Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 11, November : 2023

A SURVEY ON SECURITY, PRIVACY, ACCOUNTABILITY AND TRUST ISSUES IN CLOUD COMPUTING

#1**MANOJ KUMAR BONDUGULAPATI,** *Research Scholar,*
#2**Dr. V.MADHUKAR**, *Associate Professor,*
Department of Computer Science,
CHAITANYA (Deemed to be University), HANAMKONDA, WARANGAL-TS, INDIA

Abstract: The internet offers users the opportunity to utilize cloud computing services that are dynamic and scalable. This study explores how users can benefit from a greater range of options at a lower personal cost. Concerns over data safety prevent a significant number of software programs from being suitable for migration to cloud-based systems. This study highlights various issues within the domain of technical security, as revealed by recent research. This text discusses various problems related to browser security, cloud malware injection attacks, integrity and binding methods, and more. Ensuring compliance with regulations, efficient data management, and fostering trust among users are key factors in safeguarding personal information. This article examines various legal strategies for addressing privacy, security, and trust concerns in the digital realm.

Keywords: *Security Attacks, Trust, Privacy, Act and Laws, Accountability.*

1. INTRODUCTION

This framework defines cloud as Internet hosting. This clever super computing model, gives users access to computational resources like networks.

Infrastructure includes hosting, archiving, and services. Cloud computing is a popular distributed computing subset due to its many benefits. Cloud computing is described by the CSA as

Cloud Computing is a model for enabling ubiquitous, convinient, on-demand network access to a shared pool of configurable computing resources.

Only lately have cloud services evolved. Evolution also created it. First to offer cloud-based business software online was SALESFORCE.COM in 1999. Grid computing preceded cloud computing.

GRID COMPUTING-

More powerful computers are needed for harder jobs as computing improves. This led to grid computing in the mid-1990s. Foster and Kesselman (1999) attribute grid computing's popularity, reliability, and usability to the power grid.

GRID AND UTILITY COMPUTING
APPLICATION SERVICE PROVISION
OFTWARE AS A SERVICE

Fig1. Temporal Cloud Formation Variations

NIST The cloud computing paradigm was shown using four deployment methodologies and three cloud service types. Several examples:

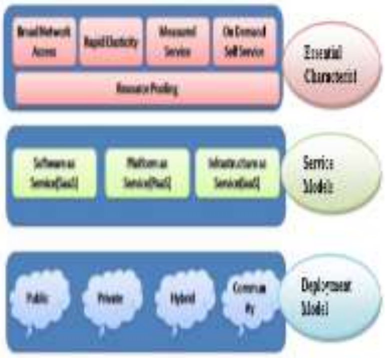


Fig .2 The NIST Definition of Cloud Computing

A 2011 Ernst & Young Global Information Security research found that enterprises are increasingly adopting cloud services, and this trend is expected to continue. A pie chart shows the study's 2010 and 2011 cloud consumer comparison.

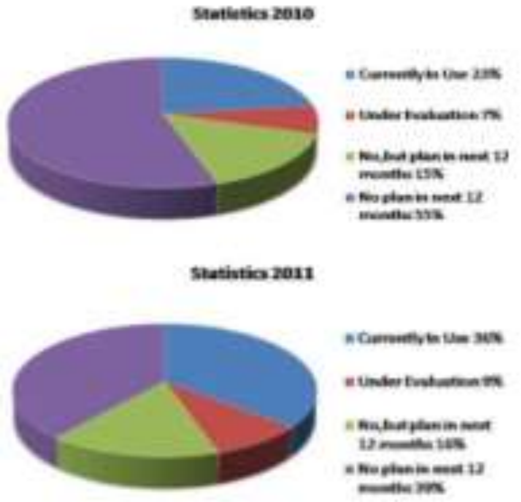


Fig 3 2011 Ernst & Young Global Information Security Survey results

2. SECURITY AND CLOUD COMPUTING

Although cloud computing has proven beneficial, it has also uncovered new security concerns. These security weaknesses have raised user concerns about the system's reliability. Threats can take many forms, including

- denial-of-service (DDOS) attacks or similar conditions could drain a server's resources,
- competitors in the same industry who employ standard methods to obstruct service.
- Cloud computing security has become a new information security branch.
- Provider security.
- Users face security risks**.**

Trend Micro's 2011 Canadian SME IT Security Survey found that cloud service providers and clients prioritize security and data privacy.

