A SURVEY ON CRYPTOGRAPHY IN CLOUD COMPUTING

PG Scholar Akshada Lenday, Mr. Neetesh Gupta

CSE Department

Technocrat institute of technology, RGPV University Bhopal

akshadalenday@gmail.com

Abstract: Cloud computing is a rapidly growing technology now a days, which will remain mostly used and advanced technology in upcoming years. As it provides user to store, access, and manipulate data with user's convenience regardless of time and location along with it provides the pool of resources such as network, storage, and services on-demand basis. With increase in the trend of using cloud computing, securing the cloud becomes more difficult from different threats and attacks. Particular attack can primarily focus on different layer of cloud architecture, vulnerability at one layers makes upper layers unstable and prone to easy attacks. In this survey paper we will be studying different internal and external threats or attack possible on cloud data to prevent data theft, data leakage, breach, and data modification by applying user authentication, user access rights, encryption of user's data from external point of view and admin authentication, access rights from internal threat point of view to eliminate both inside and outside attack on data in cloud environment.

Keywords: Cloud Computing, Encryption, Decryption, Standardization, Cloud Storage.

I. INTRODUCTION

Cloud computing is a recent technological development in the computing field in which mainly focused on designing of services which can be provided to the users in same way as the basic utilities like food, water, gas, electricity and telephony [6]. In this technology services are developed and hosted on the cloud (a network designed for storing data called data centre) and then these services are offered to users always whenever they want to use. The cloud hosted services are delivered to users in pay-per-use, multi-tenancy, scalability, self-operability, on-demand and cost effective manner[8] [7]. Cloud computing is become popular because of above mention services offered to users. All the services offered by servers to users are provided by cloud service provider (CSP) which is working same as the ISP (Internet service provider) in the internet computing [10] [9]. In the internet technology some innovative development in virtualization and distributed computing and accessing of high speed network with low cost attract focus of users toward this technology. This technology is designed with the new concept of services provisioning to users without purchasing of these services and stored on their local memory. The cloud in cloud computing originated from the habit of drawing the internet as a fluffy cloud in network diagrams. No wonder the most popular meaning of cloud computing refers to running workloads over the internet remotely in a commercial provider's data centre—the so-called public cloud model. AWS (Amazon Web Services), Sales force's CRM system, and Google Cloud Platform all exemplify this popular notion of cloud computing [13].

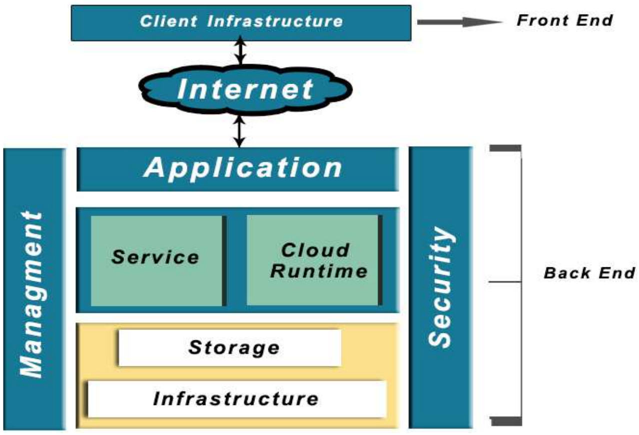


Figure 1: Architecture of cloud computing.

Cloud computing characteristics and benefits [11] [12]

Cloud computing boasts several attractive benefits for businesses and end users. Five of the main benefits of cloud computing are:

Self-service provisioning: End users can spin up compute resources for almost any type of workload on demand. This eliminates the traditional need for IT administrators to provision and manage compute resources.

Elasticity: Companies can scale up as computing needs increase and scale down again as demands decrease. This eliminates the need for massive investments in local infrastructure, which may or may not remain active.

Pay per use: Compute resources are measured at a granular level, enabling users to pay only for the resources and workloads they use.

Workload resilience: Cloud service providers often implement redundant resources to ensure resilient storage and to keep users' important workloads running -- often across multiple global regions.

Migration flexibility: Organizations can move certain workloads to or from the cloud -- or to different cloud platforms -- as desired or automatically for better cost savings or to use new services as they emerge.

