Conceivement of a Schema Assimilating a Stronghold in the Cloud Computing Realm

Julian Menezes.R, Jesu Jayarin.P

Abstract*: Within a quintessential Cloud environment 'n' number of divergent entities, to name a few we have Hardware Infrastructure, Lines of Codes, Updated Softwares to hover over a particular Hardware, RJ45 Cabling crimped Ethernet Wires, and the other services which are related to the Cloud come together in unison to overture 'n' services coupled with Computers, whilst Network of Computers, along with Virtual Private Networking gives out the pathway required for the provisioning of utilities. The breach in Jericho's Wall, equivalent in the Cloud demarcates the prosperity of the Cloud in terms of "Presentability of Resources in terms of Infrastructure, Bandwidth, Storage, etc...as and when it is required by the end-user, and the performance of the above facilities to place a controllable entity in order to Manage the same". We have a presumption that the Information Technology as well as a particular firm's certainty resolution provided in this era does not suffice to conquer the issues arising due to solidness in the Cloud. Our research probes the tasks and affairs of certainty burdens of the Cloud via variant classic and innovative resolutions. Variant inspections and specific Blueprint for inculcating various validity ideas, crafts and rule for the Cloud, with a special boom light focus on Platform as a Service, and Infrastructure as a Service. The Blueprint that which we are going to bring forth is going to be accepted universally, with independence to the variant Cloud Deployment entities. The aforementioned statements should provide an Admin with a hold on the Cloud Environment, whilst inculcating a unique resolution to combat a peril. Based on the data extracted from various trial and error methods, the cost-to-benefit analysis can be estimated by the Cloud Provider.

Index Terms: Cloud computing, Data security, User behavior, Decoy technology, Fingerprint authentication, Face recognition.

I. INTRODUCTION

In technical jargons we can describe the Cloud as a mainstay of computing habitat which is distributed in nature inculcating entities to name a few we have the pre-mentioned Infrastructure, Codings, Drivers, Internetwork of Computers put together with services. A defiance occurs when the aforementioned entities are getting clawed via a public Internet Protocol address from the Network of Computers. Although the given entities are held under the fort knox of private authority, loop holes still exist. The Network of Computers or a Virtual Private Network nor one among the other gives away a spinal support to convey the attributes given out by the Cloud. The primitives of services which formed in the conceivement of the Cloud were Software as a Service, Platform as a Service, and Infrastructure as a Service. The Cloud is showcased as the teleportation of ancient computing to the present but he only variant being the evolution. This takes care of urgent needs of the end-user when sufficing data getting stored in the Hard Disk Drive, Commencement of an App, refinement of Digital Data, keeping sensitive Data available to the end-user, Digital Information statics and much more. In terms of using power in our homes, there exists a meter to supervise the hourly delivery of electricity for our day to day activities, likewise the utilization of assets is supervised in the Cloud to achieve a reduction of expenditure in terms of HDD and Processor. Nonetheless, sans the required Test Cases for the attributes like the competence, asset, accountability and last but not the least the gilt-edge, the Cloud would transform into a hideout for fraud, defamation and slandering. The certainty of the Cloud realm handles the problems and susceptibility of the Cloud to safe guard the Computing Habitat. The unconventional Blueprint and functioning of the Cloud breaches the shield of protection, for the ingress of variant certainty and solitude penalties. The trivial essence of the Cloud in providing an Infrastructure for various end-users, metamorphosis of physical to logical, and the last attribute prolixity gives a path way for various Intrusions related to armament. The certainty in the Cloud aids in transporting pliancy for a variant of threats executed to break the furtiveness, rectitude, obtainability of Digital data respective of the Cloud and the end-user. For the enablement of ancient certainty in the Cloud, the Sending Machine as well as the Receiving Machine ought to act accordingly, inculcating a blueprint which is coherent for taking care of the blocks which peeks out due to certainty. To attenuate the issues of certainty in the Cloud the ancient blacklisted outlook ought to be shunned whilst kicking in the novel white listed ideals. Our perspective points out the fact, that we can place our trust in a machinery if it functions without any technical glitches for a limited period of time. Likewise we would say that the CSPs can be trusted on the attributes via the times a system undergoes an update, average time when the machinery is down for maintenance, any history of Intrusions in the past [1]. The certainty of the Cloud deteriorates from 'primary broker' trouble [2]. The other trivial issues naming conglomeration of clients' Logical replica of Physical Machines inside a Physical Infrastucture which is shared leads to hazards related to certainty to the connected Clients whilst incrementing the wages to the Provider of the Cloud [3]. To form a habitat of the Cloud with key stone on strong hold from the point of view of the user, it is trivial that we delve into the blocks and problems related to certainty in the Cloud realm like:

