Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 10, October -2017

AES encryption and hashing used for data Security on Amazon Web Services

[1]Richa Gautam, [2]Madhukar Dubey, [3]Vivek Jain

[1]*Research Scholar of CSE/IT ,SRCEM, Banmore, India*
[2,3]*Dept. of CSE , SRCEM, Banmore, India*

Abstract— *Cloud computing is the conveyance of processing as an administration instead of an item, whereby shared assets, programming, and data are given to PCs and different gadgets as an utility (like the power framework) over a system (commonly the Internet). Mists can be named open, private or half breed. Distributed computing, or in easier shorthand essentially "the cloud", moreover focuses on opening up the ampleness of the regular resources. Cloudsresources are regularly shared by different customers and in addition effectively reallocated per ask. This can work for circulating advantages for customers.. In our proposed work, we are giving security by applying a hash work for giving confirmation to information so that nobody can transform it before transferring and afterward scrambling the information to shield it from the unapproved get to. At that point we transfer that information to the server of Amazon Web Services(AWS). This gives security to the PaaS model and makes it a more effective cloud demonstrates.*

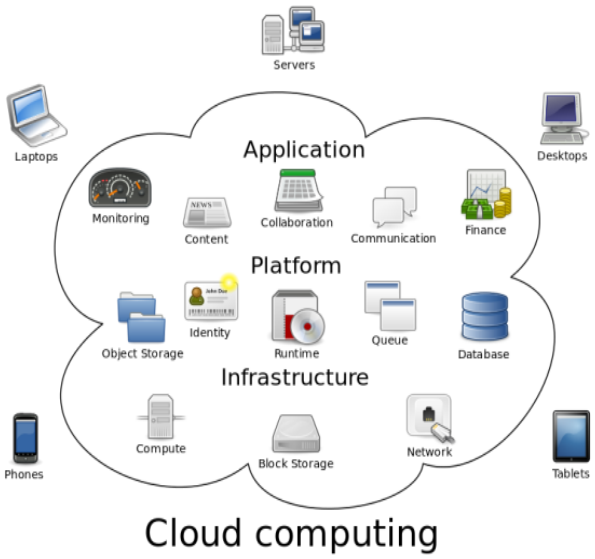
Keywords- *Cloud Computing, Cloud Service models, Cloud deployment models, Characteristics*.

I. INTRODUCTION

Cloud computing is the conveyance of processing as an administration instead of an item, whereby shared assets, programming, and data are given to PCs and different gadgets as an utility (like the power framework) over a system (commonly the Internet). Mists can be named open, private or half breed. Distributed computing, or in easier shorthand basically "the cloud", also focuses on increasing the sufficiency of the regular resources. Cloud resources are regularly shared by different customers and additionally effectively reallocated per ask. This can work for circulating advantages for customers.. In our proposed work, we are giving security by applying a hash work for giving confirmation to information so that nobody can transform it before transferring and afterward scrambling the information to shield it from the unapproved get to. At that point we transfer that information to the server of Amazon WebServices(AWS). This gives security to the PaaS model and makes it a more effective cloud demonstrates.

A cloud computing innovation is frequently utilized nowadays as it is a rising term of figuring utilities. Cloud choices are alluring different enterprises in all cases to know its significance attributes and programming offerings. The fundamental attributes that distributed computing offers today are:

- On-request self administration
- Broad system get to
- Resource pooling
- Rapid versatility
- Measured administration



A. Characteristics Of Cloud Computing

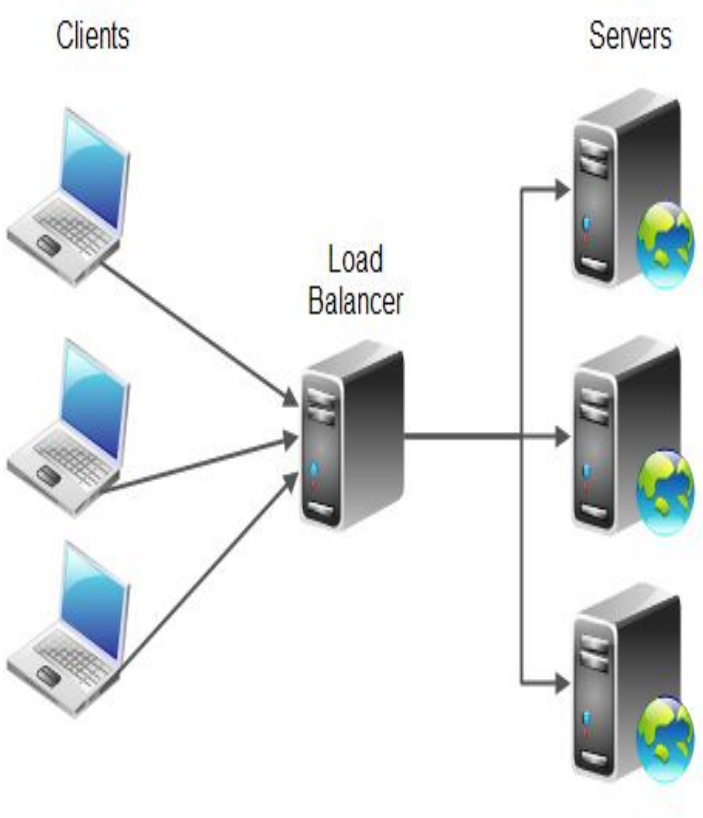
1) CLOUD SERVICE MODEL

Cloud computing is a term that portrays a wide scope of administrations. Since the cloud is a gathering of administrations, associations pick where, when, and how they utilize distributed computing.
In this paper we clarify the three distinct sorts of administration models:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as an services (IaaS)

