CLASSIFICATION OF ATTACKS IN CLOUD COMPUTING MODEL BASED ON CURRENT SCENARIOS

Swetha Pesaru[1]
[1]Department of IT, JNTUH University, Hyderabad, Telangana, India

ABSTRACT

Distributed computing is a developing figuring worldview that offers incredible potential to enhance profitability and operational productivity. This as of late created innovation bolsters asset sharing and multi-tenure which thus contributes towards diminished capital and operational use. While cost and convenience are the primary advantages of cloud registering, trust and security are the two top worries of clients of cloud administrations. The suppliers of this quickly developing Innovation need to deliver numerous issues identified with virtualization disseminated processing, application security, character administration, access control and confirmation. Notwithstanding, solid client confirmation that confines unlawful access to the administration giving servers is the principal necessity for securing cloud environment. In such manner, the paper concentrates on recognizing the different confirmation assaults in cloud environment. An endeavor has been made to comprehend the underlying driver of the confirmation assaults and propose conceivable moderation measures in a cloud situation..

Keywords - *Cloud Computing, Security Issues, Authentication Attacks, Attacks in Cloud, Cloud Solutions*

I. INTRODUCTION

Distributed computing is another era innovation that offers on-interest, system access to a mutual pool of configurable processing assets on a compensation for each utilization premise. This new figuring worldview varies from other comparable processing advancements in that, the distributed computing administrations take after a self-administration model. Distributed computing offers programming, stage furthermore, framework over the Internet and this constitutes the three kinds of cloud viz., Software-as-a-Service (SaaS),

Stage as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). This figuring model empowers the cloud clients to build their ability and capacity powerfully without putting resources into new foundation, preparing new faculty, authorizing new programming and so forth [1]. Distributed computing innovation empowers clients to remotely get to shared assets put away in cloud servers utilizing web administrations by means of the Internet. Thus the cloud inhabitant assets are reasonable to the security dangers appropriate to Internet and web administrations. The way that the assets ought to be available just to real users indicates out the necessity of inferring a protected, client validation instrument for the cloud environment. Verification includes the way toward guaranteeing that a man who exhibits an arrangement of certifications is whom he or she claims to be. The cloud administration suppliers need to handle the issues confronted by client verification components completed preceding giving access to the mutual assets. The building elements of cloud, for example, Multi-tenure and Virtualization permit the clients to accomplish better working costs and be exceptionally spry by encouraging quick obtaining of administrations and assets on a need premise. In any case, to accomplish the full advantages of cloud, the administration suppliers need to handle the security concerns raised by the quickly developing cloud purchasers. Among the different security concerns, information security, trust and protection are the significant ones that make potential clients think various times before receiving cloud administrations. In a review led by International Data Corporation (IDC), to comprehend difficulties of Cloud registering, 87.5 % of the masses having a place with changed levels beginning from IT officials to Chiefs have said that security is the top most test to be managed in each cloud administration [2]. Amongst the different dangers confronted by the diverse cloud administrations, security risk is thought to be of high hazard [3] and consequently the cloud administration

Suppliers need to consider security as a major issue to be tended to instantly for the entire hearted reception of cloud administrations. These dangers can be impeded in an application by the presentation of some appropriate components taking into account the objectives of data security worldview. The objectives incorporate Confidentiality, Data-Integrity, Authenticity, Authorization, Non- Denial, Availability, Audit and Control [4, 5, 6]. The way that cloud administration suppliers have admittance to the customer's information put away in the cloud prompts security issues. There is an absence of straightforwardness in cloud that permits clients to screen their own Privacy data, however SLA‟s ensure security of delicate information. Subscribing to different cloud administrations implies various duplicates of client qualifications, which is yet another security issue. For each cloud administration got to by the client, he needs to trade his validation data and this repetition may prompt an abuse of the verification instrument. Additionally distinctive cloud administration suppliers use diverse verification instruments which can be a security challenge for the clients. Henceforth, a dolt evidence client confirmation component is a vital necessity of the cloud environment to avert illicit access to cloud given assets.

