovery methodologies. Furthermore, a multi-tenant virtualized environment may result in a VM to escape the bounds of virtual machine monitor (VMM). The escaped VM can interfere with other VMs may access to unauthorized data. Similarly, cross-tenant virtualized network access may also compromise data privacy and integrity. Due to improper media sanitization can also leak customer's private data.

II. DATA FRAGMENTATION

The security of a large-scale system, such as cloud depends on the security of the system as a whole and the security of individual nodes. A successful intrusion into a single node may have severe consequences, not only for data and applications on the victim node, but also for the other nodes. The data on the victim node may be revealed fully because of the presence of the whole file [17]. A successful intrusion may be a result of some software or administrative vulnerability [17]. In case of homogenous systems, the same flaw can be utilized to target other nodes within the system. The success of an attack on the subsequent nodes will require less effort as compared to the effort on the first node. Comparatively, more effort is required for heterogeneous systems. However, compromising a single file will require the effort to penetrate only a single node. The amount of compromised data can be reduced by making fragments of a data file and storing them on separate nodes [17], [21]. A successful intrusion on a single or few nodes will only provide access to a portion of data that might not be of any significance. Moreover, if an attacker is uncertain about the locations of the fragments, the probability of finding fragments on all of the nodes is very low. Let us consider a cloud with M nodes and a file with z number of fragments. Let s be the number of successful intrusions on distinct nodes, such that s>z. The probability that s number of victim nodes contain all of the z sites storing the file fragments (represented by P(s,z)) is given as: $P(s, z) = \binom{s}{z}\binom{M-s}{s-z}\Big/\binom{M}{s}$. (1) If M = 30, s = 10, and z = 7, then P(10, 7) = 0.0046. However, if we choose M = 50, s = 20, and z = 15, then P(20, 15) = 0.000046. With the increase in M, the probability of a state reduces further. Therefore, we can say that the greater the value of M, the less probable that an attacker will obtain the data file. In cloud systems with thousands of nodes, the probability for an attacker to obtain a considerable amount of data, reduces significantly. However, placing each fragment once in the system will increase the data retrieval time. To improve the data retrieval time, fragments can be replicated in a manner that reduces retrieval time to an extent that does not increase the aforesaid probability.

III. COMPARITIVE TECHNIQUES

When the results of the DROPS methodology are compared with fine-grained replication strategies, namely: (a) DRPA-star, (b) WA-star, (c) A-star, (d) SA1, (e) SA2, (f) SA3, (g) Local Min-Min, (h) Global MinMin, (i) Greedy algorithm, and (j) Genetic Replication Algorithm (GRA). The DRPA-star is a data replication algorithm based on the A-star best-first search algorithm. The DRPA-star starts from the null solution that is called a root node. The

communication cost at each node n is computed as: cost(n) = g(n) + h(n), where g(n) is the path cost for reaching n and h(n) is called the heuristic cost and is the estimate of cost from n to the goal node. The DRPA-star searches all of the solutions of allocating a fragment to a node. The solution that minimizes the cost within the constraints is explored while others are discarded. The selected solution is inserted into a list called the OPEN list. The list is ordered in the ascending order so that the solution with the minimum cost is expanded first. The heuristic used by the DRPAstar is given as h(n) = max(0, (mmk(n)g(n))), where mmk(n) is the least cost replica allocation or the maxmin RC. Readers are encouraged to see the details about DRPA-star in . The WA-Star is a refinement of the DRPA-star that implements a weighted function to evaluate the cost. The function is given as: f(n) = f(n) + h(n) + (1 – (d(n)/D)h(n). The variable d(n) represents the depth of the node n and D denotes the expected depth of the goal node . The A-star is also a variation of the DRPA-star that uses two lists, OPEN and FOCAL. The FOCAL list contains only those nodes from the OPEN list that have f greater than or equal to the lowest f by a factor of 1 + . The node expansion is performed from the FOCAL list instead of the OPEN list. Further details about WAStar and A-star can be found in . The SA1 (suboptimal assignments), SA2, and SA3 are DRPA-star based heuristics. In SA1, at level R or below, only the best successors of node n having the least expansion cost are selected. The SA2 selects the best successors of node n only for the first time when it reaches the depth level R. All other successors are discarded. The SA3 works similar to the SA2, except that the nodes are removed from OPEN list except the one with the lowest cost. Readers are encouraged to read for further details about SA1, SA2, and SA3. The LMM can be considered as a special case of the bin packing algorithm. The LMM sorts the file fragments based on the RC of the fragments to be stored at a node. The LMM then assigns the fragments in the ascending order. In case of a tie, the file fragment with minimum size is selected for assignment (name local Min-Min is derived from such a policy). The GMM selects the file fragment with global minimum of all the RC associated with a file fragment. In case of a tie, the file fragment is selected at random. The Greedy algorithm first iterates through all of the M cloud nodes to find the best node for allocating a file fragment. The node with the lowest replication cost is selected. The second node for the fragment is selected in the second iteration. However, in the second iteration that node is selected that produces the lowest RC in combination with node already selected. The process is repeated for all of the file fragments. Details of the greedy algorithm can be found in . The GRA consists of chromosomes representing various schemes for storing file fragments over cloud nodes. Every chromosome consists of M genes, each representing a node. Every gene is a N bit string. If the k-th file fragment is to be assigned to S i , then the k-th bit of i-th gene holds the value of one. Genetic algorithms perform the operations of selection, crossover, and mutation. The value for the crossover rate (μc) was selected as 0.9, while for the mutation rate (μm) the value was 0.01. The use of the values for μc and μm is advocated in .The best chromosome represents the solution. GRA utilizes mix and match strategy to reach the solution. More details about GRA can be obtained from.

