IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, March 2024

An In-Depth Analysis of Trust, Security, and Privacy Concerns in Cloud Storage

Anjaney Shukla[1] and Dr. Narender Kumar[2]
Research Scholar, Department of Computer Science[1]
Research Guide, Department of Computer Science[2]
NIILM University, Kaithal, Haryana, India

Abstract: *Although cloud computing is controversial, many companies are transferring everything to the cloud. Most IT firms need cloud computing. Many users may utilize an integrated cloud computing infrastructure for storage, processing, and most significantly, scalability. Cloud computing offers scalable infrastructure for many services. Cloud computing problems include data security, access control, and privacy. Therefore, we must first identify cloud computing security threats, vulnerabilities, and issues. After assessing these issues, we must propose a cloud computing solution architecture that protects data, access, and privacy. Distribution of reused data needs data security.*

Based on well-known vulnerabilities and concerns, this paper examines major distributed computing security and protection difficulties. This article discusses security, privacy, and trust in current cloud computing settings and helps users recognize their risks, including cloud computing's. Assess distributed computing's core security, trust, and protection issues. (b) Assess approaches to reduce privacy, security, and confidence challenges to build cloud computing trustworthiness, security, and reliability. We will soon quantify cloud computing privacy, protection, and trust issues. A full cloud computing security, privacy, and trust management system will be created and deployed.

Keywords: Virtualization, Security Threats, and Vulnerabilities.

I. INTRODUCTION

As "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" [61], cloud computing exists. Digital computer paradigm shift cloud computing promotes availability, cost, and flexibility. Cloud computing is prevalent now. Cloud services use economies of scale via specialized infrastructure, productivity benefits, and other methods. However, distributed computing is evolving. The phrase has several meanings [33]. There are three common service models [58, 78, 85]. Software implementation platforms may provide one or more applications and computing resources as a SaaS service without upfront costs. Hardware and software development, repair, and maintenance expenses decrease. PaaS makes the programming platform available for application development and execution on demand. The cost and complexity of purchasing, lodging, and administering network gear and software will decrease.

IaaS provides on-demand servers, software, and network infrastructure. This infrastructure supports app creation and execution. It buys, stores, and controls conventional hardware and software infrastructure components discreetly.

Cloud computing should be utilized secretly in company computers. Cloud computing's major purpose is to allow other firms outsource specific environment features, according to service models. IT outsourcing—moving sensitive applications or data from the company's computer center to another—raises data security and privacy risks. Cost reductions are the key incentive to transition to the cloud, but security and privacy should not be sacrificed. The business oversees all outsourcing. The organization handles performance, availability, recovery, security, and privacy.

Cloud computing, a long-standing "computing as a service" idea, has transformed IT software and hardware purchases and usage and attracted national governments, international agencies, and global and local IT players [1,3,4].Cloud computing includes much. Cloud computing swiftly builds and publishes adaptable, virtualized, elastic, and widely accessible computer services using economies of scale. Little management is required in data centers. On-demand

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, March 2024

services are provided via high-speed Internet using a "X as a Service (XasS)" machine architecture with "platforms," "applications," and "infrastructure." Flexible installation and extendable processing, storage, and network software should be easy to purchase. [3][4]. Hardware and technology costs are reduced for IT organizations using distinct application technology approaches.

These issues include cloud servers that access physical files, manage identities and certificates, authenticate data, update, ensure integrity, prevent security breaches, and be irresponsible. To secure sensitive data in data centers, cloud consumers must authenticate (a) the cloud computing system's global existence. Data storage and software stability in the cloud. In cloud data centers, security and resource control are compromised.

This paper examines cloud infrastructure's significant security and privacy issues while outsourcing organizational computing functions. It detects areas of interest that require further examination and makes pertinent security judgments. Modern cloud computing systems have trust difficulties, and this article explains their vulnerabilities. We examine the major privacy, security, and trust issues in current cloud computing settings and analyze the best approaches to minimize them to create a safe, dependable, and efficient cloud storage solution.