II. ORGANIZATION OF THE PAPER

Whatever remains of the paper is composed as takes after: Section 3 talks about a couple works done by analysts in the zone of cloud Security and verification. Area 4 looks at the different classifications of confirmation assaults on cloud. A hefty portion of these assaults are relevant to web administrations and since cloud benefits regularly utilizes web administrations as an apparatus for conveying its administrations, these dangers are appropriate to cloud too. The displayed work depicts the different confirmation assaults from the viewpoint of cloud and talks about conceivable countermeasures. Segment 5 is held for a brief discourse of the work done by the specialists and for finishing up the work.

III. RELATED WORK

As of late, numerous analysts have proposed diverse ways to deal with examining security issues of cloud registering. Meiko Jensen et al. [7] consider the specialized security issues emerging from the utilization of cloud administrations and the

Fundamental advancements used to fabricate this cross-space between associated joint efforts. This work focuses more on web administrations related security issues and focuses less on verification element. Hassan Takabi et al., [8] have distinguished distributed computing as a relentless power in view of its potential advantages. The creators highlight the need proper instruments to handle the security and protection dangers in cloud. The work talks about the security challenges counting client confirmation, access control, approach coordination, trust administration and administration and proposes a far reaching security structure for distributed computing. Hsin-Yi Tsai et al [9] in their work investigates the security issues in diverse administration conveyance models from the point of view of Virtualization. S.Subashini and V.Kavitha [1] reviewed the security dangers confronted by the cloud administration conveyance models and proposes a security structure that gives information security by putting away and getting to information in view of meta-information data. B. Sumitra furthermore, M. Misbahuddin [10] has overviewed and ordered the security dangers appropriate to cloud environment. The work is a general characterization of assaults and does not dive profound into verification issues. Rohit Bhadauria et al. [11] explored the security dangers, for example, SQL infusion imperfections, cross-site scripting, uncertain capacity and so forth as appropriate to cloud environment. Yet, the attention is on the different layers of the system, for example, Network level and Application level. R.C.William et al. [12] examines the insider dangers in distributed computing. The creators consider the insiders from three alternate points of view and the conceivable effect of every insider on cloud Security. In any case, this work focuses just on a particular classification of validation assault on cloud. In spite of the fact that there is a lot of progressing examination for recognizing the security escape clauses in cloud there is a need to consider the particular difficulties confronted by different compositional segments of cloud. Likewise the advances utilized by cloud for conveying its administrations raise different security issues, which should be distinguished and tended to. The validation system utilized by cloud administration suppliers contributes a considerable measure towards the upgrade of security elements since cloud has a colossal number of shared and delicate assets. Drafting a verification structure, which can address the security concerns identified with validation, requires a reasonable comprehension of all conceivable verification assaults on cloud. Thus distinguishing the different classifications and subcategories of verification assaults, assault situations and conceivable alleviation procedures turns into the inspiration for this work.

IV. AUTHENTICATION ATTACKS IN CLOUD

Research concentrates on uncover that any verification instrument identified with web applications and cloud ought to give high security, simple to utilize interface and bolster client versatility. The clients want to get to their applications from various areas and diverse gadgets, for example, desktop, tablet, PDA, advanced mobile phones, PDAs and so forth. Those requirements posture critical prerequisites to the security of uses. The expansive scope of client prerequisites presents extensive variety of assault vectors in the cloud that makes the security of cloud applications a provocative matter. Cloud administration suppliers need to guarantee that exclusive true blue client are getting to their administrations and this focuses out to the necessity of a solid client verification system. However, there exists various assaults that can make escape clauses in the validation system what's more, subsequently recognizing the most secure verification system with high client agreeableness is a major test in the cloud environment. In this way a top to bottom thought of assaults on legitimacy and comparing aversion methods are required to draft an idiot evidence confirmation component for cloud environment.

