**CLOUD COMPUTING**

**AND SECURITYISSUES IN THE CLOUD**

**Sowmyashree O A and Thrupthi M S and chaitra O RDecember 2021**

ABSTRACTCloud computing has formed the conceptual and infrastructural basis for to-morrow’s computing. The global computing infrastructure is rapidly movingtowards cloud based architecture. While it is important to take advantages ofcould based computing by means of deploying it in diversified sectors, the se-curity aspects in a cloud based computing environment remains at the core ofinterest. Cloud based services and service providers are being evolved whichhas resulted in a new business trend based on cloud technology. With the in-troduction of numerous cloud based services and geographically dispersed cloudservice providers, sensitive information of different entities are normally storedin remote servers and locations with the possibilities of being exposed to un-wanted parties in situations where the cloud servers storing those informationare compromised. If security is not robust and consistent, the flexibility andadvantages that cloud computing has to offer will have little credibility. Thispaper presents a review on the cloud computing concepts as well as securityissues inherent within the context of cloud computing and cloud infrastructure.1 IntroductionRecent developments in the field of could computing have immensely changedthe way of computing as well as the concept of computing resources. In a cloudbased computing infrastructure, the resources are normally in someone else’spremise or network and accessed remotely by the cloud users (Petre, 2012;Ogigau-Neamtiu, 2012; Singh jangwal, 2012). Processing is done remotelyimplying the fact that the data and other elements from a person need to betransmitted to the cloud infrastructure or server for processing; and the outputis returned upon completion of required processing. In some cases, it might berequired or at least possible for a person to store data on remote cloud servers.These gives the following three sensitive states or scenarios that are of particularconcern within the operational context of cloud computing:•The transmission of personal sensitive data to the cloud server,•The transmission of data from the cloud server to clients’ computers and1

•The storage of clients’ personal data in cloud servers which are remote servernot owned by the clients.All the above three states of cloud computing are severely prone to securitybreach that makes the research and investigation within the security aspectsof cloud computing practice an imperative one. There have been a number ofdifferent blends that are being used in cloud computing realm, but the coreconcept remain same – the infrastructure, or roughly speaking, the resourcesremain somewhere else with someone else’s ownership and the users ’rent’ it forthe time they use the infrastructure (Bisong Rahman, 2011; Rashmi, SahooMehfuz, 2013; Qaisar Khawaja, 2012). In some cases, stored sensitive dataat remote cloud servers are also to be counted. Security has been at the coreof safe computing practices. When it is possible for any unwanted party to’sneak’ on any private computers by means of different ways of ’hacking’; theprovision of widening the scope to access someone’s personal data by means ofcloud computing eventually raises further security concerns. Cloud computingcannot eliminate this widened scope due to its nature and approach. As a result,security has always been an issue with cloud computing practices. Robustnessof security and a secured computing infrastructure is not a one-off effort, itis rather ongoing – this makes it essential to analyse and realize the state-of-the-art of the cloud computing security as a mandatory practice. Cloud ismainly categorized as private cloud, community cloud, public cloud and hybridcloud (Ogigau-Neamtiu, 2012; Singh jangwal, 2012; Rashmi et al., 2013; QaisarKhawaja, 2012; Kuyoro, Ibikunle Awodele, 2011; Suresh Prasad, 2012; Youssef,2012) - the discussion in this paper assumes only one category of cloud existswhich is public cloud; as this assumption will well satisfy all the characteristicsof any other type of cloud. Due to its diversified potentiality, the approach tocloud computing is being thought to be as the 5th utility to join the league ofexisting utilities water, electricity, gas and telephony (Buyya, Yeo, Venugopal,Broberg Brandic, 2009) rather than being just another service.The study presented in this paper is organized with a view to discuss andindentify the approach to cloud computing as well as the security issues andconcerns that must be taken into account in the deployment towards a cloudbased computing infrastructure. Discussion on the technological concepts andapproaches to cloud computing including the architectural illustration has beentaken into consideration within the context of discussion in this paper. Securityissues inherent in cloud computing approach have been discussed afterwards.The exploration in the technological and security concerns of cloud computinghas led to the concluding realization on the overall aspects of cloud computing.The approaches to counter security issues inherent in cloud computing are nu-merous with diversified facets and applications which has been kept out of scope.A discussion on the authentication of cloud computing has been addressed asit forms the holistic basis to embed integrity in the context of cloud computingsecurity.2