Revised Manuscript Received on December 22, 2018.

Julian Menezes.R, Research Scholar, Anna University, Chennai 600025, INDIA,researchau1811@gmail.com

Dr. Jesu Jayarin.P, Associate Professor, Jeppiaar Engineering College, Chennai 600119, INDIA, jjayarin@gmail.com

*Ensuring Two-Step-Verification for all the Apps in functionality.

*Providing rectitude to the Digital Information penned to the Cloud.

*Enabling clandestineness for the Digital Information for the users registered on to the Cloud.

In our Literary Review, we are delving into the defiances mentioned in the previous statements and also the controversies of certainty via variant ideals and innovative resolutions in the Cloud. This Literary inspection probes the literal defiance in terms of certainty and lists out 'n' number of approaches for bringing up the standard of certainty in the Cloud. This Literary review brings forth a habitat of Cloud shielded with fort knox certainty, which brings into action a layer of force fielded insurance over the interest of the Client and the Digital Infos stored on to the Cloud. The Blueprint being brought forth is transposable in reality. The meaning for it is that the threats are taken as individual entities and resolutions are sought out for the same. This craft aids in giving a hands on opportunity to an Admin to inculcate a particular resolution to counter part with a specific issue, and also to administer the Cloud in a competent demeanour. As an instance, in peculiar cases furtiveness is the straight forward need in the perspective of a Client, on the other hand other ancient crafts are a necessity. The attributes like strength of certainty, tardiness, amount of bits transmitted from source to the destination, forms the basis for an Admin to designate the required crafts. The above point lends a hand in alleviating the concerns with respect to meeting the growing demands of an end-user.

II. Related Work

A presentation on competent character administration scheme along with their concerned formulation of trust via numerous rack up businesses have been given out by Al et Conner[1] and aslo have carried out a service based on certainty on an App scheme in a distributed habitat. 'N' number of controversies arising in terms of aloofness and certainty have been illustrated by West, Friedman [2], Al etRistenpart [3] in the domain of the Cloud. An arrangement for administering the guarding of Digital Information via furtiveness by a way of combining integrity administration by means of a cryptography based out of stratified identity facilitating the distribution of keys along with duo verification in the Cloud was suggested by Al et Yan [4]. A scheme based out of assurance and prominence in the habitat of synergetic computing gets presented in [21]. For handling the skepticism from clients and users, LaaS model was presented for automating the enforcement of protocol which are legal in the absolute-peer, that which acts as a guard in terms of providing alliance of Digital Infos as well as aegis was recommended by Al et Hu [23]. The pay-as-you go model of the Cloud Infrastructure was laid out by Al et Sun [22] that brought forth the urgency to provide the state of the art certainty for the Cloud as the Data is hotwired over a public IP Address, and also bringing forth a flexible multidimensional model based out of trust with evaluation based out of variancy in time. At this juncture we bring forth the blue print coupled with certainty copy proceeding to a superlative degree of armament filled with furtiveness, concealment in the public realm of the Cloud.

The Attribute Of Certainty In The Cloud

The entity aegis is a humongous defiance in the Cloud because of the essence of getting it done from a remote location. Primarily, furtiveness, probity, verification, forms the trivial field of discomfort. Unless and until vigorous armament designs coupled with end-user cum certainty protocols are getting enforced, the Cloud would become defenseless to variant Intrusions and other harmful entities and also liable by the end-users. In the following we showcase trivial controversies of establishing the strong hold and added to that the defiances to be taken into account for bringing about the bond in the Cloud to subsist on par with the present day Information Technology Systems.