4.1 Eavesdropping: Eavesdropping includes the demonstration of listening to the correspondence channel set up between two approved clients. In a cloud domain, an activity meddler inactively catches the information exchanged inside a cloud by stacking a touch of code on a cloud server [13] or listens to information moving from a cloud customer to supplier and makes an unapproved duplicate of the message [14].The assailant can utilize the wrongfully accumulated data to get substantial accreditations of an approved client which can be client to dispatch imitating assault. Listening stealthily assault, in a cloud domain which results in data divulgence can be minimized by implementing legitimate approval methods and by transmitting the information over a safe association, for example, HTTPS. Encoding the transmitted information and appending a mark to the same can help the destination to guarantee the uprightness and legitimacy of information. Embracing security improving conventions which minimize the prerequisite of transmitting character qualifications from the cloud administration client to the verifier will dishearten the unlawful action of meddlers. Validation Protocols that ensure privileged insights, guarantees client obscurity and Password Authenticated Key trade (PAKE) conventions are quite favored in a multi-occupant cloud environment.

4.2 Man-in-the-Middle Attack (MITM): Since the origin of Web 2.0, MITM has turned out to be very famous in the SaaS environment. Here the assailant blocks the correspondence channel built up between nests to goodness clients and alters the correspondence amongst customer and server without their insight [15].The taking after passages talk about the different sorts of MITM assaults.

i) Wrapping Attack: A XML Signature wrapping assault material to web administrations is relevant to cloud also, since cloud purchasers use web administrations as a device to get to cloud administrations. This assault is dispatched by copying the qualifications in the login stage by altering the Simple Object Access Protocol (SOAP) messages traded between the program and the server amid correspondence set up [16]. The assailant changes the marked solicitation of a true blue customer by moving the unique message body to a recently embedded wrapping component inside the SOAP header. Another body containing the unapproved operation the assailant needs to perform with the first sender's approval is embedded in the position of unique message. The administration executes the changed solicitation since it contains the mark of a genuine client. Subsequently, the enemy can barge in the cloud and can run a malignant code to intrude on the typical working of the cloud servers. Fig 2 shows a use of wrapping assault. Here, the approved customer asks for a photo called "me.jpg". The assailant catches and changes the SOAP message by embeddings the same components in the solicitation of the approved customer; however the name of the photo is changed to "cv.doc" rather than "me.jpg" as appeared in fig 3. The server on seeing the mark of the approved customer forms the solicitation and sends back the "cv.doc" back to the customer.

The conceivable countermeasure would utilize a mix of WS-Security with XML Signature to sign specific component also, utilizing advanced endorsements, for example, X.509 issued by trusted authentication power (CA‟s). Kazi et al. [17] recommend expanding the security amid the message going from the web server to a web program by connecting an excess piece (STAMP bit) with the SOAP header which will be flipped when message is captured.

ii) Flooding Attack: In a cloud domain, all the calculation servers work in an administration particular way, with inward correspondence among themselves [16]. An effectively approve foe can without much of a stretch send counterfeit solicitation to the cloud. The cloud server before giving the asked for administration, checks for the credibility of the asked for occupations and the procedure expends CPU usage, memory and so forth. Preparing of these false demands, make genuine administration solicitations to starve, and accordingly the server will offload its business to another server, which will likewise in the long run touch base at the same circumstance. The enemy is along these lines effective in drawing in the entire cloud framework, by assaulting one server and proliferating the assault further by flooding the whole framework. Flooding assault can be taken care of by sorting out every one of the servers giving a particular cloud administration as an armada and these servers conveying among themselves with respect to the approaching solicitations by message passing [17]. Again a hypervisor can be used to plan the solicitations among the armadas, decide the validness of the solicitations and keep the armadas from being over-burden with false demands from a foe. This assault can be controlled by information exchange throttling, fool verification confirmation components and systems that channel out false demands.

iii) Browser Attack: This assault which results in information taking is conferred by undermining the mark and encryption amid the interpretation of SOAP messages in the middle of the web program and web server, bringing on the program to consider the enemy as an authentic client and process all solicitations, speaking with web server [16]. For validating the customers, current web programs depend upon SSL/TLS as they are not ready to apply WS-Security. By the by, SSL/TLS just backings Point-to-point interchanges and this makes the validation procedure uncertain. Likewise SSL/TLS has been broken by MarlinSpike [7] utilizing "Invalid Prefix Attack" and assailants can play out this procedure keeping in mind the end goal to demand administrations from cloud frameworks without a substantial validation [18]. The potential counter measure for this is the merchants that make web programs apply WS-Security idea, which works at message level, inside their web programs. WS-Security grants web programs to utilize XML encryption to give end-to-end encryption in SOAP messages which averts sniffing of messages.