2 CLOUD COMPUTING INFRASTRUCTUREThe term cloud computing is rather a concept which is a generalized meaningevolved from distributed and grid computing. Cloud computing is described asthe offspring of distributed and grid computing by some authors (Che, Duan,Zhang Fan, 2011).The straightforward meaning of cloud computing refers to thefeatures and scenarios where total computing could be done by using someoneelse’s network where ownership of hardware and soft resources are of externalparties. In general practice, the dispersive nature of the resources that are con-sidered to be the ‘cloud’ to the users are essentially in the form of distributedcomputing; though this is not apparent or by its definition of cloud computing,do not essentially have to be apparent to the users.In recent years, the cloud has evolved in two broad perspectives – to rent theinfrastructure in cloud, or to rent any specific service in the cloud. Where theformer one deals with the hardware and software usage on the cloud, the laterone is confined only with the ’soft’ products or services from the cloud serviceand infrastructure providers. The computing world has been introduced witha number of terminologies like SaaS (Software as a Service), PaaS (Platformas a Service) and IaaS (Infrastructure as a Service) with the evolution of cloudcomputing. As discussed earlier, the term ‘cloud computing’ is rather a con-cept, so are the terminologies to define different blends of cloud computing. Atits core essence, cloud computing is nothing but a specialized form of grid anddistributed computing which varies in terms of infrastructure, services, deploy-ment and geographic dispersion (Hashizume et al. 2013; Westphall et al., 2011;Hamlen, Kantarcioglu, Khan, Thuraisingham, 2010). In a pervasive meaningwithin the context of computer networks, infrastructure could be thought of asthe hardware as well as their alignment where platform is the operating systemwhich acts as the platform for the software (Singh jangwal, 2012; Lee, 2012).Thus the concept of cloud based services is hierarchically built from bottom totop in the order of IaaS, PaaS and SaaS. This is merely the level of abstractionthat defines the extent to which an end-user could ’borrow’ the resources rang-ing from infrastructure to software – the core concern of security and the fashionof computing are not affected by this level of abstraction. As a result, securityis to be considered within any form of cloud computing (Bisong Rahman, 2011)regardless of flavour, hierarchy and level of abstraction. Virtualization is an in-evitable technology that is highly coupled with the concept of cloud computing(Buyya et al., 2009; Ogigau-Neamtiu, 2012; Hashizume et al. 2013; Kim, 2009;Mosher, 2011; Atayero Feyisetan, 2011; Zissis Lekkas, 2012) – it is the vir-tualization technology that complements cloud services specially in the form ofPaaS and SaaS where one physical infrastructure contains services or platformsto deliver a number of cloud users simultaneously. This leads to the addition oftotal security aspects of virtualization technology on top of the existing securityconcerns and issues of cloud computing3

Figure 1:A Typical Cloud ArchitectureThe illustration of cloud architecture in figure 1 is a simplest one where fewcomplex characteristics of cloud computing (e.g. redundancy, server replication,and geographic dispersion of the cloud providers’ network) are not shown –the purpose of the illustration is to establish the arrangement that makes theconcept of cloud computing a tangible one. The network architecture is selfexplanatory with the identification of cloud users when considered in-line withthe discussion of the cloud computing concept presented earlier. One notablepart from the architecture is that, while the cloud users are clearly identified andnamed accordingly due to their remote location and means of remote access tothe cloud servers, the admin users who are administering the cloud servers arenot cloud users in any form with respect to the cloud service provider’s networkin the scenario. It is arguable whether the LAN users in figure 1 are cloud usersor not. Such room for argument could exist due to the phrase ‘cloud computing’being a concept rather than a technical terminology. If the definition of cloudcomputing is taken to have essential arrangements of being the servers locatedremotely that are accessed through public infrastructure (or through cloud),then the LAN users in figure 1 may not be considered as the cloud users inthe context. With respect to distributed and grid computing as the mothertechnology that define the infrastructural approach to achieve cloud computing,the LAN users in the scenario are essentially the cloud users when they usethe cloud services offered by the servers; the LAN users in this perspectiveare essentially using resources that are ‘borrowed’ from the servers on an on-demand basis. As depicted in figure 2, the technical details, arrangements andmanagement of the cloud service4

providers’ network is transparent to the cloud user. From the end of the clouduser, the service from the provider comes in the form of SaaS, PaaS or IaaSwhere the cloud user has no intention or worry about what goes on in the internalarrangement of the cloud service providers’ network. Any disruption of any formfor whatever is the reason, deem to the cloud users either as service unavailabilityor quality deterioration – its affect and ways to counter this disruption is acritical part for the cloud infrastructure. Security issues might play a stimulatingrole as a driving factor for any aforementioned disruption