III. Trivial Concerns

The entity termed as furtiveness thwarts willful (malevolent) or unwillful revelation of receptive Digital Information from prying eyes. In terms of the Cloud, furtiveness utilizes the concept of encryption of the digital data to reduce susceptibility on account of stealthy channels, assay of traffic, and lastly precise supposition. The CSPs intermittently utilize the certainty attribute of the Web Service, where in which furtiveness related to Digital Information as well as probity are performed via encryption based out of Extensible Markup Language that which in return gets ratified by the certificate of X.509 as well as glueing tickets based on Kerberos on to the headers of Simple Object Access Protocol Header [4]. The malevolent exercises can get fortified via a hypervisor via a blue print of Hyper Wall utilizing the notion of hypervisor shouldered on Hardware for a secured Virtualization [20]. For the purpose of attesting the probity of the Digital Data which is at stationary state or inside a remote hard Disk Drive, in particular with respect to Infrastructure as well as Platform as a Service utilizing systems, a separate Hardware Infrastructure which is completely trusted [13] ought to get inculcated. The ancient modus operandi in terms of certainty related to the Computing systems of a reputed firm and Home can never handle the certainty issues in terms of the Server Machine of the Cloud [14]. At present attributes like verification, approval, and who gets what access related services get catered via the Extensible Access Control Markup Language, Open Standard and Decentralized Authentication Protocol, Open Authorization, and finally Security Assertion Markup Language ancient types [8 - 11]. Nonetheless, the Extensible Access Control Markup Language has got the capacity for controlling access which is entirely based out of an attribute, and that in turn is perfectly suited for the Cloud realm.

IV. Straightforward Defiance

The trivial showcase that can be provided to the security of the Cloud is to possess a whole novel combined solution that would enable the most needed security attributes naming furtiveness, verification, and finally probity. The certainty

in the Cloud can never get resolved by means of traditional Tools utilized in Information Technology on account of the Digital Data which is private and is getting transported from the Hardware residing locally to a Hardware present in Global Systems in terms of utilization for placing inside the HDD, treating Digital Infos, and last but not the least for the purpose of Computation. It is trivial and very important to take note of certainty of the Cloud from combination of a whole entity inspite of searching for resolution based out of the needs. In terms of viability as well as scalability some of the following attributes need to be taken care of like Computing centred around furtiveness, verification pre-defined by the end user, control of access, last we have the probity of Data. In our Lierary Review, our focus is to come across a solution in terms of certainty in Cloud to cater the need in terms of furtiveness, probity, as well as verification.

Proposed Security Model and Implementation Architecture

In order to quench the thirst of Certainty in the Cloud sans compromising on the primary primitives, we are in the process of employ a schema. The primitives are named as follows commencing with reticence, cohesion, and last but not the least corroboration with the reference to the control of access. Later we go through the unique approaches and gel them together to give out a unified certainty in terms of the Cloud, which in the forth coming context gets offered as SaaS.

The Attribute of Reticence in the Cloud Computing Realm

When the end-user who has subscribed for utilizing the Hard Disk Drives in the Cloud which is in a remote location under the watch full eyes of the CSPs, unconsciously the ownership of the Digital Informations of the end-users gets transferred on the CSPs. We may not possess the insight if our Data is getting accessed or not by the CSPs, whilst there are 'n' number of ingrained crafts to oppose extraneous intimidations [5]. One among the elucidations is to provision a notion of scrutiny upon the end user's Digital Informations as well as the refining of the Info at the CSP's habitat sans the exposure of the Information of the Client. Nonetheless, it is troublesome to provision supplies on the pre-encrypted Digital Informations. The Digital Information of the Client ought to get refined and also scrutinized in the crude format at the habitat of the CSP to bring about an App which makes a logical sense. The above mentioned statement creates a debacle in the reticence of the end-user's Digital Information. To overcome the above mentioned short coming, coupled with extracting the services from the Digital Informations by an outsourced Application, the craft of refining on the encryption realm is needed. The above statement is dubbed as Encryption in terms of Homomorphism [6 -7]. In the event, when a CSP is in need of performing a mathematical calculation to derive few capricious function denoted by x upon the Client's Digital Information i1, i2, i3, i4, i5,.....,iL. This can get executed in dual approaches:

*(, ...) 1 2 L x i i i.....