iv) Impersonating Attack: Here the enemy professes to be a substantial server or client and draws a legitimate element to uncover the confirming accreditations which thusly is utilized to increase unapproved access to the assets. Verifier Impersonation assault, Phishing assault and so forth can be sorted as mimic assaults. The greater part of the times, in Phishing assaults the clients are made to trust that they are speaking with substantial server by making a page that seem to be like the legitimate server page. In verifier mimic assault, the assailant puts on a show to be the verifier and draw the client to share the confirmation keys or information, which may then be utilized to confirm erroneously to the verifier. . In November 2007, a representative of SaaS merchant, SalesForce was exploited by a phishing assault which brought about the presentation of the SalesForce account data of a few clients [19]. In a cloud domain this can be relieved by utilizing two-element and multi element confirmation components that depend on actually identifiable data (PII) notwithstanding passwords. Additionally security improving conventions that ensure privileged insights and dodge stockpiling of mysteries can hold mimic assaults under control.

v) SSL Attacks: Secure Socket Layer (SSL) is a major security instrument that encodes the data transmitted amongst customer and server. SSL gives a confirmed domain to running a cloud administration by checking the character of the correspondence parties [20].

a) Stripping Attack: There are no measures for the issuance of routine SSL endorsements and subsequently customer applications called depending parties can't have certainty that the association recorded as the proprietor of the endorsement is in reality the proprietor This shortcoming of SSL is abused in the stripping assault [21] which is propelled by installing an invalid character („\0‟) in a area name containing the name of a legitimate confirming power. At the point when SSL customer programming peruses the space name of the fake authentication, it will stop at the invalid quality which is dealt with as a string eliminator. Since the invalid quality shows up instantly after the name of a legitimate guaranteeing power, SSL customer regards the declaration as a substantial one.SSL Strip assault could be utilized against Server-Server interchanges with the potential for mass bargain of secret information. This ridiculing issue is settled by legitimate utilization of Extended Validation (EV) SSL declarations for verification as they contain just confirmed association data.

b) SSL Sniffing: SSL is based on uneven key cryptography, including the utilization of a private and open key. The general population key is dispatched to the customer by the server as endorsement marked by the confirming Authority (CA). The middle of the road CA authentications does not ensure the authenticity of the site and are not installed in the program. This restriction of SSL testament can be abused by the aggressors to dispatch a SSL Sniffing assault. The potential counter measure for SSL assaults is for merchants to make web programs that apply WS-Security idea. Rather than the point-to-point encryption gave by SSL/TLS, WS-Security gives end-to-end encryption and does not must be decoded at mediator has. Subsequently, aggressors can't sniff and increase plain content of SOAP messages at the middle person has.

4.3 Cookie Poisoning: In treat harming, the character related accreditations put away in the treats of an approved client are changed by the assailant to increase unapproved access to assets. Treat harming assaults in cloud can be relieved to a certain degree by utilizing Intrusion counteractive action items that inspects every HTTP ask for sent to the web server [22]. This assault which includes messing around with information can be taken care of by joining the hash estimations of the information put away in the treats and recalculating the same at the destination. Utilization of Message verification codes, alter safe conventions and Digital marks can likewise help in the identification and anticipation of altering the treats.

4.4 Replay Attack: In a catch replay assault the verification message contains the same confirmation tokens already traded between an approved client and sender and was sniffed by the aggressor [23]. The way to handle replay assault, which includes personality ridiculing, is to guarantee that something in the message changes every time. Considering this angle, numerous conventions use time stamps or haphazardly created nonce qualities to oppose replay assault, which empowers the verifier to check the freshness or the realness of the message. The utilization of time stamps requests synchronization of timing at both the cloud administration client and verifier end, which may not be doable in a dispersed cloud environment. Thus haphazardly produced nonce qualities are best in a Cloud domain and since these qualities are exceptional for each session the beneficiary will have the capacity to distinguish a replay of the already send message containing an old nonce esteem.