.3 AUTHENTICATION IN CLOUDSecurity is the most prioritized aspect for any form of computing, making itan obvious expectation that security issues are crucial for cloud environmentas well. As the cloud computing approach could be associated with havingusers’ sensitive data stored both at clients’ end as well as in cloud servers,identity management and authentication are very crucial in cloud computing(Kim Hong, 2012; Emam, 2013; Han, Susilo Mu, 2013; Yassin, Jin, Ibrahim,Qiang Zou, 2012). Verification of eligible users’ credentials and protecting suchcredentials are part of main security issues in the cloud - violation in these areascould lead to undetected security breach (Kumar, 2012) at least to some extentfor some period. A possible authentication scenario for a cloud infrastructureis illustrated in figure 35

Figure 3:Authentication in the CloudThe illustration presented in figure 3 conveys that the authentication forthe cloud users can be done either by the cloud service provider or the serviceprovider can outsource the identity management and authentication service tothird party specialists (Gonzalez, Miers, Redigolo, Simplicio, Carvalho, NaslundPourzandi, 2012; Sharma Mittal, 2013). In the later case, the cloud serviceprovider is required to have collaboration with the third party authenticationspecialist – the collaboration between the cloud service provider and the thirdparty authentication specialist during the authentication process of cloud usersis done essentially through cloud. This feature adds performance overheadsand security issues to the cloud context as the message passing between thirdparty authentication management authority and the cloud service provider aspart of collaboration might essentially be done through cloud infrastructure.As discussed earlier, the total authentication process and how they are carriedout - regardless of the involvement of third party authentication specialists – istransparent to the cloud users. The illustration on the authentication scenariopresented above is a fairly simple one – if geographically dispersed servers aredeployed by the cloud service providers then the total authentication processmight be far more complex in terms of security, underlying algorithm as wellas performance level. Whatever is the level of complexity, the introduction ofthird party authentication and identity management specialist into any cloudarchitecture should have only one goal; and the goal is to strengthen the robust-ness of security in the concerned area which the cloud service provider itself isnot capable of to deploy or offer.4 SECURITY ISSUES IN CLOUDCloud computing comes with numerous possibilities and challenges simultane-ously. Of the challenges, security is considered to be a critical barrier for cloud6

computing in its path to success (Khorshed, Ali Wasimi, 2012). The securitychallenges for cloud computing approach are somewhat dynamic and vast. Datalocation is a crucial factor in cloud computing security (Teneyuca, 2011). Lo-cation transparency is one of the prominent flexibilities for cloud computing,which is a security threat at the same time – without knowing the specific lo-cation data storage, the provision of data protection act for some region mightbe severely affected and violated. Cloud users’ personal data security is thus acrucial concern in a cloud computing environment (Joint, Baker Eccles, 2009;Ismail, 2011; King Raja, 2012). In terms of customers’ personal or business datasecurity, the strategic policies of the cloud providers are of highest significance(Joint Baker, 2011) as the technical security solely is not adequate to addressthe problem. Trust is another problem which raises security concerns to usecloud service (Ryan Falvy, 2012) for the reason that it is directly related to thecredibility and authenticity of the cloud service providers. Trust establishmentmight become the key to establish a successful cloud computing environment.The provision of trust model is essential in cloud computing as this is a commoninterest area for all stakeholders for any given cloud computing scenario. Trustin cloud might be dependent on a number of factors among which some areautomation management, human factors, processes and policies (Abbadi Mar-tin, 2011). Trust in cloud is not a technical security issue, but it is the mostinfluential soft factor that is driven by security issues inherent in cloud comput-ing to a great extent. All kinds of attacks that are applicable to a computernetwork and the data in transit equally applies to cloud based services – somethreats in this category are man-in-the-middle attack, phishing, eavesdropping,sniffing and other similar attacks. DDoS (Distributed Denial of Service) attackis one common yet major attack for cloud computing infrastructure (Dou, ChenChen, 2013). The well known DDoS attack can be a potential problem for cloudcomputing, though not with any exception of having no option to mitigate this.The security of virtual machine will define the integrity and level of security ofa cloud environment to greater extent (Rakhmi, Sahoo Mehfuz, 2013; AgarwalAgarwal, 2011). Accounting authentication as well as using encryption fallswithin the practice of safe computing - they can be well considered as part ofsecurity concerns for cloud computing (Lee, 2012; Ogigau-Neamtiu, 2012; SinghJangwal, 2012). However, it is important to distinguish between risk and secu-rity concerns in this regard. For example, vendor lock-in might be consideredas one of the possible risks in cloud based services which do not essentially haveto be related to security aspects. On the contrary, using specific type of oper-ating system (e.g. opensource vs. proprietary) might pose security threat andconcerns which, of course, is a security risk. Other examples of business risksof cloud computing could be licensing issues, service unavailability, provider’sbusiness discontinuity that do not fall within the security concerns from a tech-nical viewpoint. Thus, in cloud computing context, a security concern is alwayssome type of risk but any risk cannot be blindly judged to be a security concern.Allocation of responsibilities among the parties involved in a cloud computinginfrastructure might result in experiencing inconsistency which might eventu-ally lead to a situation with security vulnerabilities. Like any other network7