2) LOAD BALANCING

With the expanding notoriety of distributed computing, the measure of preparing that is being done in the Distributed computing is rising quickly. As the solicitations of the customers can be irregular to hubs, in this manner the heap on every hub can likewise fluctuate i.e. a few hubs are over-burden and some are under stacked which specifically influences the nature of cloud administrations. Subsequently, some heap adjusting instrument is expected to guarantee that each figuring asset is conveyed productively and decently. Stack Adjusting is a PC organizing technique to circulate workload over numerous PCs or a PC bunch, arrange joins, focal handling units, plate drives, or different assets, to accomplish ideal asset use, augment throughput, limit reaction time, and evade over-burden [6]. It is an instrument that circulates the dynamic neighborhood workload equitably over every one of the hubs in the entire cloud to accomplish a high client fulfillment and asset usage, subsequently enhancing the general execution and asset utility of the framework. It additionally guarantees that each processing asset is disseminated effectively and reasonable, forestalls bottlenecks and bomb over.



B. CLASSIFICATION OF LOAD BALANCING ALGORITHMS

In general, load balancing algorithms follow two major classifications [7]:

1) STATIC ALGORITHAM

A static load balancing calculation does not consider the past state or conduct of a hub while appropriating the heap. In this approach earlier learning of framework is required. This majorly affects the general framework execution because of the unusualness of load variance of the disseminated framework. It doesn't rely on current condition of framework. Static calculations are substantially easier when contrasted with element calculations.

2) DYNAMIC ALGORITHAM

THIS approach considers the present condition of the framework amid load balancing choices and is more appropriate for broadly conveyed frameworks, for example, distributed computing [8]. The dynamic load adjusting calculation is

connected either as a circulated or non-disseminated. The benefit of utilizing element stack adjusting is that if any hub falls flat, it won't end the framework; it will just influence the framework execution. In a dynamic load adjusted framework, the hubs can associate with each other producing more messages when contrasted with a non-conveyed condition

C. GOALS OF LOAD BALACING

- To enhance the execution significantly
- To have a reinforcement arrange on the off chance that the framework bombs even mostly
- To keep up the framework solidness
- To suit future change in the framework

D. LOAD BALANCING CHALLENGES IN THE DISTRIBUTED COMPUTING

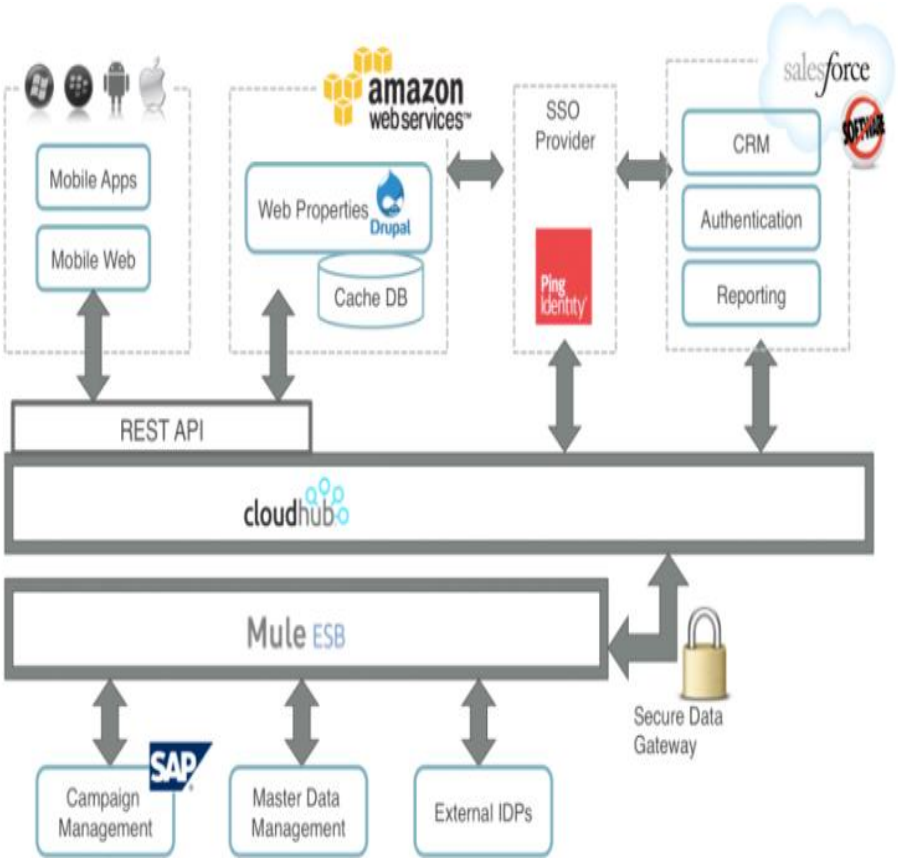
In spite of the fact that distributed computing has been generally embraced. Investigate in distributed computing is still in its initial stages, and some logical difficulties stay unsolved by established researchers, especially stack adjusting challenges:

- Automated Administration Provisioning
- Virtual Machines Relocation:
- Energy Administration
- Put Away Information Administration
- Emergence Of Little Server Farms For Distributed Computing

E. AMAZON WEB SERVICES (AWS)

Amazon Web Services (AWS) is an extensive, advancing distributed computing stage gave by Amazon.com. Web administrations are at times called cloud administrations or remote registering administrations. The primary AWS offerings were propelled in 2006 to give online administrations to sites and customer side applications.