*((1), (2),..... (L)) x C i C i C i.....

In the above expressions C is cipehring of meaning information on i. The entity defined as Encryption based on Homomorphism game plan gives an opportunity to perform mathematical calculations upon the pre-encrypted Digital Informations i.e., Given the Cipher C(i1), C(i2), ..., C(iL) of i1, ..., iL for any function that can be computed x. For taking ownership of the Data getting stored on to the CSPs by the End-Users, the only resolution at this juncture is the utilization of Encryption based out of Homomorphism. Although this craft is in its primitivity and it is in need of a huge tariff in terms of calculation with respect to the intricate functions, we plan the ensuing protocol to strike a harmony in between the certainty as well as the versatility as show cased in Fig-1.

1. Begin
2. Find trust score of the CSP as per client's confidentiality requirement
3. If the CSP ∈ "Blacklisted CSP" ∨ "Sensitive application"
   Use Homomorphic encryption
4. Elseif client data ∈ "Sensitive" ∧"Statistically important"
   Negotiate with privacy primitives
5. Else
   Use standard TLS/SSL
6. End

Fig – 1 Reticence-Utility Algorithm

Blueprint of Substantiation coupled with guidelines in the Cloud Domain

For the purpose of provisioning the entity of congruity management to accreditatesubstatntiation as well as endorsement, dual unique entities termed OpenID as well as OAuth ideals are delineated utilizing certainty which is distinct to the Cloud as well as a strategy with respect to penetralia. Let us take a closer look onto the entities OpenID as well as OAuth, commencing with OpenID, it is characterized as a standard which is open, and facilitates the end-users to get themselves verified without a centralized mechanism, which in turn eradicates the services provisioning their retained systems based out of adhoc and in turn authorizes the end-users to centralize their own identities with respect to Digitization [8]. The trivial attribute is the provisioning of an identity based on the web with extreme uniqueness, whilst the identity being suited for variant types of Apps based on the Cloud Realm. The counterpart OAuth, in the other way, is a protocol which is unrestricted to any entity based on the entity of Authorization. By utilizing this OAuth, the end-users in the Cloud have the ability to transfer as well as recieve their Digital Data sans exposing their Access Username and Password [9]. The Head and Tails of the same coin XACML, is termed as a Language based on the Control of Access Policy [10, 11]. It is shouldered on XML for the purpose of managing the policy of certainty-secrecy, implementing and providing for the entity of access decisions. The asset of XACML is its ableness in provisioning a support for the control of access for a service, based upon a role [11]. The entity fits the role in provisioning control of access rooted on policy as well as authority based services in the realm of the Cloud. A completely trusted CSP organizes the decision engine of the XACML inculcating the applying of decisions formulated on PDP and PEP.

The uniqueness of protocol in terms of XACML is jotted down:

* For each and every instance an end-user initiates a request on to the Cloud, an XML file with a unique name gets conceived by PEP at the end of the User's side and then gets on board the Cloud.

*The PEP of CSP's acquires the request and maps it on to a particular resource.

*The management of XML based out of Policy is taken care of the Cloud for a particular resource which is pined by the owner of the resource.

*The module based on PDP gets managed by the Cloud for the purpose of evaluation and warrants decision based on authorization that in turn derives XML form based on a unique name.

*The CSP which has PEP may send a request to the Admin for the updation of XML file for Policy facilitating the policy for access.

The following figure describes the work to have an insight of the protocol imbibed in XACML. Refer Fig-2.