scenario, the provision of insider-attack remains as a valid threat for cloud com-puting (Ogigau-Neamtiu, 2012). Any security tools or other kinds of softwareused in a cloud environment might have security loopholes which in turn wouldpose security risks to the cloud infrastructure itself. The problem with thirdparty APIs as well as spammers are threats to the cloud environment (BisongRahman, 2011; Singh Jangwal, 2012).As cloud computing normally means using public networks and subsequentlyputting the transmitting data exposed to the world, cyber attacks in any formare anticipated for cloud computing. The existing contemporary cloud basedservices have been found to suffer from vulnerability issues with the existenceof possible security loopholes that could be exploited by an attacker. Securityand privacy both are concerns in cloud computing due to the nature of suchcomputing approach (Bisong Rahman, 2011). The approach by which cloudcomputing is done has made it prone to both information security and networksecurity issues (Rakhmi, Sahoo Mehfuz, 2013; Qaisar Khawaja, 2012). Thirdparty relationship might emerge as a risk for cloud environment along withother security threats inherent in infrastructural and virtual machine aspects(Hashizume et al., 2013). Factors like software bugs, social engineering, humanerrors make the security for cloud a dynamically challenging one (Kim, 2009).Intrusion detection is the most important role in seamless network monitoringto reduce security risks. If the contemporary IDSs (Intrusion detection Systems)are inefficient, the resultant consequence might be undetected security breachfor cloud environment (Westphall et al., 2011).The facets from which the security threat might be introduced into a cloudenvironment are numerous ranging from database, virtual servers, and networkto operating systems, load balancing, memory management and concurrencycontrol (Hamlen et al., 2010). Data segregation and session hijacking are twopotential and unavoidable security threats for cloud users. One of the chal-lenges for cloud computing is in its level of abstraction as well as dynamism inscalability which results in poorly defined security or infrastructural boundary.Privacy and its underlying concept might significantly vary in different regionsand thus it may lead to security breach for cloud services in specific contexts andscenarios (Chen Zhao, 2012). Data loss and various botnets can come into ac-tion to breach security of cloud servers. Besides, multi-tenancy model is also anaspect that needs to be given attention (Kuyoro et al., 2011; Ogigau-Neamtiu,2012) when it comes to security. Security in the data-centres of cloud providersare also within the interests of security issues, as a single physical server wouldhold many clients’ data (Okuhara, Shiozaki Suzuki, 2010) making it a commonshared platform in terms of physical server or operating system. The storagesecurity at the cloud service providers data centres are also directly linked withthe security of the cloud services (Mircea, 2012). All the traditional securityrisks are thus applicable with added degree of potency in a cloud infrastruc-ture which makes the ongoing success of cloud computing a quite challengingone. Confidentiality, availability and integrity are the generalized categories intowhich the security concerns of a cloud environment falls. Threats for a cloudinfrastructure are applicable both to data and infrastructure (Agarwal Agar-8