To limit the effect of blackouts and guarantee heartiness of the framework, AWS is topographically differentiated into districts. These locales have focal center points in the Eastern USA, Western USA (two areas), Brazil, Ireland, Singapore, Japan, and Australia. Every district contains different littler geographic regions called accessibility zones.



The developing AWS gathering offers more than three dozen differing administrations including

- Cloud drive,
- Cloud search, An Scalable
- Dynamo Database (Otherwise Called Dynamo Or Ddb)
- Elastic Compute Cloud

- Elastic cache
- Mechanical Turk,

F. SECURITY

Any system condition requires some security estimations with a specific end goal to work proficiently. Many assignments are to be mulled over, for example, information security in the trade procedure, information protection while capacity, get to consents, benefit levels, and keeping up the system sage from external malevolent interlopers. Lattices are no special case; distinctive safety efforts are to be taken including confirmation, approval, and secure record sharing. In any case, the security prerequisites in a framework domain require the support of adaptable, dynamic, conveyed virtual associations (VOs), which are cross-hierarchical joint efforts. Being scattered more than a few topographical territories, VOs increment security dangers. Moreover, they confuse the administration of security assignments because of their dynamic nature. A security method in a network ought to give a few qualities. To begin with, is ought to empower the VOs to give information coordination and interoperability. Moreover, a framework security method shouldn't upset the formation of VOs andthink about their dynamic nature. At long last, it ought to keep up the capacity of the end clients to progressively make new administrations. In basic words, security must be guaranteed without influencing the execution of the brace. The issue here or the point that is under review by this paper is the endeavors of actualizing and executing the security errands and schedules, these assignments ought to be overseen in a way that it not influencing the effective execution of the Grid Environment. Notwithstanding the security conventions and models that are taken in the Grid it is requiring some exertion from the hubs to play out these assignments to secure the correspondence and information sharing. Likewise with the essential of the field that is utilizing the Grid Environment the security will build substantially higher and the hubs will perform greater security assignments.

As we are moving into web based cloud show, it requires extraordinary accentuation on Data Security and Privacy. Information misfortune or Data spillage can have extreme effect on business, brand and trust of an association. Information spill anticipation is considered as most essential component with 88% of Critical and Very vital difficulties. Additionally Data Segregation and Protection has 92% effect on security challenges.

G. ENCRYPTION AND DECRIPTION

In cryptography, encryption is the way toward encoding messages or data such that exclusive approved gatherings can get to it. Encryption does not of itself avoid obstruction, but rather denies the message substance to the interceptor. In an encryption plan, the proposed data or message, alluded to as plaintext, is encoded utilizing an encryption calculation, creating cipher text that must be perused if unscrambled. The reason for encryption is to guarantee that lone some person who is approved to get to information (e.g. an instant message or a document), will have the capacity to peruse it, utilizing the unscrambling key. Some person who is not approved can be rejected, in light of the fact that he or she doesn't have the required key, without which it is difficult to peruse the scrambled data.

Decoding is the way toward taking encoded or scrambled content or other information and changing over it once again into content that you or the PC can read and get it. This term could be utilized to depict a technique for un-encoding the information physically or with un-scrambling the information utilizing the correct codes or keys. Information might be encoded to make it troublesome for somebody to take the data. A few organizations likewise encode information for general security of organization information and competitive innovations. In the event that this information should be visible, it might require decoding. On the off chance that an unscrambling password or key is not accessible, exceptional programming might be expected to decode the information utilizing calculations to split the decoding and make the information meaningful.

H. TECHNIQUE OF ENCRYPTION AND DECRIPTION

AWS Multi-Factor Authentication (MFA) is a straightforward best practice that includes an additional layer of security on top of your client name and secret key. With MFA empowered, when a client signs into an AWS site, they will be provoked for their client name and secret word (the primary variable—what they know), and also for a confirmation code from their AWS MFA gadget (the second component—what they have). Taken together, these various components give expanded security to your AWS account settings and assets.

You can empower MFA for your AWS account and for individual IAM clients you have made under your record. MFA can be likewise be utilized to control access to AWS benefit APIs. After you've gotten a bolstered equipment or virtual MFA gadget, AWS does not charge any extra expenses for utilizing MFA

There are three steps involved – establishing trust between accounts, configuring MFA devices for users, and performing privileged actions. Let’s dive in to the details of each.

I. AUTHENTICATION FACTORS

A confirmation variable is a classification of qualification utilized for character check. For MFA, each extra variable is planned to build the affirmation that an element required in some sort of correspondence or asking for access to some framework is who, for sure, they are proclaimed to be. The three most regular classifications are frequently portrayed as something you know (the learning component), something youhave (the ownership element) and something you are (the inherence figure).