ADVANTAGES:

- Easy implementation. Cloud hosting allows business to retain the same applications and business processes without having to deal with the backend technicalities. Readily manageable by the Internet, a cloud

infrastructure can be accessed by enterprises easily and quickly.

- Accessibility. Access your data anywhere, anytime. An Internet cloud infrastructure maximizes enterprise productivity and efficiency by ensuring your application is always accessible. This allows for easy collaboration and sharing among users in multiple locations.
- No hardware required. Since everything will be hosted in the cloud, a physical storage center is no longer needed. However, a backup could be worth looking into in the event of a disaster that could leave your company's productivity stagnant.
- Cost per head. Overhead technology costs are kept at a minimum with cloud hosting services, enabling businesses to use the extra time and resources for improving the company infrastructure.
- Flexibility for growth. The cloud is easily scalable so companies can add or subtract resources based on their needs. As companies grow, their system will grow with them.
- Efficient recovery. Cloud computing delivers faster and more accurate retrievals of applications and data. With less downtime, it is the most efficient recovery plan.

DISADVANTAGES:

- No longer in control. When moving services to the cloud, you are handing over your data and information. For companies who have an in-house IT staff, they will be unable to handle issues on their own. However, Stratosphere Networks has a 24/7 live help desk that can rectify any problems immediately.
- May not get all the features. Not all cloud services are the same. Some cloud providers tend to offer limited versions and enable the most popular features only, so you may not receive every feature or customization you want. Before signing up, make sure you know what your cloud service provider offers.
- Doesn't mean you should do away with servers. You may have fewer servers to handle which means less for your IT staff to handle, but that doesn't mean you can let go of all your servers and staff. While it may seem costly to have data centers and a cloud infrastructure, redundancy is key for backup and recovery.
- No Redundancy. A cloud server is not redundant nor is it backed up. As technology may fail here and there, avoid getting burned by purchasing a redundancy plan. Although it is an extra cost, in most cases it will be well worth it.
- Bandwidth issues. For ideal performance, clients have to plan accordingly and not pack large amounts of servers and storage devices into a small set of data centers.

PRESENT THREATS

- The neighboring entity may provide an opportunity to an attacker to bypass the user defenses.
- The off site data storage cloud utility requires users to move data in clouds visualization and shared environment that may cause various security concerns.
- Pooling and elasticity of the cloud, allow the physical resources to be shared among many users. These shared resources may be reassigned to other users for some instance of time that may result in data compromise.
- A multi tenant virtual environment may result in VM to escape the boundaries of virtual machine monitor(VMM) which can

interfere to other VMs may access to unauthorized data.

- In cross tenant virtualized network, due to improper media sanitization, the customer data can also get leaked.

PRESENT STRATEGIES USED TO DEAL WITH THREATS (PRESENT)

- In the DROPS methodology, a file is divided into fragments, and replicate the fragmented data over the cloud nodes, which is duplicating the data. Each of the nodes stores only a single fragment of a particular data file that ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker.
- The nodes storing the fragments are separated by a certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments.
- For a cloud to be secure all participating entities must be secure. In a system with multiple units, the highest level of systems security is equal to the security level of the weakest entity.

UNIDENTIFIED PREVAILING THREATS (AS STUDIED AFTER REVIEWING THE ARTICLE)

- If user id and password for the cloud account is hacked our data stored in public cloud is at high risk.
- If the servers of the company providing cloud storage are hacked all the individual data with the company lies under risk of miss use against individual as well as company.
- In case of war, if our data lies with a company of a country with which our country is at war our data may be compromised or misused by the nation with which we are at a war. In such case our personal data can act as a weapon against our nation.

SUGGESTED STRATEGIES

- Data stored over cloud must be secured with biometric password (like: fingerprint, iris scan, etc) so that it reduces or nullify the risk of data from being hacked.
- Companies providing cloud data storage service must have a very strong firewall against hackers and should consider the security against hacking of utmost importance.
- Data storage servers must be contented within the same country where the user of the cloud presides and there must be a government body which can take over the data from the foreign company providing cloud facility in case of any emergency.

IV. CONCLUSION

We studied about cloud drops technology and threats with which it is fighting with the help of fragmentation and came up with future or unidentified threats which are still present even after utilization of the present technology and its strategies.

We also came up with some strategies which could be used against the threats still prevalent.

V. REFERENCES

[1]. Bhole Laxmikant, Mrs. M.S haikh, Patil Pratik kumar, Salve Rahul, Warade Pratik :‖A SURVEY ON CLOUD DATA ACCESS PRIVILEGE WITH FULLY ATTRIBUTE – BASED ENCRYPTION WITHGEO SOCIAL SECURITY‖, Vol. 3, Issue 11, November 2015

[2]. DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security‟ Mazhar Ali, Student Member, IEEE, Kashif

Bilal, Student Member, IEEE, Samee U. Khan, Senior Member, IEEE, Bharadwaj Veeravalli, Senior Member, IEEE, Keqin Li, Senior Member, IEEE, and Albert Y. Zomaya, Fellow, IEEE

[3]. T. Loukopoulos and I. Ahmad, —Static and adaptive distributeddata replication using genetic algorithms,‖ Journal ofParallel and Distributed Computing, Vol. 64, No. 11, 2004,

[4]. SLIMON OBLERDING, JURGEN STEIMLE, SURANGA NANAYAKKARA AND PATTIE MAES.