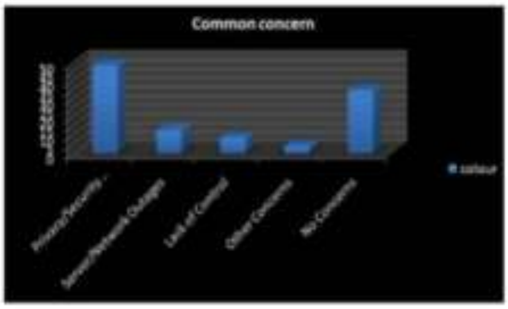


Fig 4. Trend Micro studied

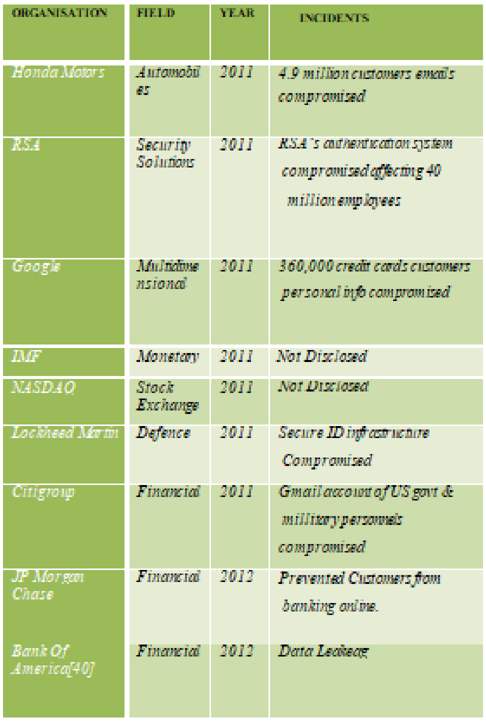
Recent Security Attacks In Cloud

IDC cloud research emphasizes cloud service demand's exponential growth, topping $55.5 billion that year. However, recent data breaches and crimes have raised concerns about cloud security. Recent security holes have compromised client data.

Epsilon Breach : Epsilon, a third-party email marketing and security provider, reported that an unauthorized user had accessed their system using an application layer protocol vulnerability on April 1, 2011. Epsilon may have lost $412 million to $637 million due to cyber breaches that affected 3% of its clients and 75 organizations, according to a risk analytics intelligence firm.

Amazon Breach : Foursquare and Quora were inaccessible due to Amazon cloud service issues. Financial malware is being transmitted via Amazon cloud to steal hardware and software data, according to Kaspersky.

Sony Playstation Network Breach: The PlayStation Network was hacked, exposing 77 million PlayStation owners' personal data. One of the biggest compromises ever. Goals are endless:



ORGANISATION	FIELD	YEAR	INCIDENTS
Honda Motors	Automobiles	2011	4.9 million customers emails compromised
RSA	Security Solutions	2011	RSA`s authentication system compromised affecting 40 million employees
Google	Multidimensional	2011	360,000 credit cards customers personal info compromised
IMF	Monetary	2011	Not Disclosed
NASDAQ	Stock Exchange	2011	Not Disclosed
Lockheed Martin	Defence	2011	Secure ID infrastructure Compromised
Citigroup	Financial	2011	Gmail account of US govt & millitary personnels compromised
JP Morgan Chase	Financial	2012	Prevented Customers from banking online.
Bank Of America[40]	Financial	2012	Data Leakeag

According to Gartner research titled Assessing the Security Risks of Cloud Computing, customers should ask about security in the following seven ways before using cloud service providers.

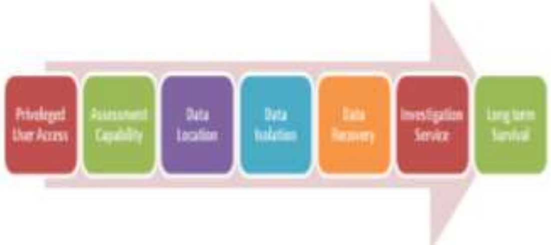


Fig 5. Client concerns to fix (Gartner)

3. SECURITY ATTACKS AND SOLUTIONS IN CLOUD

The results of cloud security polls have raised concerns. Given recent security incidents and data breaches, we must act promptly. The following assaults are described, along with possible countermeasures and execution methods:

Xml Signature Wrapping Attack /

XML Signature protects against XML Rewriting Attacks by verifying the authenticity, integrity, and confidentiality of SOAP interactions. Web Service Security (WS-Security) safeguards SOAP messages with XML Signatures and Encryption. The SOAP message body is this.