wal, 2011).Different modes of data transfer and communication means (e.g. satellite com-munication) might need to take into account. Huge amount of data transfer isa common anticipation in a cloud environment, the communication technologyused along with the security concerns of the adapted communication technol-ogy also becomes a security concern for the cloud computing approach. Thebroadcast nature of some communication technology is a core concern in thisregard (Celesti, Fazio, Villari Puliafito, 2012). Cloud environment is associatedwith both physical and virtual resources and they pose different level of secu-rity issues – having no sophisticated authentication mechanism to fully addressthe security threats is an existing problem for cloud computing. It has mainlyresulted in the situations where grid computing has been taken as an embeddedpart of cloud computing (Casola, Cuomo, Rak Villano, 2013). As the virtual-ized resources are highly coupled with a cloud infrastructure, intrusion relatedsecurity concerns are of utmost priority as part of security issues. Arbitraryintermittent intrusion needs to be monitored in the operational context of acloud computing infrastructure where the severity of possibility for a virtualmachine to be compromised is to be taken into account (Arshad, TownsendXu, 2013). Some authors have argued that using Internet technologies is nota must for cloud computing (Khorshed et al., 2012) - but the cost efficiencyand globalization trends will enforce and motivate almost all the businesses toadmit Internet and associated technologies to be the ultimate means towardscloud computing approach. As a result, total Internet related security concernsare anticipated to be automatically added on top of the cloud-specific securityissues. Bringing portability is one of the means to make cloud services flexi-ble. The portability of cloud services would also be associated with securityconcerns. Cloud portability enables the cloud users to switch among differentcloud service providers without being affected with the necessity to change theways to accomplish tasks in different ways. It is a clear provision on bargainingpower for the cloud users; but at the same time, the security issues with cloudportability are to be counted. Cloud portability might bring severe degree ofAPI based security threats (Petcu, Macariu, Panica Craciun, 2013).The wide transition to mobile computing practices in recent years has madeit imperative to include mobile computing and its associated technologies asan essential part of cloud computing. Resource scarcity as well as other con-straints of mobile computing is barriers to cloud computing. The demand ofhuge data processing is a problem for mobile end-user devices which has beenfurther complemented by the security concerns of mobile cloud computing. Formobile cloud computing, the device level limitations has inspired researchers tosuggest the inclusion of another level of cloud termed as ‘mobile cloud’ to aidthe processing of the specific computing and processing for mobile computingdevices (Fernando, Loke Rahayu, 2013). The earlier explained broadcast na-ture of satellite communication and related security issues are equally applicableto the mobile cloud computing due to its being wireless communication. Be-sides, the addition of mobile cloud into the perspective would add another cloudwith all its security issues for a service provider having both mobile cloud and9

conventional cloud. The addition of mobile cloud in the scenario would boostperformance, but it would also add another layer of security issue not only tothe mobile cloud users, but also to the total infrastructure of the cloud serviceprovider. The hierarchical arrangement of cloud computing facilitates differentlevel of extensibility for the cloud users with varying degree of associated secu-rity issues (Che et al., 2011). Security issues for cloud computing are describedby some authors as an obvious one due to its nature. In a business model, therisks for the consumers are related to and dependent on the relevant approachesand policies of the cloud service providers the consumers are dealing with. Usingcloud products or services may lead to security concerns for the consumers ifthey are not well aware with the type and particulars of the products or servicesthey are to procure or to use in a cloud environment; this is also related to thecloud providers’ identity and reliability. One of the inherent problems in thiscontext is that, the consumers might normally not be able to identify or foreseeall the risks involved in the specific cloud transaction they are dealing with orinvolved in (Svantesson Clarke, 2010).5 CONCLUSIONSCloud computing has enormous prospects, but the security threats embeddedin cloud computing approach are directly proportional to its offered advantages.Cloud computing is a great opportunity and lucrative option both to the busi-nesses and the attackers – either parties can have their own advantages fromcloud computing. The vast possibilities of cloud computing cannot be ignoredsolely for the security issues reason – the ongoing investigation and research forrobust, consistent and integrated security models for cloud computing could bethe only path of motivation. The security issues could severely affect could in-frastructures. Security itself is conceptualized in cloud computing infrastructureas a distinct layer (Dukaric Juric, 2013). Security for cloud computing envi-ronment is a non-compromising requirement. Cloud computing is inevitable tobecome the ideal (and possibly the ultimate) approach to business computingthough the security barriers along with other issues need to be resolved forcloud computing to make it more viable (Marston, Li, Bandyopadhyay, ZhangGhalsasi, 2011) . Yet, given its total advantages and dynamism and provided itis deployed within an integrated and secured infrastructural framework, cloudcomputing can offer virtual ownership and access to ’super computers’ with-out procuring them physically. Perhaps this is what inspired coining the termSCC (Scientific Cloud Computing). Research effort has been contributed todevelop faster yet secured SCC tools (Jorissen, Villa Rehr, 2012) which willgreatly influence the pace of research and motivation in various fields togetherwith clouding computing itself. The social implications of cloud computing ap-proaches might emerge with severe impact if robust security models for cloudcomputing do not exist. The security issues for cloud computing are not relatedto the technical and direct security breach only; a number of social inconsis-tency might also be resulted even without any ‘hard’ security breach having10