➢ CRYPTOGRAPHY

Some of the concepts used in Cryptography are mentioned here [1]:

Purpose of Cryptography

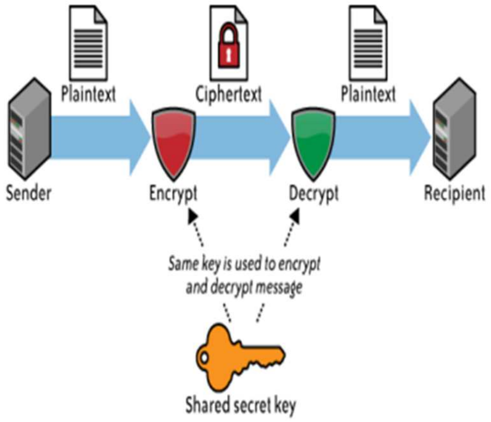
¬ Authentication: Authentication mechanisms help to establish proof of identities. This process ensures that the origin of the message is correctly identified.

¬ Confidentiality: The principle of confidentiality specifies that only the sender and the intended recipient should be able to process the contents of a message.

¬ Availability: The principle of availability states that resources should be available to authorized parties all the times.

¬ Integrity: The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender.

¬ Access Control: Access Control specifies and controls who can access the process.



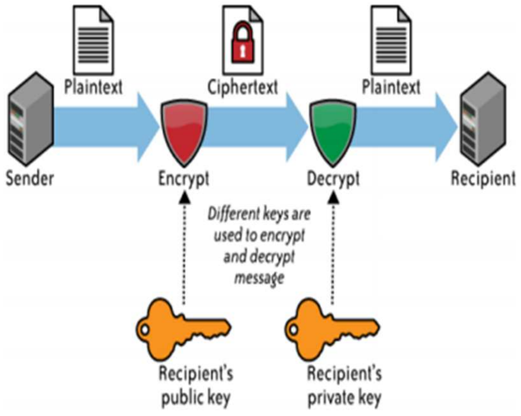


Figure 2: secret key cryptography. Figure 3: public key cryptography.

Types of Cryptography

¬ Secret Key Cryptography: When the same key is used for both encryption and decryption, DES, Triple DES, AES, RC5 and etc., may be the examples of such encryption, then that mechanism is known as secret key cryptography.

¬ Public Key Cryptography: When two different keys are used, that is one key for encryption and another key for decryption, RSA, Elliptic Curve and etc., may be the examples of such encryption, then that mechanism is known as public key cryptography.

Cryptography

¬ Plain Text: Any communication in the language that we use in the human language, takes the form of plain text. It is understood by the sender and the recipient and also by anyone who gets an access to that message.

¬ Cipher Text: Cipher means a code or a secret message. When a plain text is codified using any suitable scheme the resulting message is called as cipher text.

¬ Key: An important aspect of performing encryption and decryption is the key. It is the key used for encryption and decryption that makes the process of cryptography secure.

II. LITERATURE REVIEW

In this paper author explains about The major benefit of cloud application migration is that it allows an application provider (SaaS provider) to reuse the intrinsic components of a system that are compatible with cloud environments instead of building software applications from scratch. However, there are a number of diverse primary obstacles that impede the migration of applications. Current approaches do not support automatic migration for the cloud environment and are very limited to particular cloud environments [1]. The cloud lock-in problem is a situation where customers are dependent on a single cloud provider and cannot move to a different cloud environment. One solution to the cloud lock-in problem is cloud migration, which enables the moving of applications of customers in one cloud to another cloud. However, current migration techniques mostly focus on migrating VMs between physical servers that reside in a single cloud. In this paper, we consider an automated cloud migration system that enables the migration of VMs between different clouds. Such a system can be used by customers to change cloud providers if they can take the advantages of moving to a new cloud environment.

In this paper author discuss enhancements of the CloudSim [2] tool to support cloud migration from the cloud users' point of view. The produced enhancements are applicable and accurate compared to the deployment of the Amazon Elastic Compute Cloud (EC2) with respect to costs and performance. Subsequently present a tool-based approach known as CDOSIM for simulating cost and performance in terms of the response time of cloud deployment options to support software system migration. The results of the proposed approach are accurate prediction of performance (response time) and cost compared with Amazon EC2 and Eucalyptus, present a tool for evaluating cost and performance analysis before an application is deployed to the cloud. The proposed tool achieves accurate estimates of performance. Future plan is to develop an optimization engine for exploring costs to satisfy cloud customers with QoS constraints as well as provide ways to choose an appropriate service provider.