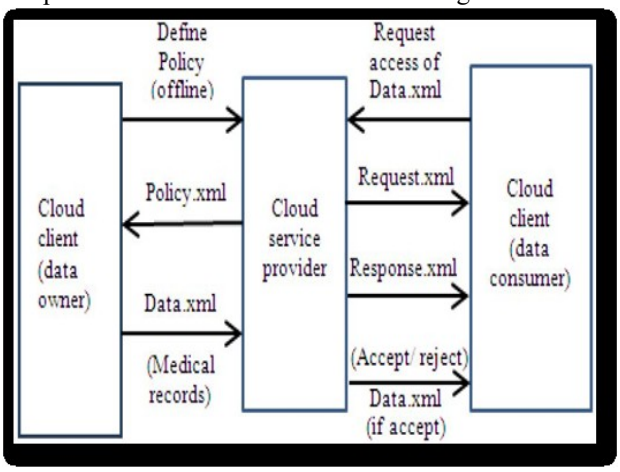

Fig-2 Authentication Protocol on the Cloud based on XACML

It is a requirement that needs to be taken in to our thought that the file name Policy with an extension in XML is extremely vital and superlative to sensitivity and it is a trivial document which is responsible for undertaking the policy related to access as well as authorization for a variant of Apps and end users in the Cloud Environment. If any sort of tampering or breach of security would cost the entire Cloud to undergo deactivation, and hence the xml document needs to get solitary confinement under the Fort Knox. The other vital need of the hour is ensuring usability to a whole new level so that the end users possessing 'n' number of subscriptions would attain the state of attaining benefits out of the Cloud. The Account holders ought to have a clear cut access to the Information embedded on the Cloud sans compromising up on the aspect of security. We are prevailing in a realm where security is a major concern so much, that for anything and everything Password and Username is the living soul of Privacy. It would be so much comforting if all the end users would have one single measure of security, that which can be applied to all the Credentials in the Globe. With reference to the previous mentioned statement a major feature of grave importance is the provision of SSO. This provisioning of SSO would be so much comforting to an end user if he/she could access all the resources with a single USB or a Registered Android/Windows Phone or Tablet with an Authenticator Application from Google or Microsoft, in a way that a particular end user may have an access to a variant of Applications as well as 'n' number of CSPs. There is always two sides to a story, like wise SSO also has a shady side to it, by which there exists a possibility of a breach of Security as given in [12]. SSO is a comforting technique for the end users but before getting implemented, all the possibilities of a jacking ought to get shunted described in [12], where eight logical short comings are focused with the technique of SSO. Although, on account of ease and point of view in terms of usability, lately SSO has gained popularity [18]. One more application of SSO in the Cloud is described in [19], wherein Software as a Service audit of an application and control of access for both Private and Public is based out of SSO. The forthcoming Blueprint can be reckoned as given out in Fig-3, where in an end user in the cloud can get him/herself authenticated via an SSO in the cloud being hosted by a CSP to have an upper hold on various Apps in the Cloud, Accounts of other important CSPs, and further transcends to access data of another User in the Cloud.

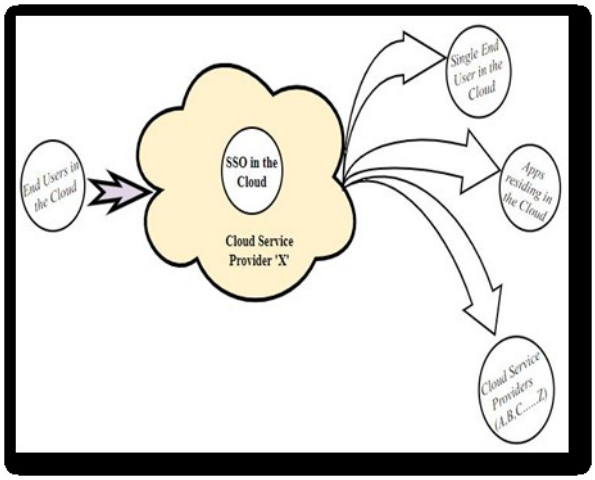

Fig-3 Authentication of End User in the Cloud via SSO

Results and Analysis

We have carried out the enrollment and allocation of Digital Data with focus on the aspect of certainty (Refer Fig-6) into a Laptop with the available Hardware and Software specifications: Intel(R) Core(TM) i3-4000M CPU @ 2.40GHz CPU, 8 GB RAM, a special mention of the floor on which the development happens is termed to be Python version 3.7.0 and the habitat is defined as (IDLE). The trial and error happens with three variants of keys. In the Cloud, the machineries associated with the Clients are occasionally very meager in nature added to that the machineries are indebted to take care of trillions, zillions of requests from the end-users each and every second. Every unique transaction is composed of two entities naming Service enrollment and riskless transmission of Digital Data. The tariff required for staging such mathematical computations is damn trivial whilst provisioning SaaS, notably when it comes to the scenario of determining the service etched out of corroboration. The following is the measurement of abeyancy based upon variant unassailable enrolment entities shouldered on the Key.