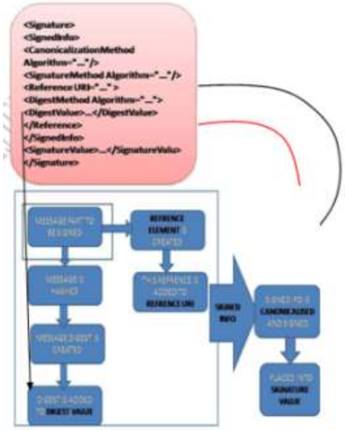

<Signature>
<SignedInfo>
<CanonicalizationMethod Algorithm="..."/>
<SignatureMethod Algorithm="..."/>
<Reference URI="..." >
<DigestMethod Algorithm="...">
<DigestValue>...</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>...</SignatureValue>
</Signature>
REFERENCE ELEMENT IS CREATED
REFERENCE URI
SIGNED INFO
CANONICALISED AND SIGNED
SIGNATURE VALUE
DIGEST VALUE

Fig6. The SOAP XML Signature Header Process

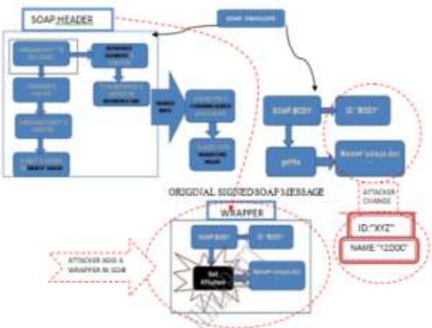


Fig 7 Changes to the Soap Envelope Before Sealing
How Wrapping Attack Is Done

The attacker should know the following before attacking:

- Hackers know the web service's endpoint.
- An attacker must check if a web service verifies security header signatures.

A web server generates a SOAP message in response to a client application, such as a browser. SOAP message translation at the Transport Layer Security (TLS) layer is attacked. The attacker injects malicious code at the start, moves the target components, and sends the modified SOAP message to the web server. Once the server verifies the signature, integrity is verified. Attackers may then run malicious code on the server. Figure 3.2 contextualizes the scenario.

Counterattack Defenses

- TLS must be secured when the SOAP preamble is exchanged in transit.
- To prevent tampering and signature validation failure, the header should include a checksum or redundant bit (STAMP bit).
- Building a good reputation earns the verification key.
- Example: X.509 certificate validation.
- To verify signed data with the key. Check references .

Malware Injection Attack /CrossCloud Injection

Malware, short for malicious software, is software that compromises a computer's availability, security, or privacy. Malware comprises viruses, worms, trojans, spyware, adware, crimeware, botnets, and scareware. Malware can disrupt network services, data breaches, theft, pop-ups, and other computer activities.

Infected cloud-injected content, usually via a web application, can infect a device.

Malware Injection Process [Advance Persistent Malware (Apt Malware)]- This attack is done by Dynamically created APTs exploit privilege escalation to compromise multiple cloud providers' data by acquiring administrator access and modifying cloud applications. Malware dissemination chain example:

Cloud providers develop malware by storing VM images in their proprietary image repository when customers connect to their services. Thus, the attacker first distributes a cloud-based picture. This picture has harmful script on any OS.

A malware seeder uploads a photo to a public cloud without authentication, which the attacker already owns.

An attacker launches malware on a web 2.0 application like a social network. Infected apps inject malware into a user's VPC.

Check download security before downloading.

- Malware analysis tools are recommended.
- Hide function names, global offset tables, and return addresses.
- JavaScript can be defeated via client-side encryption and user input verification.
- Recent photo hashes can be verified using cryptographic hashing.

Flodding Attacks [Dos/Ddos Attacks]

Flodding is a DDoS attack that redirects a lot of traffic to the target server. It may cause network disruptions, incomplete requests, server failures, and other difficulties.

How Flodding Attack Works- A cloud web server transfers instances to another server when they reach a certain threshold or capacity to maintain operation. An attacker must authenticate each packet, which requires server memory and processing power, to increase traffic. An attack begins with the penetration of several devices and the redirection of all network traffic to a single server. (Distributed Denial of Service Attack) terminates the server when its resources run out. ICMP and UDP packets are often used in flooding attacks.