In this paper author explains about the Architecture-based approach [4] an architecture-based approach needs to be adaptive during transformation runtime migration in order to support the move of applications or software systems to cloud environments. However, very limited architecture-based approaches have been proposed in the literature relevant to cloud migration optimization. Author proposes a framework that can be used to prepare an application, the design of a runtime system, workflow and deployment, and optimizations. The proposed solution improves the flexibility of deployment based on user-level virtualization by isolating the virtual machine from the application software. The findings of the experiments indicated that the solution is efficient in terms of performance and storage. Propose an architecture based approach to optimization service deployment to reduce costs, improve the efficiency of deployment and guarantee the consumers' QoS requirements. In particular, they propose three algorithms to standardize and optimize the requirements of service deployment.

In this paper author proposed the need for SLA violation prevention most cloud service providers offer services based on general availability with SLAs may not consider an SLA violation if a server goes down. Typically, the service provider allows for a certain amount of failure before a problem qualifies as an outage. For example, in the Amazon EC2, it is considered a true outage only if the entire user's instances within two availability zones (AZs) are down. That means that if a single AZ is down, or if the user is running in only a single AZ, the user is not covered by the SLA. However, a few CMO approaches support. There is a critical need for SLA violation prevention in order to avoid the need for service providers to pay penalties to consumers [5].

Existing Approaches like ACO (Ant Colony Optimization), Genetic Algorithm etc. are not provide long term optimal solution for data workload sharing & balancing problems. In short term data workload sharing & balancing solution, there is no assurance for the efficient execution for the next task is provided. A long term data workload sharing & balancing solution for the resource allocation problems is presented by the authors[14]. LB-BC (data workload sharing & balancing based on bayes and clustering) is regular usage from conduct the data workload sharing & balancing task.

Cloud Approach and its computation scenario or on-demand computing is a Para diagram where various on-demand services and usable components are offered for the users. In Cloud Approach and its computation scenario, simultaneous access of the usable components is conducted by the cloud users. That generates extra load for the system because of the load issues like fault tolerance, storage overhead, degrading performance are occurs. Thus effective data workload sharing & balancing Approach is required to provide better performance in cloud scenario. There are two type of data workload sharing & balancing Approaches either an open source data workload sharing & balancing where session switching or packet switching schemes are used or a pre-processor data workload sharing & balancing[15] .

Optimal data handling and processing of the usable components is one option from the available biggest issue in Cloud Approach and its computation scenario. Proper balancing of the nodes is required to provide flexible and scalable cloud service for the user. Load of the usable components is based on the factors like processing capacity, storage usage, access time etc. after calculating the status of the usable components and cloud users or nodes various data workload sharing & balancing schemes are used to provide a uninterrupted cloud service for the user [16].

Genetic algorithm and its variants are used to provide an optimize data workload sharing & balancing solution for the cloud users. But these Approach not able deal with exploration problems in the Cloud Approach and its computation scenario. A firefly algorithm to overcome the issues of the genetic algorithm and provide an enhanced functionality to access usable components over the cloud is presented. Firstly status of the cloud usable components and requests generated by the cloud users is listed. Data workload sharing & balancing operation on the basis of firefly algorithm is conducted. That Approach provides an optimal solution for the data workload sharing & balancing problem but the time limit for the operation is high.

Thus the section help in understanding of the previously given technique.

III. KEY SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing consists of applications, platforms and infrastructure segments. Each segment performs different operations and offers different products for businesses and individuals around the world. The business application includes Software as a Service (SAAS), Utility Computing, Web Services, and Platform as a Service (PAAS), Managed Service Providers (MSP), Service Commerce and Internet Integration. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure and mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. The given below are the various security concerns in a cloud computing environment.