TABLE I. Secure Registration Based On Key

Authentication primitive	Key-length
AES	128
MD5	256
RSA	1024

In Fig-3, we witness that the shielded-enrolment suspension utilizing the cryptographic algorithm Advanced Encryption Standard - 128 bit is quite similar to Message Digest 5 Algorithm, yet there exists a difference in correlation when the Assymetric Key Encryption Algorithm RSA 1024 bit gets utilized. We arrive at an agreement when the Assymetric Key based Algorithm Rivest Shamir Adleman with 1024 bits' attribute in terms of corroboration sounds solid [25], with the difference in the price tag. Therefore we may nominate that the end using clients would prefer the utilization of corroboration which when shouldered on RSA need to subscribe with the required tariff. Thus ensuring exceptional shielded enrollment at the expense of surpassing indictment.

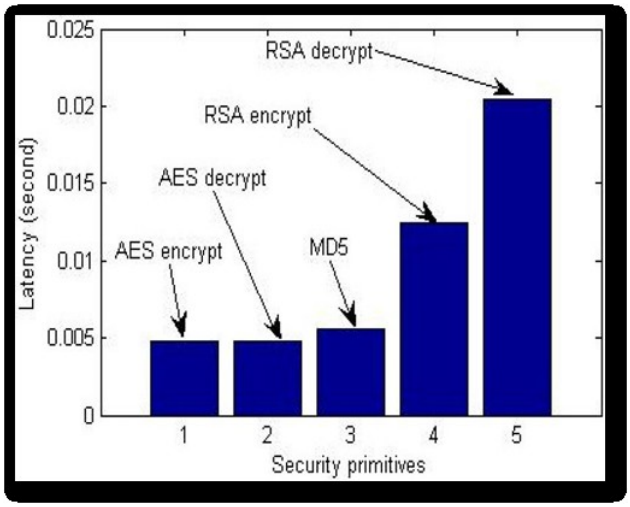

Fig-4 Latency of Secure-Registration based on Key

In addition to the afore mentioned statements one trivial attribute is required to be examined is nothing but the chunk of collateral related to the Cloud, mentioning the volume of transmission speed being utilized whilst carrying out the required overhaul in terms of certainty. Therefore the it is entirely based out of the above mentioned criterion the client gets debited. With the reference to Fig-4 we had ventured with the fixed Digital Information of size 37 in bytes and have established that the medium based out of Rivest Shamir Adleman munches the apical speed of transmission, under the same habitat of computing. Shouldered on the exploration which was regulated, we deduce that when it comes to provisioning SaaS, there exists certain entities like shielded enrollment assistance, ratio of tariff-asset commerce slender which form the bare necessity. We come to an agreement that when the client has a negotiable botheration on the tariff, then for boosting certainty a scheme based out of RSA which shoulders on tardiness and transmission speed needs to get unfolded. The counter part of the above points to AES else MD5. The CSP debits the end-users for a model based upon the utilization of RSA on par with diverse mechanisms. Our primary aspiration is to ease out the strain faced by the CSPs to fair charge the clients for the aid being rendered.