Udp Flood Attack- The target machine receives many UDP packets over an intended or random port. It uses a lot of bandwidth.

Icmp Flood Attack- Malware reduces network throughput by pinging the system.

Extensible Markup Language (Xml) Based Denial Of Service (X-Dos)- Powerful parsing attacks require opening XML elements and use the entire CPU. Erroneous XML messages instead of packets flood the network, impeding data transfer.

Hypertext Transfer Protocol (Http) Based Denial Of Service (H-Dos)- Up to 1500 threads are launched by an HTTP flooder, flooding web servers with sporadic HTTP requests and jamming the channel. Recent intrusions compromised Iran's cloud-based security systems.

Flodding Tools

Agobot: The following C++ viruses can infect computers. These viruses can do more than uninstall embedded bots, keylogging, network sniffing, DDoS attacks, and remote updates.

Mstream: Zombies are malware deployed on compromised systems to initiate a network assault. The attacker launches attacks via telnet with the master controller system. Another hijacked system runs the Master Controller, which controls zombies. A system receives a deluge of TCP ACK packets from random IP addresses from stream.c. Every hostile ACK packet creates a RST and ICMP host/destination unreachable packet and degrades service on targeted systems and the network.

Trinoo: This collection of apps launches DDoS attacks. A typical system attack comprises 3 steps. In the beginning of an assault, the attacker lists target hosts. After programming these hosts into trinoo masters, he attacks.

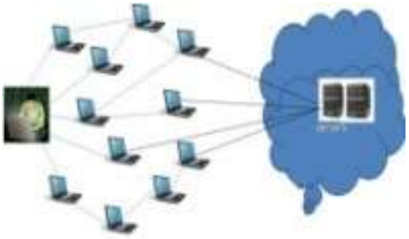


Fig 8 Denial of service after many assaults

Countermeasures Of Flodding Attack

- Load balancing mitigates attacks.
- Cyberattack prevention requires software upgrades and packet-filtering firewalls.
- Honeypots and honeynets are used. Covert honeypots simulate a compromised condition to acquire assault strategy and equipment information. Researchers called honeynets honeypots.
- DMM (DOS Mitigation Module) should safeguard firewalls and intrusion detection systems.

Other Security Attacks And Issues

Due to rapid technological improvement and changing attack types. New approaches for adversaries to exploit breakthrough technologies are continually developed. Despite the rise in threats, cloud security has significant flaws. Some examples are:

Interfering with two parties' secret is the man in the middle role. Place a virtual computer with malicious code near the target cloud server to gain information through timing data, electromagnetic leakage, and other side channels.

Browser Security: Adversaries exploit many browser weaknesses. The main attacks against these vulnerabilities are JavaScript and cross-site scripting. Use a modern scriptable browser.

Corruption, data theft, and disclosure can hurt the economy and competitiveness. Trojans and keyloggers can sneak into a target's computer and steal confidential data.

Cloud Tracebacking

Web services (WS) security is provided by inserting a security header to SOAP, although spoofing makes it useless against DDOS. Service Oriented Traceback Architecture (SOTA) helps find an intrusion source. DPM, a packet marketing technique that reserves the IP field and indication in the IP header, underpins SOTA. Packets entering and leaving the edge are marked and discarded. The SOTM replaces the client authentication token header in the SOAP header. It remains unchanged during network transmission. The target of a DDOS assault can trace its origin and take preventive measures.

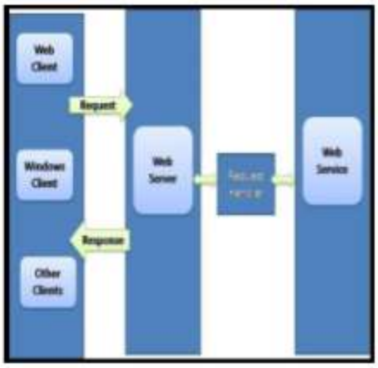


Fig 9 No SOTA Notation in Web Service Architecture

4. PRIVACY ISSUES IN CLOUD

Controlling personal data is essential for privacy.

Privacy comprises the right to decide when, how, and how much personal information is shared with third parties.

Alan Westin, Privacy and Freedom, 1967

Privacy is a vital human right.

Movius and Krup ,2009

- Privacy terms include limited
- self-access,
- personhood,
- intimacy, secrecy, and
- contextual integrity.