- Access to Servers & Applications

- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management

Access to Servers & Applications: In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections which are not the case of cloud data centers. In cloud computing administrative access must be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access to data and monitor this access to maintain visibility of changes in system control. Data access issue is mainly related to security policies provided to the users while accessing the data. In a typical scenario, a small business organization can use a cloud provided by some other provider for carrying out its business processes. Some organization will have its own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations wherein some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users [9].

IV. ALGORTIHM USED

Blowfish is one of the most common public domain encryption algorithm provided by Bruce Schneier one of the worlds leading cryptologists, and the president of Counterpane Systems and a consulting firm specializing in cryptography and computer security

Blowfish encrypts 64-bits block cipher with variety length key and it contains two parts.

Data Encryption: It involves the iteration of a simple function of 16 times. Each round contains a key dependent permutation and data dependent substitution.

Subkey Generation: It involves converts the key up to 448 bits long to 4168 bits.

V. CONCLUSION

This paper gives a detailed study of Cryptography. Among those algorithms and concepts the security for the data has become highly important since the selling and buying of products over the open network occur very frequently. In this paper it has been surveyed about the existing works on the encryption techniques. This paper presents the performance evaluation of selected symmetric algorithms. The selected algorithm is Blowfish. In future we can use encryption techniques in such a way that it can consume less time and power of furthermore and high speed and minimum energy consumption.

REFEERENCES

[1] Sarita Kumari, A research Paper on Cryptography Encryption and Compression Techniques, Volume 6 Issue 4 April 2017.

[2] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. F. De Rose, and R. Buyya, CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms, Software - Practice and Experience, vol. 41, pp. 23-50, 2011.

[3] A. Jula, E. Sundararajan, and Z. Othman, Cloud computing service composition: A systematic literature review, Expert Systems with Applications, vol. 41, pp. 3809-3824, 2014.

[4] A. Abdelmaboud, D. N. A. Jawawi, I. Ghani, A. Elsafi, and B. Kitchenham, Quality of service approaches in cloud computing: A systematic

mapping study, Journal of Systems and Software, vol. 101, pp. 159-179, 3// 2015.

[5] V. C. Emeakaroha, M. A. S. Netto, R. N. Calheiros, I. Brandic, R. Buyya, and C. A. F. De Rose, Towards autonomic detection of SLA violations in Cloud infrastructures, Future Generation Computer Systems, vol. 28, pp. 1017-1029, 2012.

[6] Pancholi, V.R. proposed Enhancement of Cloud Computing Security.|Volume 2 | Issue 09 | February ISSN (online): 2349-6010(2016)

[7] Rashmi, Sahoo,G. Mehfuz,.S. in Securing Software as a Service Model of Cloud Computing Services and Architecture (IJCCSA), Vol.3, No.4, August (2013)

[8] Mehfuz, S. in Securing Software as a Service Model of Cloud Computing on big data analytics in Cloud Computing (IJCCSA), Vol.3, No.4, August (2013)

[9] Kumar, S. Proposed in Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications and Communication, Vol. 1, No. 4, December(2012)

[10] Padhy,R.V. proposed Cloud Computing: Security Science, Information Technology and challenging issues in cloud computing (IJCSITS) Vol. 1, No. 2, December (2011)

[11] Mohamed el. Ibrahim, Cloud computing challenges and characteristics, International Journal of recent trends in engineering and research.

[12] Mohamed A. Hussein, Cloud computing challenges and characteristics, International Journal of recent trends in engineering and research.

[13] Thota,S. In a data compression for the securing data elements in cloud computing Database Theory and Application database.20170401.01(2017)

[14] Shahrzad Aslanzadeh, Venkatesh Mahadevan, Christopher Mcdermid, Availability and Load Balancing in Cloud Computing, International Conference on Computer and Software Modeling IPCSIT vol.14 IACSIT Press, Singapore 2011.

[15] Sreenivas Velagapudi, M.Prathap and Kemal Mohammed, Load Balancing Techniques: Major Challenge in Cloud Computing – A Systematic Review,IEEE, International Conference on Electronics and Communication Systems (ICECS) - Coimbatore, India (2014).

[16] T. Kokilavani and Dr. D.I. George Amalarethinam, Load Balanced Min-Min Algorithm for Static Meta-Task Scheduling in Grid Computing, International Journal of Computer Applications Volume 20– No.2, pp.0975-8887, April 2011.