- Learning elements
- Ownership elements

- Inherence components
- Area components
- Time elements

J. VIRTUAL MFA APPLICATIONS

Applications for your Smartphone can be installed from the application store that is specific to your phone type. The following table lists some applications for different Smartphone types.

- Android
- iPhone
- Windows Phone
- Blackberry

K. HASHING

Hashing is the change of a series of characters into a normally shorter settled length esteem or key that speaks to the first string. Hashing is utilized to record and recover things in a database since it is quicker to discover the thing utilizing the shorter hashed key than to discover it utilizing the first esteem. It is likewise utilized as a part of numerous encryption calculations.

As a straightforward case of the utilizing of hashing in databases, a gathering of individuals could be masterminded in a database like this

The hash capacity is utilized to file the first esteem or key and afterward utilized later each time the information related with the esteem or key is to be recovered. Along these lines, hashing is dependably a restricted operation. There's no compelling reason to "figure out" the hash work by dissecting the hashed values. Truth be told, the perfect hash work can't be inferred by such investigation. A decent hash work additionally ought not to create a similar hash an incentive from two distinct data sources. On the off chance that it does, this is known as a crash. A hash capacity that offers to a great degree generally safe of impact might be viewed as satisfactory.

L. OBJECTIVE OF THE WORK

At the point when numerous associations share assets there is a danger of information abuse. In this way, to stay away from hazard it is important to secure information archives and furthermore the information that includes stockpiling, travel or process. Insurance of information is the most imperative difficulties in distributed computing. To improve the security in distributed computing, it is critical to give validation, approval and get to control for information put away in cloud. The three primary ranges in information security are

1) Confidentiality

Top vulnerabilities are to be checked to guarantee that information is shielded from any assaults. So security test must be done to shield information from vindictive client, for example, Cross-site Scripting, Access Control systems etc..,.

2) Intrigirity

To give security to the customer information, a thin customer is utilized where just couples of assets are accessible. Clients ought not to store their own information, for example, passwords with the goal that trustworthiness can be guaranteed.

3) Accessibility

Availability is the most vital issue in a few associations confronting downtime as a noteworthy issue. It relies on upon the understanding between the seller and the customer.

II. LITERATURE SURVEY

J. Hu et al. [19] proposed a scheduling strategy on load balancing of VM resources that uses historical data and current state of the system. Proposed strategy achieves the best load balancing and reduced dynamic migration by using a genetic algorithm.

Mohamed E.M et.al [20] presented the data security model of cloud computing based on the study of cloud architecture. They also implemented software to enhance the work in Data Security model for cloud computing.

LBVS H. Liu et al. [21] proposed a load balancing virtual storage strategy (LBVS) that provides a large scale net data storage model and Storage as a Service model based on Cloud Storage. The Storage virtualization is achieved using an architecture that is three-layered and load balancing is achieved using two load balancing modules. It helps in improving the efficiency.

A.Singh et al. [22] proposed a novel load balancing algorithm called VectorDot. This algorithm handles the hierarchical complexity of the datacenter and multidimensionality of resource loads across servers network switches and storage in an agile data center that has integrated server and storage virtualization technologies.

Stanojevic et al. [23] proposed a mechanism CARTON for cloud control that unifies the use of LB and DRL. The LB (Load Balancing) is used to equally distribute the jobs to different servers so that the associated costs can be minimized and DRL (Distributed Rate Limiting) is used to make sure that the resources are distributed in a way to keep a fair resource allocation.

Y. Zhao et al. [24] in this paper addressed the problem of intra-cloud load balancing amongst physical hosts by adaptive live migration of virtual machines. The load balancing model is designed and implemented to reduce virtual machines migration time by shared storage to balance load amongst servers according to their processor or IO usage.

H. Mehta et al. [24] Proposed a new content aware load balancing policy named as work-load and client aware policy (WCAP). Proposed work uses a parameter named as USP to specify the unique and special property of the requests as well as computing nodes. The USP helps the scheduler to decide the best suitable node for processing the requests.

Y. Lua et al. [25] proposed a Join-Idle-Queue load balancing algorithm for dynamically scalable web services. Work provides large-scale load balancing with distributed dispatchers by, first load balancing idle processors across dispatchers for the availability of idle processors at each dispatcher and then, assigning jobs to processors to reduce average queue length at each processor.

V. Nae et al. [25] presented an event driven load balancing algorithm for real-time Massively Multiplayer Online Games (MMOG). The algorithm after receiving capacity events as input, also analysis its components in context of the resources and the global state of the game session, then generating the game session load balancing actions.

Punit Gupta et al. [26] proposed a new load balancing algorithm for better distribution of load and further enhancing the QoS. In this paper, a trust model has been presented which is based on current trust models and it uses initialization time, Machine Instruction per Second (MIPS) and fault rate parameters to calculate trust value for each data center. In this algorithm, users and data centers are categorized into two groups: trusted and untrusted groups. According to these groups, the overloaded nodes' VMs which belong to trusted or untrusted users can migrate to trusted or untrusted data centers that are under-loaded and suitable for migrating.