Numerous privacy standards apply to one's person, communications, physical location (including residence), and information. Cloud computing services are outsourced, thus users who save their data and apps on centralized servers risk data theft for corporate competitiveness and personal benefit. Email addresses, account balances, corporate asset values, etc. It can therefore provide exceptional service.

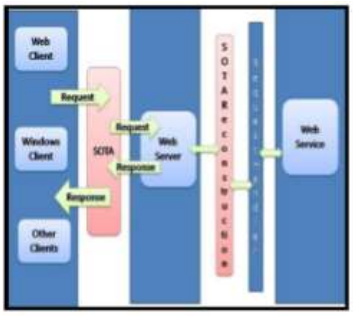


Fig 10 SOTA for Web Service Architecture

Risky for users. According to Pew Internet and American Life Project statistics, people fear their data will be shared without their consent. This is shown below.

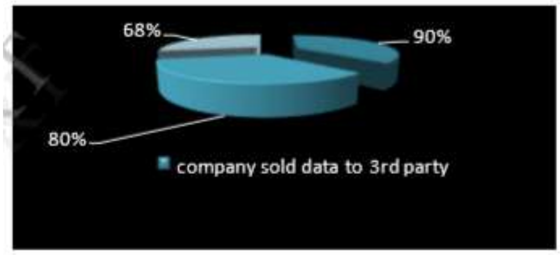


Fig 11 The Pew Internet & American Life Project found rising privacy concerns.

The user should review the cloud service provider's privacy and terms of service. He should know any restrictions and security measures before providing his information. Data placement is crucial since it must meet local regulations.

Countermeasures- Due to widespread worry that data privacy will increasingly threaten national security, immediate action is needed.

Need Of Strong Governance- Implementing powerful governance will streamline the deployed service's policies, procedures, design, and implementation. Exploiting vulnerable systems may leave legal repercussions undetected, putting personal data at risk.

Data Location- Internal data storage is safer than external transmission. Legal and regulatory differences between countries might make transnational data transfer difficult. A critical data breach might threaten national security. Therefore, data transfer must be permitted by the destination country's rules.

Privacy Laws

Privacy laws vary widely worldwide. Sector-specific protections are common in the US; the FCC governs telecommunications. All EU member states must pass laws that fully protect privacy as a human right under the European Data Protection Directive. Many nations have privacy commissioners and state and national privacy commissions.

HIPAA (Health Insurance Portability and Accountability Act, 1996)- Amendments to US law

COPPA (Children's Online Privacy Protection Act, 1998)- Websites that target children under 13 must ask their parents' permission before collecting personal data.

GLB (Gramm-Leach-Bliley-Act, 1999)- Financial institution clients should know about and opt out of privacy policies.

Safe harbor(Approved July 26, 2000 by EU)- Signatories must disclose the data collected, describe its purposes and recipients, and offer opt-in or opt-out of third-party transfers.

FTC(Fair Information Practise Principles,1998)- The US, Canada, and Europe apply these personal data protection standards.

- The five FIP principles are security,
- accountability,
- openness,
- and integrity.
- Making amends

Fair Credit Reporting Act(FCRA)- Credit reporting agencies collect American customer data. This law enforces all FIP principles.

USA – Patriot Act(2001)- Congress authorized US intelligence services to gather information on suspected terrorist actions in September 2001. Foreign clients of US cloud service providers worry that this rule will provide the US government access to their private data.

The USA Patriot Act has threatened global cloud computing privacy norms at academic and research institutions, according to a University of Amsterdam analysis. Research indicates that the US government can intercept data leaving Europe, despite tight privacy restrictions. Privacy policymakers in several European countries are concerned.

EU Directive 95/46/EC(1995) - According to Birnhock (2008), this is the Data Protection Directive. This regulation aimed to standardize EU data protection laws. It includes personal data and PII.

Payment Card Industry- Data Security Standard(PCI- DSS Sensitive client data must be encrypted per industry standard. It includes regulating building access and controlling admittance based on interpersonal connections.