The paper's sections follow. Section II covers data security. Cloud data privacy is covered in Section III. Cloud computing trust is addressed in Section IV. Section V addresses data availability. Conclusions and research ideas are in Section VI.

Data Security Issues

Data safety is "a combination of privacy, the prevention of unauthorized information exposure, information integrity, information withholding prevention, and unauthorized information modification or deletion" [13]. Data security prohibits unauthorized system changes. Security requires efficiency, confidentiality, and honesty. Security hinders the long-awaited computing as a service future.

Cloud computing security has six subcategories: data and entity confidentiality, preventing malevolent insiders from doing unlawful activities, and deterring them due to the provider system's lack of transparency [5,6,7,11,14]. (d) Strategies to prevent network hijacking in settings prone to phishing, malware, and harassment, common IT issues; and (e) Methods for managing numerous instances in multi-tenancy network environments assuming all instances are isolated. But this principle will fail, allowing attackers to traverse virtual machine side channels, bypass the sandbox, and gain full host access; and (f) ways to establish regulatory jurisdiction and create regulations that let consumers hold vendors accountable.

Cloud data is used in global user data networks. Thus, organizations that migrate sensitive data to the cloud must safeguard access and preserve it.

Data-Isolate:

Many data formats exist. In addition to development tools, cloud-based application development involves programs, templates, and configuration settings. This includes user account data, documentation, and application-generated or utilized things. Encryption or access limits may prevent data theft. User identity verification is critical in cloud computing since it restricts data access.

The cloud database environment varies. Some arrangements employ multi-instance, others multi-intent. Service customers may acquire a VM with a database management system for job definition, user permission, and other security-related administrative tasks. Adding a user ID to data provides a shared cloud service client environment.

Many databases provide multi-tenant solutions. Service separation and consumption vary when resources are pooled [26, 65]. Other factors must be considered. Data encryption needs independent databases, not shared ones. The data management system's compatibility with essential data must be considered due to these tradeoffs. Healthcare standards may affect application storage and data management. Many worry about privacy-sensitive data [52].

Data must be protected throughout storage, transfer, and use, and access regulated. Public key certificates and protocol standards secure cryptographic data transmissions. Due to unique applications, data storage at rest requirements vary, hindering interoperability. Incompatibility hinders cloud service provider application, data transmission, and access. Cloud clients now handle crypto keys. To prevent hardware authentication devices that scale poorly, key generation and storage are done outside the cloud. To solve the problems, government-use cryptographic secret key management and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, March 2024

exchange systems are being developed. The confidence approach [22] is the most important information usage security protection, an emerging cryptographic issue with few experiments.

Data-Sanitize:

Data sanitization by the service provider affects safety. Decommissioning or moving a storage unit eliminates sensitive data. Backups to restore the service and residual data after termination are included. Due of physical data integration, cloud computing may be challenging. Given talent and equipment, service providers' improperly disposed-of broken drives may hold data.

Data Location:

Firms with sensitive data often face this compliance difficulty [30, 51]. An internal database center helps the organization coordinate processes and assess data storage and security. Multiple cloud storage companies offer inaccurate data status information. The existing condition makes assessing safeguards and legal and regulatory compliance challenging. Security certifications and external audits may assist, but not cure.

International legislation makes protecting sensitive data across borders challenging. The USA Patriot Act's broad authority worries other nations because it might provide the US government access to sensitive data, including medical records outsourced to American corporations [5]. Data confidentiality and cross-border transit of non-classified private information are covered by domestic and international privacy and security legislation [12]. Cross-border data transfers must examine how much the jurisdiction where the data is obtained authorizes the flow, how those restrictions apply to transferred data, and external challenges to the legislation at the destination [12]. Access is limited and institutional, physical, and technical safeguards apply. For European data relocated to the US, data protection standards may need additional processing and administration [9].

Data Privacy Issues

Privacy lets individuals and organizations differentiate themselves or reveal information selectively. Includes (15): In what context: a person may be more worried about sharing current or future information than prior information; in what manner: a user may accept peers manually asking their information without notifying them. The scope For business, consumer, and privacy reasons, client information must be safeguarded and handled correctly to meet customer expectations. Organizational privacy involves processes, rules, and norms for managing personal data [8].