Osman Scrod et al. [27] stated that virtualization have some negative effects on HPC application. In the paper, a load balancing algorithm is proposed to achieve load balancing for tightly coupled parallel and HPC application executions in virtualized and cloud computing environments. For balancing the workloads in this proposed algorithm, processing cores is divided into two over heap (overloaded) and under Set (under-loaded) cores. Then the biggest task from most overloaded core will transfer to a suitable under-loaded core. This process is repeated until no overloaded cores are left. This load balancing algorithm is suitable for HPC applications which run iteratively and also there is interference from different VMs on the same node in their executions.

Shu-Ching Wang et al. [28] proposed a two phases scheduling and load balancing algorithm which is presented in a three level cloud computing network. The algorithm is a combination approach of two OLB (Opportunistic Load Balancing) and LBMM (Load Balancing Min-Min). The algorithm is shown in a three level cloud computing network as follow in the third level, there are service nodes. Level two which consists of some service mangers is used for dividing tasks to some subtasks and assigning them to appropriate service nodes. Finally, in the first level, there is a request manager which receives the incoming workloads and sends tasks to appropriate nodes. This algorithm uses the agent-based method for gathering required information. The proposed load balancer is represented in two phases which uses the OLB algorithm for assigning tasks to service managers and in the next phase the LBMM is used to assign subtasks to the third level.

Brototi Mandal et al. [29] proposed a load balancing algorithm that it was soft computing based. Stochastic hill climbing is a variant of hill climbing algorithm that is an incomplete approach for solving optimization problems. Because the represented load balancing algorithm is a centralized algorithm and therefore dealing with bottleneck problem, the solving optimization problem has taken into consideration for an efficient distribution of system workload.

Y. Fang et al. [20] discussed a two-level task scheduling mechanism based on load balancing to meet dynamic requirements of users and obtain high resource utilization. Algorithm achieves load balancing by first mapping tasks to virtual machines and then virtual machines to host resources thereby improving the task response time, and resource utilization also overall performance of the Cloud computing environment.

M. Randles et al. [21] investigated a decentralized honey bee based load balancing technique that is a nature inspired algorithm for self-organization. Algorithm achieves global load balancing through local server actions. Performance of the system is enhanced with increased system diversity but throughput is not increased with an increase in system size. This is best suited for the conditions where the diverse population of service types is required.

M. Randles et al. [21] investigated a distributed and scalable load balancing approach that uses random sampling of the system domain to achieve self-Organization thus balancing the load across all nodes of the system.

M. Randles et al. [21] investigated a self-aggregation load balancing technique that is a self-aggregation algorithm to optimize job assignments by connecting similar services using local re-wiring. Overall performance of the system is enhanced with high resources thereby in-creasing the throughput by using these resources effectively.

Z. Zhang et al. [22] proposed a load balancing mechanism based on ant colony and complex network theory (ACCLB) in an open cloud computing federation. Proposed algorithm uses small-world and scale-free characteristics of a complex network to achieve better load balancing. Proposed technique overcomes heterogeneity is adaptive to dynamic environments and has good scalability Hence helps in improving the performance of the system.

S.-C. Wang et al. [23] proposed a two-phase scheduling algorithm that combines OLB (Opportunistic Load Balancing) and LBMM (Load Balance Min-Min) scheduling algorithms to utilize better executing efficiency and maintain the load balancing of the system. This OLB scheduling algorithm keeps every node in working state to achieve the goal of load balance and LBMM scheduling Algorithm is utilized to minimize the execution time of each task on the node thereby minimizing the overall completion time..

III. **PROPOSE WORK**

3.1 Problem Statement

In existing work, they used MFA (Multi factor Authentication) which is not a very secure technique. MFA is used didn't change the data and it only generates a hash value which is sent with the original data. Since data can be changed during transmission by any unauthorized users so this is not an efficient method in the network.

A confirmation variable is a classification of qualification utilized for character check. For MFA, each extra variable is planned to build the affirmation that an element required in some sort of correspondence or asking for access to some framework is who, for sure, they are proclaimed to be. The three most regular classifications are frequently portrayed as something you know (the learning component), something you have (the ownership element) and something you are (the inherence figure).

3.2Problem Justification

In existing work, they used MFA which is not a very secure technique. Secure Hash Algorithms didn't change the data and it only generates a hash value which is sent with the original data. Since data can be changed during transmission by any unauthorized users so this is not an efficient method in the network.

- **The AWS Shared Security Model and Amazon EC2**

A key part of the AWS shared security display is the capacity to secure remote access to your Amazon EC2 occurrences. On account of Linux servers, remote access more often than not implies setting up an association with the server by utilizing the SSH convention. Verification ordinarily happens either by giving a client name and watchword or by giving a private key that is checked against an open key on the server. As a matter of course, most Amazon EC2 occurrences utilize the last approach for client verification: when you initially dispatch an EC2 case, you are asked to alternatively allot it a key combine. AWS utilizes the client name alongside the PEM document that is related with the key combine to confirm with the server and open a SSH session.