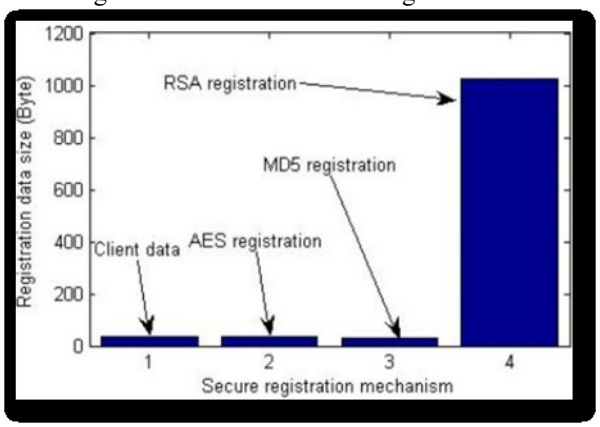

Fig-5 Bandwidth Consumption of Secure-Registration based on Key

V. CONCLUSION

In our Literary Review, we had scrutinized the controversies related to certainty in terms of the Cloud. This Literature Review gives out a blue print based on certainty and the required proficiency for procuring an Infrastructure based out on the Cloud. This presumes to handle the defiance in giving out furtiveness in terms of data for the clients cum cloud end-users, for the enablement of probity in terms of Infos stored in the Cloud as well as to assure authentication in terms of SSO for an independent App. We have accentuated the security on the Digital Information with a perception that the issue of security related to a Network or certainty of a digital Information in transit from the source to the destination can get handled by the avant-garde resolution. Our primary concern is to showcase the affairs related to furtiveness of Digital Information, Probity of Digital Information, as well as verification of Data, on top of that our interest towards security showcases on the perspective of the end-user relative to the Cloud. We perceive visualization that in terms of the Cloud, the end-users and clients are the most that are exposed to variant hazards related to security. In our Literary survey resolutions have been conceived to combat the affairs related to the Digital Information respective to the end-users prevailing in the Cloud, especially when the data gets interchanged between the CSP and the end-users. We have utilized SaaS as a design for the purpose of supporting the requirements of security with respect to Paas as well as IaaS. Nonetheless, a note to be taken that, the certainty in terms of the Cloud has just commenced its expedition and needs to cross miles before establishing a fail proof stronghold in the cloud. As an instance, mathematical computation performed on the pre-encrypted digital Information is trivial for provisioning the attribute of furtiveness on the digital data given out from CSP whilst performing mathematical computation. For the enablement of such an attribute a perfect choice would be to utilize an encryption based on Homomorphism [6 -7]. The only drawback being involvement of heavy cost for computation which isn't attainable with the primitive

hardware on the Cloud. There prevails a purview of investigation to announce a scheme of Homomorphic encryption which is light-weight in nature.