Cloud privacy issues come into four categories. [5][6][8]. Subcategories include (a) ensuring clients retain data control throughout cloud gathering and processing and (b) preventing illegal selling, misuse, and infringement. (b) This section describes how to accurately replicate consumer data in multiple acceptable locations and a jurisdiction where data loss, misuse, unauthorized modification, or fabrication can be prevented; (c) This section specifies the entity that enforces personal information security obligations.

Trust Issues

Quantified trust requires informed judgment to make reliable judgments. It linked individuals in social science and secures distant computer systems today. Secrecy, dependability, honesty, impartiality, protection, and competence are soft security qualities of confidence. Situational, non-symmetrical, ambiguous, and partially transitive, trust between individuals is the most difficult relationship [9,10].

Trust assessment is a phased, multidimensional procedure that uses time and multiple elements to connect or avoid nodes. Applying [16]'s trust perception definition: "Party A's trust in Party B's service X is A's observable expectation that B will behave consistently." Reference [17] presents another mathematical confidence standpoint. "Confidence, or, conversely, distrust, is a straightforward degree of subjective probability by which an agent ascertains whether a specific action will be executed by another agent or a group of agents, both prior to its ability to independently or independently monitor the action and in a manner that influences its own action." Security measures like encryption and permission safeguard cloud environments. Malignant actors exploit cooperation's breadth and transience, decreasing its effectiveness.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, March 2024

Trust's soft social security technique protects communications from malicious actors and builds a reliable cloud computing infrastructure. Four kinds of cloud computing trust challenges exist [5][6,8,12]. These include how to establish and quantify trust in cloud computing settings, handling very sensitive harmful suggested data, recognizing and reporting the service security-trust gap, and creating A company offers a cloud service provider full authority over security domains, boosting trust.

Insider Access:

Data outside a business is exposed to firewalls and other security mechanisms. Most organizations worry about insider security, particularly in cloud outsourcing [21,54]. Insider dangers include current and former employees, partners, suppliers, and anyone who utilized the company's networks, systems, and data. Accidents may happen. Moving data to the cloud may protect service provider personnel and consumers. A user created 20 accounts and ran virtual machine instances for each in an internal denial of service attack on Amazon Elastic Compute Cloud (EC2). These accounts spawn 20 additional accounts and system instances, intensifying the attack and consuming resources [76].

Composite Services:

Additional cloud providers may supply services in nesting and stratification. PaaS or IaaS may be used by SaaS vendors. Cloud service providers may have third-party administration, obligations, and solutions difficulties. Ensure that third-party agreements are current before signing a contract with the service provider and that particular agreements are followed throughout the partnership, unless the service provider gives thorough information of any anticipated modifications. Composite cloud companies' performance and responsibility may be an issue. Online storage company Linkup folded, depriving 20,000 users access to loads of content. Responsibility for the disaster was unclear since Nirvanix stored The Linkup's data while Savvis hosted its application and database [18].

Visibility:

Cloud computing provides service providers power over enterprise data and software networks. Implementation must follow internal organizational system rules to prevent administrative, technological, security, and control breaches. Since the two computer systems' security requirements are being studied [27], the problem is insoluble. Operational audits and exposure are affected by most service agreements' network and system access limitations. Service agreements should make the provider's compliance processes more visible and durable. This ensures the equipment follows rules throughout its life.

Risk Management:

Software and knowledge regulators cannot control cloud-based application subsystems or components. Controlling systems and equipment makes people feel safer. Superiors inspire people to evaluate alternatives, prioritize, and make solid decisions that benefit the organization in unforeseen circumstances. Consider uncertainty before in-house or cloud implementation. Cloud risk evaluation and mitigation are difficult. The organization's capacity to oversee the external service provider's security measures to secure the operation and evidence of such controls should build confidence [29]. However, security measures and module functionality cannot be appraised as accurately as the operational framework, thus extra factors must be considered when judging confidence.