Reducing risk with two-factor authentication

Two-factor verification, or multi-factor confirmation (MFA), requires a client to give different evidences of character to access an asset. For instance, you can design access to the AWS Management Console to expect clients to enter a client name and secret key notwithstanding a turning code from an equipment or programming MFA gadget. This approach is likewise progressively used to include an additional layer of security for access to servers and workstations, where a private key or a client name/secret key must be given notwithstanding a confirmation code from a MFA gadget before a session is opened on the working framework.

One utilize case that we find in the field is two-factor verification utilized on "hop" or "bastion" hosts to give expanded security on EC2 occurrences that are utilized for SSH port sending or aberrant access to inside confronting administrations. Another basic utilize case is to arrangement EC2 occasions with two-factor validation and appoint them AWS Identity and Access Management (AWS IAM) parts with secured approaches. Support and operations groups would then be able to safely associate with these EC2 occasions and utilize the AWS CLI and SDKs without supplying accreditations.

You generally open yourself to a level of hazard when you work a server with intuitive logins empowered. Given that you sufficiently secure your PEM document and that SSH is effectively set up on your EC2 occurrences, key-based validation is generally a change over basic client name/secret key confirmation since it is less vulnerable to savage power assaults. Shockingly, PEM records, similar to passwords, can be shared and inadvertently left unsecured. Including an additional layer of security, for example, two-factor validation, is a decent approach to moderate this whether you are utilizing secret key or key-based verification as your essential factor of confirmation.

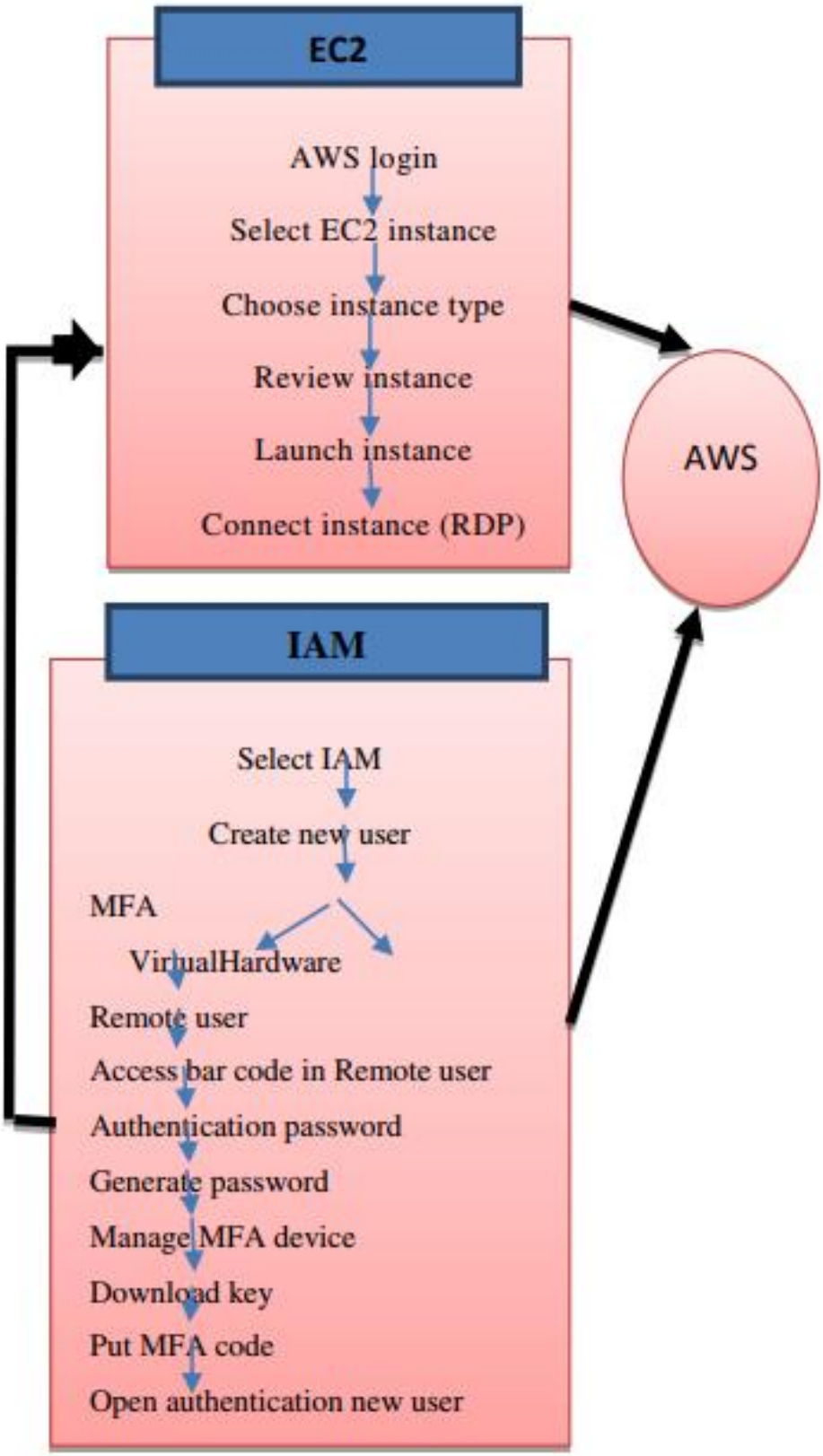
- ***Time-based One-time Passwords (TOTP)***

Google Authenticator executes the TOTP calculation from RFC 6238. When you introduce the Google Authenticator application on your Amazon EC2 case, AWS creates a mystery key. This mystery key is then imparted to a moment gadget of your decision, for example, an application running on your cell phone. The trading of the mystery key more often than not happens when you utilize the versatile application to examine a QR code produced by Google Authenticator.