4.5 Session Hijacking: Session seizing is conceivable, if the Session ID issued to the validated clients is not ensured appropriately, which thusly can be utilized for mocking personality. Session side-jacking utilizes bundle sniffing instruments to catch a login arrangement and along these lines access the user's session key Encrypting the correspondence channel can keep this sort of Session seizing assault. These assaults misusing the provisos, for example, shaky correspondence conventions and decoded information can be defeated by Utilizing a safe correspondence convention, for example, HTTPS, by scrambling the records that store client or regulatory login accreditations and so on. A solid verification system that guidelines out the likelihood of unapproved confirmation and systems that secure insider facts, for example, session keys or stay away from the capacity of privileged insights is required in a cloud situation to counteract such assaults. The side-jacking assault can be moderated by keeping away from the exchange of session keys over the correspondence channel. A key trade instrument, that includes the count of session key independently by the customer what's more, server, bringing about the same key quality, can likewise be received.

4.6 Shoulder Surfing Attack: The assailant picks up information of the mystery accreditations such of the casualty by secretly watching his entrance of delicate information by means of the console. In broad daylight puts, this assault is propelled by utilizing spy cameras. Indeed, even a incompletely fruitful shoulder surfing assault can be unsafe when utilized with other security danger blends. For occurrence the watchword length data got by shoulder surfing assault can be utilized to dispatch a secret key disclosure assault. This assault results in data divulgence and in a cloud situation it can be moderated by utilizing secure two component verification and out-of band validation instruments.

4.7. Cloud Malware Injection Attack: The assault goes for infusing a malevolent administration usage or virtual machine example, which shows up as one of the substantial administration occurrences running in the cloud. The enemy dispatches the assault by making its own particular malignant administration execution module (SaaS or PaaS) or virtual machine occasion (IaaS) and infuses it into the cloud. In the event that the aggressor is effective, then the cloud framework regards the new occurrence as a legitimate occasion for the specific administration assaulted by the foe. The server from that point begins diverting the legitimate client solicitations to the noxious server usage and the adversary's code is executed. The code can complete distinctive exercises, for example, listening stealthily through unobtrusive information adjustments to full usefulness changes.

One method for handling this assault is to store hash esteem on the first administration instance's picture document and contrasting and that of all new administration occurrence pictures. On the off chance that an alteration is done to a legitimate administration example, then the hash worth will be adjusted which demonstrates the nearness of an assailant. Again if another administration case is made by an assailant and embedded into the cloud, then it ought to have hash esteem like that of a current one. In any case, the likelihood of making an administration example with hash esteem, like the hash of another administration example is practically irrelevant.

4.8 Password Discovery Attacks: Attackers embrace a few components to recover passwords put away or transmitted by a PC framework to dispatch this assault. A couple of techniques embraced relying on the accessibility of data identified with the watchword are examined in the accompanying passages:

i) Guessing Attack: Most regularly individuals utilize simple to recollect passwords which make them powerless against speculating assault. A foe watches some data identified with the secret key, tries to get it and afterward checks it by attempting to login numerous times until he gets the entrance. In disconnected situation, the assailant has a high risk of speculating the right secret key as there is no confinement on the quantity of endeavors he makes. Be that as it may, in internet speculating situation the framework obstructs the client after a specific number of login endeavors.

ii) Brute Force Attack: This assault is propelled by speculating passwords containing every single conceivable blend of letters, numbers and alphanumeric characters until the aggressor get the right secret key. Animal power assault as a rule did utilizing robotized techniques requests a ton of figuring force and time to be fruitful.

iii) Dictionary Attack: Here the assailant tries to figure a secret key from a pre-registered word reference of passwords. To stand up to this kind of an assault, the secret key ought to be arbitrary and ought not to be a lexicon word. Indeed, even passwords in mother tongues are not secure as aggressors have lexicons of the greater part of the provincial dialects [15].

iv) Video Recording Attack: In such sort of assault dispatched in broad daylight puts, the aggressors with the assistance of camera prepared cellular telephones or small scale camera catches the watchword while the casualty enters the same.

v) Stolen Verifier Attack: The aggressor plays out this assault by getting to the secret key table put away at the verifier. At that point he dispatches a disconnected speculating assault by running a script which performs hash on every section of the word reference and looks at the created message digest with the put away process of the verifier, until a match is found. This assault can have an awful impact in a cloud domain facilitating information having a place with numerous clients.