Availability Issues

Availability implies users always have full access to computer services. Disability may be temporary or permanent. Natural disasters, service rejections, and system outages threaten availability.

Temporary Outages:

Cloud computing services might fail and slow down despite strong availability and reliability [58]. Amazon's Easy Storage Infrastructure (S3) and EC2 services were unavailable to Twitter and other startups for three hours in February 2008 [55,63]. A June 2009 lightning storm left EC2 partially down for four hours [64]. In February 2008, the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, March 2024

Salesforce.com storage cluster failure caused a several-hour outage, while in January 2009, a network problem caused a shorter outage [31,37]. Networking modifications took Azure unavailable for 22 hours in March 2009 [24].
With 99.999 percent reliability, 8.76 hours of disruption are projected annually. An organization must assess its cloud infrastructure's backup and recovery capabilities and stability and develop strategies to restore damaged cloud systems and processes via alternative networks, facilities, and locations. Cloud computing may be susceptible to hosted software. When this occurs, another cloud storage provider may backup primary provider data. This keeps data available and speeds up important tasks after a severe catastrophe or main-level disruption.

Prolonged and Permanent Outages:
The FBI seized hundreds of computers from Texas data centers in April 2009 to investigate fraud charges against several corporations [86]. The hack affected network operations at hundreds of other firms, not involved in the probe. Magnolia lost a lot of data, Bookmark abruptly stopped, and Omni Drive, an online storage firm, shut down without warning in 2008 [37, 58].

Denial of Service:
Application denial attacks flood the target with bogus requests to prevent it from responding to genuine ones. An opponent generally requires a botnet or multiple computers to access. Defense against a thwarted DDoS attack might be expensive. Cloud provisioning flaws may let attackers strike. Machines may break into cloud services, which are valuable [28]. Bit Bucket, a code hosting platform, was down for 19 hours by an Amazon cloud infrastructure denial of service assault [19, 62]. Denial of service attacks may target public and private networks, including cloud computing. Exponential system instance replication was used in an Amazon Cloud Services API DDoS assault [76]. Service providers' centrally assigned non-routable addresses used to administer network services may be attack vectors. An atom from one cloud is less likely to be attacked by another or its components [45].

II. CONCLUSION AND FUTURE WORK

The largest security risks have been handled, but other uncertainties persist despite the cloud's cost savings and performance improvements. Insufficient development of key technical components like a federated confidence system inhibits deployments. The long-term challenge of securing sophisticated computer systems follows large-scale computing. Information security professionals must meet high software quality standards. This continues in cloud computing. Strong processing and cryptography are needed for cloud reliability. Enterprise cloud or service center rules must secure organizational data. A complete support framework for cloud services and entities is missing. Starting with conventional outsourcing requirements—privacy and security procedures, compliance and regulatory difficulties, service quality standards and penalties, change management processes, quality of service implementation, and the ability to cancel—is practicable [51]. The cloud storage transfer may be dangerous. Research employs qualitative and quantitative methodologies. Given the organization's security duties, risks and benefits must be weighed against available solutions. If benefits outweigh costs and hazards, many restrictions may be disruptive and harmful. Control strength and program and process risk must be balanced.
High security precludes the long-awaited benefit of computers in the contemporary day. They employ virtual PCs to move critical systems and data to cloud storage centers. Virtualization, mobile app, and accessibility issues arise from these specific qualities. The rise of cloud computing and users may bring stability, privacy, and trust concerns. L-paragraphs deserve indentation. Right- and left-justified paragraphs must be justified. To protect sensitive data in data centers, the cloud user wishes to check (a) the global cloud computing environment, (c) cloud data security, and (b) cloud storage service security.
This article shows the major cloud computing security, privacy, and confidence challenges to assist users grasp the physical and intangible. This article explores current cloud computing's main data protection, security, and confidence challenges and proposes solutions to privacy, trust, and future technological threats to establish a stable, safe, and efficient ecosystem.
An initial survey and review approach is used to quantify cloud computing privacy, security, and trust problems. Quantitative evaluation and assessment will be the focus of future study. (b) providing maximal privacy protection,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, March 2024

trust assessment, and management privacy concerns; and (c) demonstrating cloud computing framework implementation.