Once the mystery enter is put away in the versatile application, it joins it with the current timestamp by utilizing a cryptographic hash capacity to produce one-time passwords (OTPs). An OTP is the second confirmation factor that you will be provoked to enter after effectively verifying by utilizing a client name and secret word or PEM record. The OTP is hard to trade off in light of the fact that it auto-pivots over the long haul, generally at regular intervals, and is created by utilizing a gadget that you as a rule keep with you constantly, (for example, your telephone).

You can look over an assortment of TOTP-good versatile applications to store the TOTP mystery key and produce the OTP. In this post, we demonstrate to utilize Google Authenticator on the server-side and AWS Virtual MFA as the TOTP-perfect portable application to produce the OTPs for confirmation. Different cases of mainstream TOTP-perfect portable applications incorporate the official versatile application of Google Authenticator, the portable application of Duo Security, Duo Mobile, and Authenticator.

3.3 PROPOSED MODEL



The aim of this study is to provide a conceptual model that can assist in defining and analyzing the interactive documentary**.** This type of documentary has emerged as a result of the advanced technology and the transformation from Web. The technological features have progressively activated the latent interactive aspects in the linear documentary such as two-way communication in the real time. Those features have also reformulated the relationship between the

viewer, the author and the narrative. The presented model in this study provides the fundamental components of the interactive documentary: user, interactivity, and documentary. It analyses the interactive documentary in the terms of these components in order to propose a convenient definition

3.4 Proposed Algorithm

Proposed algorithm is divide two sections:

i) EC2 instances
ii) IAM (Identity Access Management)

EC2 INSTANCES

Step 1: Registration in AWS
Step 2: Login in AWS
Step 3: Home page services
Step 4: Select EC2 Instances
Step 5: Create instance
Step 6: Choose instances (choose as your required)
Step 7: Choose an instance type
Step 8: Configuration instance Details.
Step 9: Add storage in instances
Step 10: Adding tag and key-value
Step 11: Configure security groups
Step 12: Review instance Launch
Step 13: Select an existing key pair or create a new key pair
Step 14: Launch instance and connect instance
Step 15: Connect to your instance Remote desktop file (RDF)
Step 16: Connect to your instance with get password
Step 17: Connect to your instance decrypt password
Step 18: Connect to decrypt password and select password
Step 19: Paste the password
Step 20: Connect to RDF with Remote desktop connection
Step 21: The identity of the remote computer cannot be verified. Do you want to correct anyway.
Step 22: Connect to remote computer

IAM (IDENTITY ACCESS MANAGEMENT)

Step 1: Selected to IAM (Identity and Access Management)
Step 2: Welcome page to IAM
Step 3: Add new user in IAM
Step 4: Set user details
Step 5: Add Groups details
Step 6: Create group and permission
Step 7: Review services
Step 8: Complete the user services.
Step 9: Create IAM New_User1
Step 10: Summary of permission IAM
Step 11: Summary of group IAM
Step 12: Summery credentials of MFA
Step 13: Selected to MFA Device (Virtual or Hardware)
Step 14: Manage MFA Virtual Device
Step 15: Access to barcode in mobile phone.
Step 16: Generate Authenticate MFA Password
Step 17: Manage MFA Device to successfully associated with your account
Step 18: Download access Key
Step 19: Save to Access in key and URL in MS Excel sheet
Step 20: Put the URL and Access account to IAM user
Step 21: Put the MFA code (This code generated by Google authenticator App)
Step 22: Put AWS sign In with Authentication Device
Step 23ss: Open authenticate New_user1 using MFA

III. CONCLUSION

Cloud computing gives everything as an administration and are conveyed as open, private, group, and crossover mists. Despite the fact that distributed computing is the new rising innovation that shows a decent number of advantages to the clients, it confronts loads of security difficulties. In this paper information security difficulties and arrangements are accommodated these difficulties to beat the hazard required in distributed computing. In our proposed work, we are giving security by applying a hash work for giving confirmation to information so that nobody can transform it before transferring and after that scrambling the information to shield it from the unapproved get to. At that point we transfer that information to the server of Amazon Web Services (AWS). This gives security to the PaaS model and makes it a more effective cloud display.

In future scope if your multi-factor authentication (MFA) device is lost, damaged, or not working, you can sign in using alternative methods of authentication. This means that if you can't sign in with your MFA device, you can sign in by verifying your identity using the email and phone that are registered with your account. If the device appears to be functioning properly, but you cannot use it to access your AWS resources, then it simply might be out of synchronization with the AWS system. For information about synchronizing an MFA device, see Devices. Before you sign in using alternative factors of authentication, make sure that you have access to the email and phone number that are associated with your account.

- Required instrument (Mobile phone)
- Attached E-mail with application.
- Only 30 sec Generated so increase time duration

v. REFERENCES

[1] A. Beloglazov and R. Buyya, *"Energy efficient resource management in virtualized cloud data centers"*, Proc. 10th IEEE/ACM international conference on cluster, cloud and grid computing, 826-83, 2010.