Adoption Of Privacy Enhancing Technologies

Protection of anonymity requires privacy-enhancing technologies. The following methods could achieve this goal: Internet anonymizers like P3P privacy policy languages and Tor XACML

Legal Implications Between Cloud Provider And User

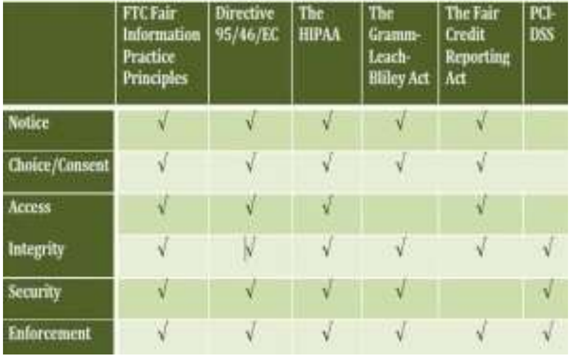
In case of conflict, the supplier and user must have a detailed agreement. Subcontractors' legal infractions may force organisations to respond . Contract questions may include:

Service Level Agreements

- Cloud services protect web platform data loss due to their reliability.
- Accountability for third-party security breaches

General contractual matters

- The legal risks of a cloud service provider acquisition or merger, treaty violations, and captive data management.
- Data Privacy Law regulations.



	FTC Fair Information Practice Principles	Directive 95/46/EC	The HIPAA	The Gramm-Leach-Bliley Act	The Fair Credit Reporting Act	PCI-DSS
Notice	√	√	√	√	√	
Choice/Consent	√	√	√	√	√	
Access	√	√	√		√	
Integrity	√	√	√	√	√	√
Security	√	√	√	√		√
Enforcement	√	√	√	√	√	√

Fig 12 Common Principles In Privacy Regulation

Vertical axis of Figure 1. There are many privacy regulations and rules on the horizontal axis and common privacy concepts on the vertical.

5. TRUST ISSUES IN CLOUD

Trust-The origin of trust came from the nature and behaviour of human societies.We can say that trust is an amalgation of mental and emotional attitude. So trust is a subjective notion based on opinion andvalues of an individual.

Thus trust in cloud plays a very vital role because user is accesing and giving information as he is having trust in the service providers of cloud. Thus, lot of factors came into existence in users mind because of which he lacks confidence in cloud.

Trust Management

The cloud's main purpose is to supply SaaS services, but if users' concerns aren't addressed, it fails. Developing trust between clients and service providers requires extensive trust management.

- Both development and post-release require tremendous prudence.
- Promote client safety.
- The user must trust that trustworthy firms make his software and hardware.
- The customer must trust the data provider.
- Thus, end-user trust is essential for IT industry alignment with the economy, society, and government. Therefore, socio-mechanisms must be introduced to strengthen values.

Security-How can I trust my data will be secure?,
Reliability-Can I truly rely on them? What if my data goes?
Performance-Will it be able to perform my service?
Availability???
Scalability???
Interoperability?

Fig 13 Cloud trust concerns

Trusted Zones

Trustworthy zones should be included in virtual network architectures. Virtualize and categorize applications by users, hardware, software, and services. Thus, cyber intelligence and rigorous verification can beat fraudsters in trusted regions. Policies managing the three trust levels remain.

Provisioning policies and trusted zones are applied to VMs to achieve this.

Cloud data management and breach protection provider.

Identification controls departure and restricted area access.

Trusted Zones Key Capabilities

Fig 14 RSA-secured areas

Identity Management

It simplifies system user permission monitoring. It verifies identity and authorizes every action more reliably.

- Technology solutions like identity management platforms are one alternative.
- Regulations on data privacy Law enforcement identity theft
- Internal privilege segregation (security and social)

All of the above improve constraint-free computation. The graphic below shows trust management control as indistinct lines and data and services as solid lines.

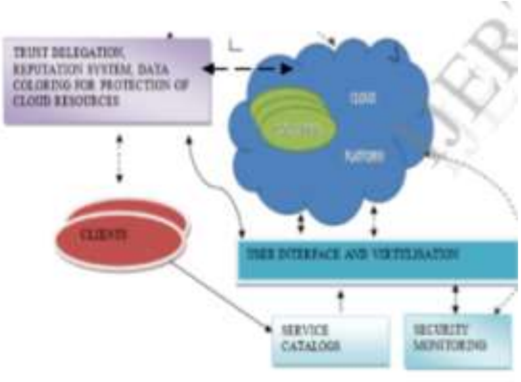

TRUST DELEGATION, REPUTATION SYSTEM, DATA COLORING FOR PROTECTION OF CLOUD RESOURCES
CLIENTS
USER INTERFACE AND VIRTUALISATION
SERVICE CATALOGS
SECURITY MONITORING

Fig 15 The Virtue Model

6. ACCOUNTABILITY ISSUES

Accountability might mean responsibility, management, execution, or anything else in a leadership situation. Reporting and auditing are linked in computer science. Data protection methods that comply with regulations are being developed. The Galway Project defines accountability as protecting and using personally identifiable information ethically. It also involves accepting responsibility for incorrect information use.