REFERENCES

[1]. 20-Year Term in Plot to Bomb IRS Offices, Nation InBrief, Los Angeles Times, August 10, 1996
A. Greenberg, IBM's Blindfolded Calculator, ForbesMagazine, July 13, 2009
[2]. Ahamed S I, Haque M M, Endadul Hoque M, Rahman F, Talukder N. Design, analysis, and deployment of omnipresent formal trust model (FTM) with trust bootstrapping for pervasive environments. Journal of Systems and Software ; 2010;83(2):253–270.
[3]. Algirdas A, Jean-Claude L, Brian R, Carl L. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing; 2004;1(1):11–33.
[4]. Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A View of Cloud Computing. Communications of the ACM; 2010;53(4):50–58.
[5]. B. R. Kandukuri, R. Paturi V, A. Rakshit, Cloud Security Issues, IEEE International Conference on Services Computing, Bangalore, India, September 21- 25, 2009
[6]. Buyya R, Chee Shin Y, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems; 2009;25(6):599–616.
[7]. C. Brooks, Amazon EC2 Attack Prompts Customer Support Changes, Tech Target, October 12, 2009, http://search cloud computing.techtarget.com/news/article/0,289142,sid201_gci1371090,00.html
[8]. C. Metz, DDoS Attack Rains Down on Amazon Cloud, The Register, October 5, 2009, http://www.there gister.co.uk/ 2009/ 10/05/amazon_bitbucket_outage/
[9]. D. Cappelli, A. Moore, R. Trzeciak, T. J. Shimeall, Common Sense Guide to Prevention and Detection of Insider Threats,3rd Edition, Version 3.1, CERT, January 2009, http://www.cert.org/archive/pdf/CSG-
[10]. D. Goodin, Salesforce.com Outage Exposes Cloud's Dark Linings, The Register, January 6, 2009, http://www.theregister.co.uk/2009/01/06/salesforce_outage/
[11]. D. Goodin, Webhost Hack Wipes Out Data for100,000 Sites, The Register,June 8, 2009,http://www.theregister.co.uk/2009/06/08/webhost_atta ck/
[12]. D. Jacobs, S. Aulbach, Ruminations on Multi-Tenant Databases, Fachtagung für Datenbanksysteme in Business, Technologie und Web, March 2007, http://www.btw2007.de/paper/p514.pdf
[13]. Foster I, Zhao Y, Raicu I, Lu, S. Cloud Computing andGrid Computing 360-degree compared. Proceedings ofthe Grid Computing Environments Workshop, GCE2008; IEEE Press, Nov. 2008, 1-10.
[14]. G. Clarke, Microsoft's Azure Cloud Suffers FirstCrash, The Register, March 16, 2009,http://www.theregister.co.uk/ 2009/03/16/azure_cloud_crash/
[15]. G. Fowler, B. Worthen, The Internet Industry is on a Cloud – Whatever That May Mean, The Wall Street Journal, March 26, 2009
[16]. Guide for Applying the Risk Management Framework to Federal Information Systems, Joint Task Force Transformation Initiative, Special Publication 800-37,
[17]. Iltaf N, Hussain M, Kamran F. A mathematical approach towards trust based security in pervasive computing environment. Proceedings of the Third International Conference and Workshops, ISA 2009IEEE Press, Jun. 2009, 702-711.
[18]. J. Brodkin, Loss of Customer Data Spurs Closure of Online Storage Service 'The Linkup,' Network World, August 11,2008,
[19]. J. E. Dunn, Ultra-secure Firefox Offered to UK BankUsers, Techworld, February 26, 2010, http://news.techworld.com/security/3213740/ultra- secure-firefox-offered-to-uk-bank-users/
[20]. J. E. Dunn, Virtualised USB Key Beats Keyloggers,Techworld, February 22, 2010, http://news.techworld.com/security/3213277/virtualise d-usb-key-beats-keyloggers/
[21]. J. Oberheide, E. Cooke, F. Jahanian, Empirical Exploitation of Live Virtual Machine Migration, Black Hat Security Conference, Washington, DC, February 2008