[2] Qi Zhang, Lu Chengand RaoufBoutaba, *"Cloud computing: state-of-the-art and research challenges"*, Journal of Internet Services and Applications, 7-18, 2010.

[3] Amandeep Kaur Sidhu and SupriyaKinger, *"Analysis of Load Balancing Techniques in Cloud Computing"*, International Journal of Computers & Technology,737-741, 2013.

[4] R. Mishra and A. Jaiswal, *"Ant colony optimization: A solution of load balancing in cloud"*, International Journal of Web & Semantic Technology, 33, 2012.

[5] E. Caron, L. Rodero-Merino, F. Desprez and A. Muresan, *"Auto-scaling, load balancing and monitoring in commercial and opensource clouds"*, 2012.

[6] P.Mathur, *"Cloud Computing: new challenge to the entire computer industry"*, 1stInternational conference on parallel, distributed and grid computing, pp978-1- 4244-767, 2010.

[7] U.Chatterjee, *"A Study on Efficient Load Balancing Algorithms in Cloud computing Environment"*, International Journal of Current Engineering and Technology, Vol.3, 11 November 2013.

[8] S.Mohinder, R,Ramesh and D.Powar, *"Analysis of Load Balancers in Cloud Computing"*, International Academy of Science, Engineering & Technology, vol.2, May 2013.

[9] B.KalaiSelvi and Dr.L.Mary Immaculate Sheela,*"A Survey of Load Balancing Algorithms using VM"*, International Journal of Advancements in Research & Technology, Volume 3, Issue 8, August-2014.

[10]. Buyya R., R. Ranjan and RN. Calheiros, *"InterCloud: Utility-oriented federation of cloud computing environments for scaling of application services"*,in proc. 10th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP), Busan, South Korea, 2010.

[11]. Foster, I., Y. Zhao, I. Raicu and S. Lu, *"Cloud Computing and Grid Computing 360-degree compared",* in proc. Grid Computing Environments Workshop, pp: 99-106, 2008.

[12]. Grosu, D., A.T. Chronopoulos and M. Leung, *"Cooperative load balancing in distributed systems",* in Concurrency and Computation: Practice and Experience", Vol. 20, No. 16, pp: 1953-1976, 2008.

[13]. Ranjan, R., L. Zhao, X. Wu, A. Liu, A. Quiroz and M. Parashar, *"Peer to- peer cloud provisioning: Service discovery and load-balancing",* in Cloud Computing Principles, Systems and Applications, pp: 195-217,2010.

[14] G. Lee and J. Choi, *"A Survey of Multipath Routing for Traffic Engineering",* 2002.[http://vega.icu.ac.kr/~gmlee/research/]

[15] A. Toguyeni and O. Korbaa, *"DiffServ Aware MPLS Traffic Engineering for ISP Networks: State of the Art and New Trends",* Journal of Telecommunications and Information Technology, Vol. 1, pp. 5-13,2009.

[16] Amit Garg *"A Literature Review of Various Load Balancing techniques in Cloud Computing Environment",* International Journal of Enhanced Research in Management & Computer Applications ISSN: 2319-7471, Vol. 5 Issue 2, February-2016.

[17] Rajesh Kumar, Charanjit Singh *"Survey: Cloud Partitioning Using Load Balancing Approach For Public Cloud Infrastructure",* (ISRA), April, 2015.

[18] NajlaaAlHuwaishel and Soha S. Zaghloul,*"A Technique for Load-Balanced Management of Security Tasks Load in Grids"*, 978-1-4673-5943-6/13/$31.00 ©2013 IEEE.

[19] Hu J., Gu J., Sun G. and Zhao T., 3rd International Symposium on Parallel Architectures, Algorithms and Programming, 89-96, 2010.
[20] EmanM.Mohamed, Hatem S Abdelkader, Sherif EI Etriby, *"Enhanced Data Security Model for Cloud Computing*", 8th International Conference on Informatics and Systems(INFOS), Cairo, p.12-17,May 2012.
[21] Fang Y., Wang F. and GeJ.,Lecture Notes in Computer Science, 6318, 271-277,2010.
[22] Singh A., Korupolu M. and Mohapatra D., ACM/IEEE conference on Supercomputing, 2008.
[23] Stanojevic R. and Shorten R., IEEE ICC, 1-6, 2009.
[24] Zhao Y. and Huang W., 5th International Joint Conference on INC, IMS and IDC, 170-175, 2009.
[25] Nae V., Prodan R. and Fahringer T., 11th IEEE/ACM International Conference on Grid Computing (Grid), 9-17,2010.
[26] Gupta, P., M.K. Goyal, and P. Kumar. Trust and reliability based load balancing algorithm for cloud IaaS. in Advance Computing Conference (IACC), 2013 IEEE 3rd International. 2013. IEEE.
[27] Sarood, O., A. Gupta, and L.V. Kale. Cloud Friendly Load Balancing for HPC Applications: Preliminary Work. in Parallel Processing Workshops (ICPPW), 2012 41st International Conference on. 2012. IEEE.
[28] Wang, S. C.,Towards a load balancing in a threelevel cloud computing network. in Computer