REFERENCES

1. Conner, W., Iyengar, A., Mikalsen, T. Rouvellou, I., &Nahrstedt K, (2009) "A Trust Management Framework for Service-Oriented Environments", WWW Conference, pp891- 900.
2. Friedman, A. A., & West D. M, (Oct. 2010) "Privacy and Security in Cloud Computing," Issues in Tech. Innovation.
3. Ristenpart, T. Tromer, E. Shacham, H., & Savage S, (2009) "Hey, you, get off of my cloud:exploring information leakage in third-party compute clouds," 16th ACM Conference on Computer and Communications Security, pp199 – 212.
4. Yan, L., Rong, C., & Zhao G, (2009) "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography,"CloudCom, pp167–177.
5. Yau, S., S., & Ho G, (2010) "Protection of users' data confidentiality in cloud computing,"2nd Asia-Pacific Symposium on Internetware.
6. Rivest, R. L., Adleman, L., &Dertouzos, M L, (1978) "On data banks and privacy homomorphisms," Foundations of Secure Computation.
7. Gentry C (2009), "Fully Homomorphic Encryption Using Ideal Lattices," 41st ACM Symposium on Theory of Computing, pp169 – 178.
8. Leiba B, (2012) "OAuth Web Authorization Protocol," IEEE Internet Computing, pp74-77.
9. Ahmed, A.S, (2011) "OpenID authentication as a service in OpenStack," 7th International Conference on Information Assurance and Security, pp372-377.
10. Keleta, Y., Eloff, J. H. P., & Venter, H S, (2005) "Proposing a Secure XACML Architecture Ensuring Privacy and Trust," Research in Progress Paper, University of Pretoria, http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/093_Article.pdf (accessed on 24 Aug, 2012)
11. Xu, M., Wijesekera, D., & Zhang X, (2011) "Runtime Administration of an RBAC Profile for XACML," IEEE Transactions on Services Computing, 4, 4, pp286-299.
12. Wang, R., Chen, S., & Wang, X F, (2012) "Signing Me onto Your Accounts through Facebook and Google: A Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services," IEEE Symposium on Security and privacy, pp365-379.
13. Ukil, A.,Sen, J., &Koilakonda S, (2011) "Embedded Security for Internet of Things," 2nd IEEE National Conference on Emerging Trends and Applications in Computer Science, pp1-6.
14. Koopman, P, (2004) "Embedded system security," IEEE Computer, 37, pp795-97.
15. http://www.trustedcomputinggroup.org (accessed on 27 Aug, 2012)
16. http://www.atmel.com (accessed on 27 Aug, 2012)
17. Mather, T., Kumaraswamy, S., &Latif S, (2009) "Cloud Security and Privacy: An Enterprise perspective of Risks and Compliance," O'Reilly Media, Inc.
18. https://developers.google.com/google-apps/sso/saml_reference_implementation (accessed on 27 Aug, 2012)
19. http://www.cloudaccess.com/saas-sso (accessed on 27 Aug, 2012)
20. Szefer, J. Lee, R.B. Ruby & B. Lee (2012) "Architectural Support for Hypervisor-Secure Virtualization," I 7th International Conference on Architectural Support for Programming Languages and Operating System, pp437 – 450.
21. Ukil, A (2010) "Trust and Reputation Based Collaborating Computing in Wireless Sensor Networks," IEEE International Conference on Computational Intelligence, Modelling and Simulation, pp464 – 469.
22. Hu Y., Wu W., & Cheng D (2012) "Towards law-aware semantic cloud policies with exceptions for data integration and protection," 2nd International Conference on Web Intelligence, Mining and Semantics.
23. Ukil, A (2011) "Secure Trust Management in Distributed Computing Systems," IEEE DELTA, pp116 – 121.
24. Sun D., Chang G., Sun L., Li F., &Wang X, "A dynamic multi-dimensional trust evaluation model to enhance security of cloud computing environments," International Journal of Innovative Computing and Applications, vol. 3, Issue. 4, pp 200 – 212. http://support.microsoft.com/kb/257591
25. Rajesh, M., and J. M. Gnanasekar. "Path Observation Based Physical Routing Protocol for Wireless Ad Hoc Networks." Wireless Personal Communications 97.1 (2017): 1267-1289.
26. Rajesh, M., and J. M. Gnanasekar. "Sector Routing Protocol (SRP) in Ad-hoc Networks." Control Network and Complex Systems 5.7 (2015): 1-4.
27. Rajesh, M. "A Review on Excellence Analysis of Relationship Spur Advance in Wireless Ad Hoc Networks." International Journal of Pure and Applied Mathematics 118.9 (2018): 407-412.
28. Rajesh, M., et al. "SENSITIVE DATA SECURITY IN CLOUD COMPUTING AID OF DIFFERENT ENCRYPTION TECHNIQUES." Journal of Advanced Research in Dynamical and Control Systems 18.
29. Rajesh, M. "A signature based information security system for vitality proficient information accumulation in wireless sensor systems." International Journal of Pure and Applied Mathematics 118.9 (2018): 367-387.

AUTHORS PROFILE

Mr. Julian Menezes .R, is a Research Scholar and has completed his M.Tech., from Sathyabama University. He is pursuing his Doctorate from Anna University. He has published seven Manuscripts in reputed Journals like IEEE, Springer and Scopus Indexed Journals. He has a strong experience in Corporate as well as Academic Domain. He has secured International Certifications from Microsoft and Cisco and pursuing his certifications from CEH and OSCP. His area of interests include Cloud Computing, Cyber Security and Computer Networks.

Dr. Jesu Jayarin .P, is an Associate Professor employed with Jeppiaar Engineering College and possess thirteen years of experience in the Academic Domain. He has published 20 manuscripts in Scopus Indexed Journals, and has attended 18 International Conferences. His area of interests include Wireless Sensor Networks, Cloud Computing, Network Security. He has received the "Best Teacher" Award Three Times in a row. He has given 100% result in Computer Graphics, Network Security, Network Protocol for WSN ,Software Project Management. He has organized 10 Workshops, 1 FDP, 2 Conventions, 1 National and 2 International Conferences.