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, March 2024

[22]. J. Wei et al., Managing Security of Virtual Machine Images in a Cloud Environment, ACM Cloud Computing Security Workshop, Nov. 13, 2009,

[23]. J.D.Sutter,Twitter Hack Raises Questions about 'Cloud Computing', CNN, July 16, 2009, http://edition.cnn.com/2009/TECH/07/16/twitter.hack/

[24]. K. Vieira, A. Schulter, C. Westphall, C. Westphall, Intrusion Detection Techniques in Grid and Cloud Computing Environment, IT Professional, IEEE Computer Society, August 26, 2009.

[25]. K. Zetter, FBI Defends Disruptive Raids on Texas Data Centers, Wired Magazine, April 7, 2009, http://www.wired.com/threatlevel/2009/04/data- centers-ra/

[26]. Karaoglanoglou K, Karatza H. Resource discovery in aGrid system: Directing requests to trustworthy virtual organizations based on global trust values. Journal of Systems and Software; 2011;84(3):465–478.

[27]. Krumm J. A survey of computational location privacy. Personal and Ubiquitous Computing; 2009;13(6):291–399.

[28]. L. M. Vaquero1, L. Rodero-Merino1, J. Caceres, M. Lindner, A Break in the Clouds: Towards a Cloud Definition, Computer Communication Review, January 2009, http://ccr.sigcomm.org/online/files/p50-v39n1l-vaqueroA.pdf

[29]. L. Whitney, Amazon EC2 Cloud Service Hit by Botnet, Outage, December 11, 2009, CNET News, http://news.cnet.com/8301-1009_3-10413951-83.html

[30]. L. Youseff, M. Butrico, D. D. Silva, Toward a Unified Ontology of Cloud Computing, Grid Computing Environments Workshop, held with SC08, November 2008.

[31]. M. Calore, Ma.gnolia Suffers Major Data Loss, SiteTaken Offline, Wired Magazine, January 30, 2009, http://www.wired.com/epicenter/2009/01/magnolia- suffer/

[32]. M. Gunderloy, Who Protects Your Cloud Data?, WebWorker Daily, January 13, 2008, http://web worker daily.com/2008/01/13/who-protects- your-cloud-data/

[33]. M. Jensen, J. Schwenk, N. Gruschka, L. L. Iacono, On Technical Security Issues in Cloud Computing, IEEE International Conference on Cloud Computing,

[34]. M. Krigsma, Amazon S3 Web Services Down. Bad, Bad News for Customers, ZDNET, February 15, 2008, http://blogs.zdnet.com/projectfailures/?p=602

[35]. M. P. Eisenhauer, Privacy and Security Law Issues in Off-shore Outsourcing Transactions, Hunton & Williams LLP,The Outsourcing Institute, February 15,2005,

[36]. M. P. Eisenhauer, Privacy and Security Law Issues in Off-shore Outsourcing Transactions, Hunton & Williams LLP, The Outsourcing Institute, February 15,2005,

[37]. M. Slaviero, BlackHat presentation demo vids: Amazon, part 4 of 5, AMIBomb, August 8, 2009,http://www.sensepost.com/blog/3797.html

[38]. Malicious-Firefox-Add-Ons.htm

[39]. Mell P, Grance T. The NIST Definition of Cloud Computing. Communications of the ACM; 2010;53(6):50.