So accountability is done to –

- Accountability is to resolve concerns,
- penalize inappropriate behavior, develop confidence,
- Encourage openness, and reward right behavior.
- Deal with Faults.

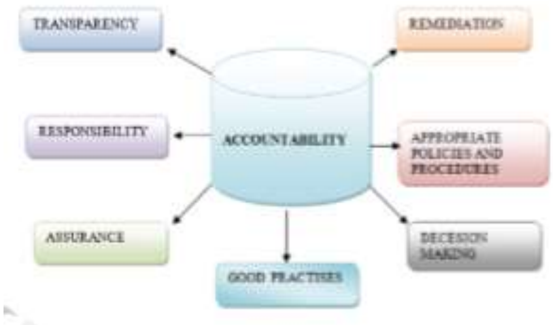


Fig16 Key elements of accountability

OECD

The council promoted accountability. Figure 6 illustrates cloud accountability issues. If Bob, the service recipient, and Alice, the provider, both experience a software bug, how would they decide liability?

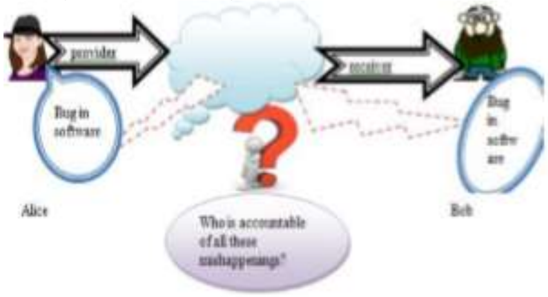


Fig17 Case-study accountability investigation

In this situation, the cloud must precisely identify the mistake cause. The participating parties can identify problems, compare notes, and take necessary disciplinary action using the cloud's tamper-evident log of all activity. Thus, service providers might attract customers and solve difficulties. Accountable Virtual Machines (AVM) are needed.

To comply with laws and standards, an organization should select someone to supervise privacy policies and processes. The system should be audited regularly to verify compliance. Be attentive in all issues because regional regulations vary. The OECD Council has established an accountable implementation framework for data security and privacy. HIPAA has given hospitals and other healthcare organizations many precautions. Therefore, cloud service providers must follow these security and privacy regulations.

7.CONCLUSION

Cloud services have many benefits, but the problems expressed suggest they may not be secure. Consumers should understand the cloud's legal framework and terms of service before migrating. Both the service provider and the consumer should be cautious because assaults can happen anywhere and anytime. Constant sky monitoring will keep clouds from fading.

REFERENCES

1. A history of cloud computing. http://www.computerweekly.com/feature/A-history-of-cloud-computing.
2. Into the cloud out of the fog. Ernst & Young’s 2011 Global Information Security Survey. http://www.ey.com/Publication/vwLUAssets/Into_the_c l oud_out_of_the_fog2011_GISS/$File/Into_the_cloud_o u t_of_the_fog-2011%20GISS.pdf
3. Cloud Computing Security- Wikipedia. http://en.wikipedia.org/wiki/Cloud_computing_security
4. Trend Micro- Canadian IT SME Survey 2011. http://ca.trendmicro.com/imperia/md/content/ca/environics_-_trend_micro_it_security_-_final_report_-_jul_18-2011.pdf
5. Troubles in Clouds. http://www.experian.com/blogs/data-breach/2011/07/19/trouble-in-the-clouds-data-breaches-threaten-cloud-computing/
6. http://www.idc.com/prodserv/idc_cloud.jsp.
7. Epsilon breach http://www.infosecisland.com/blogview/12814-Epsilon-Breach-Deals-Another-Blow-to-Cloud-Security.html
8. Epsilon breach .http://www.insideprivacy.com/data-security/data-breaches/epsilon-data-breach-highlights-security-challenges-in-the-cloud
9. Epsilon breach .http://bizcloudnetwork.com/epsilon-and-amazon-cloud-security-issues-not-adequately-addressed
10. Citigroup acknowledges Breach http://searchsecurity.techtarget.com/news/2240036729/Citigroup-acknowledges-data-security-breach