The above examined watchword revelation assaults, concentrates on acquiring the secret word of a legitimate client which thus is utilized to wrongfully imitate the client to a verifier. Such assaults will bring about an effective confirmation, if and just if the validation procedure is exclusively taking into account static passwords. In a cloud situation, this can be relieved by utilizing graphical passwords, one-time passwords, evading the capacity of passwords, utilizing Zero Knowledge Proof (ZKP) systems, conventions actualizing 2-element validation components without secret word tables and so forth.

4.9 Reflection Attack: Reflection assault is performed on shared validation plans wherein the assailant traps the focus into uncovering the key to its own test. This assault typically done by making parallel session is dispatched by an unapproved client to set up a legitimate session with the server. The assailant imitates a substantial client and solicitations a login session to the server. The server, as a major aspect of validating the requester, sends him a test and demands the aggressor to send back his mystery reaction. Since he is not a honest to goodness client, the aggressor won't know this mystery. He makes another session and sends to the server, the mystery got from the server in the primary session. Accordingly, when the server answers with another mystery, the assailant utilizes this as a part of the main session which will be accepted by the server. The assailant in this manner picks up access to the framework assets with the benefits of a legitimate client. In March 2013, the anti spam supplier, Spamhaus was hit by an uncommon kind of reflection assault prompting one of the greatest foreswearing of administration assaults ever seen, creating more than 300 gigabit in traffic[24]. In a cloud situation, monitoring the sessions and the privileged insights utilized for every session and in addition constraining the quantity of set up sessions can minimize reflection assaults. Again guaranteeing that the correspondence messages traded between the client and the cloud server amid the validation procedure is not symmetrical in nature can alleviate reflection and parallel session assaults.

4.10 Customer Fraud Attack: This is a unique kind of assault where in the customer intentionally bargains its verification token. The assault should be possible to take individual focal points or to criticize the association. To keep this write of assault, the verifier must have the capacity to demonstrate that the validation disappointment was the victim's own shortcoming [25]. In a cloud situation this assault can be by utilizing one time passwords or haphazardly produced nonce values in confirmation conventions. These qualities which are one of a kind to every session are safely imparted to the client by the verifier. This mystery needs to be submitted to the verifier by the client to pass the confirmation procedure.

4.11 Denial-of-Service (DOS Attacks): The fundamental goal of DOS assault is to over-burden the objective machine with false administration solicitations to keep it from reacting to true blue solicitations. Not able to handle all the administration demands all alone, it delegates the work burden to other comparable administration occasions which eventually prompts flooding assaults. Cloud framework is more defenseless against DOS assaults, since it bolsters asset pooling. This assault on accessibility can be controlled to a certain degree by information exchange throttling which intentionally directs the measure of information exchanged per unit time among the imparting substances and by restricting the assignment of system transfer speed. A verification convention that does one level of validation at the customer side will decrease the overhead of verification procedure at the server side.

4.12 Insider Attacks: Insider assault is propelled by somebody inside the security border who is intentionally trading off the security. An insider can be a present or previous worker, temporary worker or business accomplice of an association who abused his entitlement to get to the delicate assets of the association that adversely influenced the secrecy, respectability or accessibility of the association or associations data frameworks [26]. In a cloud situation an insider can be a maverick cloud supplier manager, the workers in the casualty association that endeavors cloud shortcomings for unapproved access, and the insider who utilizes cloud assets to complete assaults against the company's nearby IT framework [12]. The Cloud supplier must have self evident security access control approaches and specialized arrangements set up that anticipate benefit heightening by standard clients, empower examining of client activities, and backing the isolation of obligations, and guideline of slightest benefit for special clients with a specific end goal to counteract and recognize malevolent insider action.