[40]. N. Gruschka, L. L. Iacono, Vulnerable Cloud: SOAP Message Security Validation Revisited, IEEE International Conference on Web Services, Los Angeles, CA, July 2009

[41]. N. Katz, Austin Plane Crash: Pilot Joseph Andrew Stack May Have Targeted IRS Offices, Says FBI, CBS News, February 18, 2010, http://www.cbsnews.com/8301-504083_162-6220271-504083.html?tag=content Main%3bcontentBody

[42]. N. Leavitt. Is Cloud Computing Really Ready forPrime Time?, IEEE Computer, January 2009

[43]. N. Provos et al., The Ghost In The Browser: Analysis of Web-based Malware, Hot Topics in Understanding Botnets (HotBots), April 10, 2007, Cambridge, MA

[44]. N. Provos, M. A. Rajab, P. Mavrommatis, Cybercrime 2.0: When the Cloud Turns Dark, Communications of the ACM, April 2009

[45]. Office, New York Times, December 29, 1995

[46]. P. A. Karger, I/O for Virtual Machine Monitors: Security and Performance Issues, IEEE Security and Privacy, September/October 2008

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, March 2024

[47]. P. Ferrie, Attacks on Virtual Machine Emulators, White Paper, Symantec Corporation, January 2007, http://www.symantec.com/avcenter/reference/Virtual_ Machine_Threats.pdf

[48]. P. Mell, T. Grance, The NIST Definition of Cloud Computing, Version 15, October 7, 2009, http://csrc.nist.gov/groups/SNS/cloud-computing

[49]. P. Wainewright. Many Degrees of Multi-tenancy, ZDNET News and Blogs, June 16, 2008, http://blogs.zdnet.com/SAAS/?p=533

[50]. Paquette S, Jaeger P T, Wilson S C. Identifying the security risks associated with governmental use of cloud computing .Government InformationQuarterly; 2010;27(3):245–253.

[51]. Pearson S, Benameur A. Privacy, security and trust issues arising from cloud computing. Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010; IEEE Press, Nov. 2010, 693-702.

[52]. R. Chow et al., Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control, ACM Workshop on Cloud Computing Security, Chicago, IL, November 2009

[53]. R. Mc Millan, Hackers Find a Home in Amazon's EC2Cloud, Infoworld, IDG News Network, December 10,2009, http://www.infoworld.com/d/cloud- computing/hackers-find-home-in-amazons-ec2-cloud- 742 Hospital, PC Magazine, News Service Sept.17,2009,http://www.pcworld.com/bu sinesscenter/article/172185/misdirected_spyware_infec ts_ohio_hospital.

[54]. R. Mc Millan, Sales force.com Warns Customers ofPhishing Scam, PC Magazine, IDG News Network, November 6, 2007, http://www.pcworld.com/businesscenter/article/ 139353/salesforcecom_warns_customers_of_phishing

[55]. R. Miller, Lightning Strike Triggers Amazon EC2 Outage, Data Center Knowledge, June 11, 2009, http://www.datacenterknowledge.com/archives/2009/0 6/11/lightning-strike-triggers-amazon-ec2-outage/

[56]. R. Miller, Major Outage for Amazon S3 and EC2,Data Center Knowledge, February 15, 2008,http://www.data center knowledge.com/archives/ 2008/02/15/ major-outage-for-amazon-s3-and-ec2/

[57]. S. Cocheo, The Bank Robber, the Quote, and the Final Irony, nFront, ABA Banking Journal, 1997 http://www.banking.com/aba/profile_0397.htm

[58]. S. Frei, T. Duebendorfer, G. Ollmann, M. May, Understanding the Web Browser Threat, ETH Zurich, Tech Report Nr. 288, 2008, http://e- collection.ethbib.ethz.ch/eserv/eth:30892/eth-30892-01.pdf

[59]. S. Gajek, M. Jensen, L. Liao, and J. Schwenk, Analysis of Signature Wrapping Attacks and Countermeasures, IEEE International Conference onWeb Services, Los Angeles, CA, July 2009

[60]. S. Garfinkel, An Evaluation of Amazon's Grid Computing Services: EC2, S3 and SQS, Technical Report TR-08-07, Center for Research on Computationand Society, Harvard University, July 2007

[61]. S. King et al., SubVirt: Implementing Malware with Virtual Machines, IEEE Symposium on Security and Privacy, Berkeley, California, May 2006

[62]. S. Labaton, 2 Men Held in Attempt to Bomb I.R.S.

[63]. S. M. Kerner, Mozilla Confirms Security Threat from Malicious Firefox Add-Ons, eSecurity Planet, February 5, 2010,http://www.esecurityplanet.com/news/article.php/3863 331/Mozilla-Confirms-Security-Threat-From-

[64]. S. Overby, How to Negotiate a Better Cloud Computing Contract, CIO, April 21, 2010, http://www.cio.com/article/591629/How_to_Negotiate

[65]. S. Pearson, Taking Account of Privacy when Designing Cloud Computing Services, ICSE Workshop on Software Engineering Challengesof Cloud Computing, May 23, 2009, Vancouver,

[66]. Safe Harbor Privacy Principles, U.S. Department of Commerce, July 21, 2000, http://www.export.gov/safeharbor/eg_main_018247.as p

[67]. Sangroya A, Kumar S, Dhok J, Varma V. Towards analyzing data security risks in cloud computing environments.Communications in Computer and Information Science; 2010;54:255-265.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, March 2024

[68]. Security Within a Virtualized Environment: A New Layer in Layered Security, White Paper, Reflex Security, retrieved April 23, 2010, http://www.vmware.com/files/pdf/partners/security/sec urity-virtualized-whitepaper.pdf

[69]. Shah, Kernel-based Virtualization with KVM, Linux Magazine, issue 86, January 2008, http://www.linux magazine.com/w3/issue/86/Kernel_B ased_Virtualization_With_KVM.pdf

[70]. Shekarpour S, Katebi S D. Modeling and evaluation of trust with an extension in semantic web. Journal of Web Semantics;2010;8(1):26–36.

[71]. Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal ofNetwork and Computer Applications; 2011;34(1):1–11.

[72]. T. Ferguson, Salesforce.com Outage Hits Thousands of Businesses, CNET News, January 8, 2009, http://news.cnet.com/8301-1001_3-10136540-92.html

[73]. T. Garfinkel, M. Rosenblum, When Virtual is Harder than Real, HotOS'05, Santa Fe, NM, June 2005

[74]. T. Ormandy, An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments, 2007,

[75]. T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, ACM Conference on Computer and Communications Security, November 2009

[76]. T. Shelton, Remote Heap Over flow, ID: ACSSEC- 2005-11-25 - 0x1, http://packet storm security.org/0512-advisories/ACSSEC-2005-11-25-0x1.txt

[77]. Takabi H, Joshi J B D, Ahn G. Security and privacy challenges in cloud computing environments. IEEE Security & Privacy;2010;8(6):24–31.

[78]. Tchifilionova V. Security and privacy implications of cloud computing - Lost in the cloud. Proceedings ofthe IFIP WG 11.4 International Workshop on Open Research Problems in Network Security, iNetSec 2010; Springer Verlag Press, Mar.2010,149-158.

[79]. Twitter Email Account Hack Highlights Cloud Dangers, Infosecurity Magazine, July 23, 2009, http://www.infosecurity- magazine.com/view/2668/twitter-email-account-hack- highlights-cloud-dangers-/

[80]. USA Patriot Act Comes under Fire in B.C. Report,CBC News, October 30, 2004,

[81]. Vaquero L M, Rodero-Merino L, Morán D. Locking the sky: A survey on IaaS cloud security. Computing; 2011;91(1):93–118.

[82]. VMware Hosted Products and Patches for ESX and ESXi Resolve a Critical Security Vulnerability, VMware Security Advisory,VMSA-2009-0006, http://www.vmware.com/security/advisories/VMSA-2009-0006.html

[83]. VMware Vulnerability in NAT Networking, BugTraq, Security Focus, December 21, 2005, http://www.securityfocus.com/archive/1/420017

[84]. W. Jansen, Directions in Security Metrics Research, Interagency Report 7564, National Institute ofStandards and Technology (NIST), April 2009

[85]. Xen Architecture Overview, Version 1.2, Xen WikiWhitepaper, February 13, 2008,

[86]. Y. Keleta, J. H. P. Eloff, H. S. Venter, Proposing a Secure XACML Architecture Ensuring Privacy and Trust, Research in Progress Paper, University of Pretoria, 2005,