V. CONCLUSION

Distributed computing is a quickly developing innovation that offers an extensive variety of advantages to little and medium ventures. Be that as it may security, protection and trust are the significant concerns keeping the mass appropriation of cloud. A cloud situation that gives differed administrations and hosts various assets can be secured just by permitting honest to goodness clients to get to the assets. Thus solid client validation components confining unlawful access are the essential prerequisite for securing cloud. A client validation system intended for cloud ought to be sufficiently solid to shield cloud from different conceivable validation assaults. This work studies the verification assaults on cloud and the relating moderation measures.

REFERENCES

[1] S. Subashini and V.Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal of Network and Computer Applications, vol. 34, no.1, pp. 1 - 11, 2011.

[2] H. Lv and Y. Hu, "Investigation and Research about Cloud registering security ensure approach", in Proc. IEEE Int. Gathering on Intelligence Science and Data Engineering. pp. 214-216, 2011

[3] A. Bakshi and B.Yogesh, "Securing Cloud from DDOS Attacks utilizing Intrusion Detection System as a part of VM," in Proc. IEEE Second Int. Gathering on Correspondence Software and Networks, pp. 260-264, 2010

[4] N.S Chauhan and A.Saxena, "Vitality Analysis of Security for Cloud Application," in Proc. Yearly IEEE India Conference, pp. 1-6, 2011

[5] W.Liu, "Research on Cloud Computing Security Problem and Strategy," in Proc. IEEE second Int. Meeting on Consumer Electronics, Communications what's more, Networks, pp. 1216-1219, 2012

[6] X. Yu and Q. Wen, "A perspective about Cloud information security from information life cycle,(2010)," in Proc. IEEE Intl. Meeting on Computational Intelligence and Programming Engineering, pp. 1-4, 2010

[7] M. Jensen, J.Schwenk, N. Gruscka and L.L Iacono, " On Technical Security Issues in Cloud Computing," in Proc. IEEE International Conference on Distributed computing, pp.109-116, 2009

[8] H. Takabi, J.B.D Joshi, G.Ahn, "Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments, " in Proc. IEEE 34th Annual Computer Software and Application Conference Workshops, pp. 393-398, 2010

[9] T. Hsin-Yi, M.Siebenhaar. A.Miede, H.Yulun, and R.Steinmetz, "Danger as a Service? The Impact of Virtualization on Cloud Security," IT Proficient, vol. 14, Issue:1, pp.32-37, 2011

[10] B. Sumitra and M. Misbahuddin, "A Survey of Traditional and Cloud Specific Security Issues", Security in Computing and Communications, Correspondences in Computation and Information Science, Springer Verlag, Vol.377, pp 110-129, 2013

[11] Rohit Bhadauria and Sugata Sanyal, "Overview on Security Issues in Cloud Computing and Associated Mitigation Techniques," International Journal of Computer Applications, pp. 47-66, 2012

[12] William R ClayComb, Alex Nicoll, "Insider Threats to Cloud Computing: Directions for New Research Challenges",[Online], www.cert.org/document/pdf/CERT_cloud_insiders.pdf

[13] Larry Hardesty, "Ruining the Cleverest assault", May 1, [online] web.mit.edu/newsoffice/2012,thwarting-spying information 0501.html, 2012

[14] Maventek, Cloud Security Consulting [WWW] Available from: www.maventek.com/administrations /Cloud-security-counseling, 2012

[15] M.Misbahuddin, "Secure Image Based Multi-Factor Authentication (SIMFA): A Novel methodology for Web Based Services, Ph.D Thesis, Jawaharlal Nehru Technological University, [Online], http://shodhganga.inflibnet.ac.in/handle/10603/3473, 2010

[16] B.Meena and K.A. Challa, "Distributed computing Security Issues with conceivable arrangements," Int, Journal of Computerr Science and Technology, vol.2, Issue: 1, Jan–March, 2012

[17]Kazi Zunnurhain and Susan V. Vrbsky,,"Security Attacks and Solutions in Clouds, [Online] http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf, 2010

[18] Danish Jamil and Hassan zaki, "Security Measures in Cloud figuring and Counter measures", International Journal of Engineering Science and Technology (IJEST), Vol.3 No.4, 2011

[19] Y.Andree, "Ramifications of Salesforce Phishing Incident", [Online] http://www.ebizq.net/web journals/security_insider/2007/11/implications_of_salesforce_phi.php, 2007