Journal of Physics: Conference Series

PURPOSE-LED PUBLISHING™

PAPER • **OPEN ACCESS**

A study of the cloud security attacks and threats

To cite this article: V Sureshkumar and B Baranidharan 2021 *J. Phys.: Conf. Ser.* **1964** 042061

View the article online for updates and enhancements.

A study of the cloud security attacks and threats

V Sureshkumar[1] and B Baranidharan[2*]
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur 603 203, Kanchipuram, Chennai, Tamilnadu, India.
E-mail: *jrp557791@gmail.com

Abstract. Cloud storage has become an essential computational model today, providing flexible, defective resistant resources and dramatically reducing costs. However, there are major obstacles to protection issues in the wider adoption market. The multiformity of the cloud and the multi-location storing of data exacerbate these problems. The major issues to be discussed in protection are secrecy, authenticity, honesty, availability and auditability. Enabling more customers to switch to the cloud environment would allow for safe data and transfers from the service provider. Intrusion Detection Mechanisms, Cryptographic Methodology and Electronic Forensic Software are some of the assurance that a trustful service provider will have for the recuperation and collection of digital proof of intrusion activities. This paper provides a survey into some of the prevalent challenges, risks and ways to resolve these challenges in cloud platforms. We also discussed major cloud storage service for data storage and protection model.

1. Introduction:

Gartner listed online cloud service as one of the top ten strategic innovations for 2012 with the ability to have a huge effect on businesses over the next few years (Gartner, 2011). Softwares installed on the cloud environment have the potential to extends and fall, demonstrated by the abundance of unlimited computational capacity. This strategy provides consistency when allocating resources, enabling cloud clients to pay for resources only, thereby avoiding expense associated with supply and downtime. The pay-as-you-go concept is lucrative for organisations not wanting to care over holding the hardware or hiring operating employees. The current Everything-as-a-service market model follows the notion that the cloud delivers applicational, storage and processing power digitally [1-5].

As a service, network, applications and technology are well-known machine paradigms. Platform as a service (PaaS) offers a stage for the creation of web apps and utilities and the ecosystem. Software as a Service (SaaS) is a service that removes requirement for organisations to deploy and maintain apps. Users provide on-demand connexions to virtual computers in the Technology as a service cloud. The customer sees just an operating device in a barebone computer. The consumer will install and set up applications on this computer entirely in a modular manner. Database-as-a-service (DaaS) is the same term. In recent times, there are more transition in storage service from in-house to cloud hosting.

On-demand access to data base functionality such as data description, replication and retrieval is accessible at Cloud Database-as-a-service (Chaitanya, 2020). It also offers computer connectivity and storage facilities and encourages end customers to neglect the position and setup of the facilities distribution system. More and more businesses joining the cloud computing service need to take serious care of the safety effects of motions or networks in the cloud. The protection approach implemented by Cloud vendors will support small and medium-sized companies who usually struggle to commit capital to resolve security concerns. The privacy issues of both data owner and end consumer must be resolved in order for the cloud to be well received by businesses. Going into the cloud brings threats and opportunities to light. The unified data model although the clouds makes it simple to track data access, it also puts at risk accurate data leakage (Balding, 2008) (see. [6-11]).

Moreover, businesses must focus on the software and data from a third-party provider. This lack of data access usually held in-house poses several new problems in protection management. Furthermore, resource sharing allows the idea of limitless cloud services. This multi-component cloud of resource sharing raises many issues regarding privacy as conventional networking firewalls and protected socket layers are not a cloud protection shield. Data from a corporation was usually placed in the cloud on a virtual computer which possibly runs on another system that may theoretically be harmful to other virtual machines. Cloud data is often accessible through the internet, ensuring only a certain degree of protection.

2. Related work

Cloud-related protection challenges and risks became the primary subject of several reports. A few common cloud threats are introduced by Vaquero et al (2011) and correlated with the numerous layers of IaaS framework: the network domain, the system domain and the physical domain. A survey on security problems in various cloud-based services model was proposed by Subashini et al.(2011): SaaS, PaaS, and IaaS. They describe the protection of the SaaS model as data privacy, data confidentiality, availability of data and networking protection. An example of the protection challenges posed by the PaaS model are attacks on identifiable such as a program executing in user context. Examples of IaaS concept problems are security flaws in the virtualization manager (see. [12-17]).

Minqi et al. (2010) have problems linked to multi-data positioning. In order to maximise accessible data, various global cloud vendors such as Amazon and Google are replicated throughout geographical regions worldwide [18-27]. This is also worse because consumer data's privacy legislation is still based on the position of the data. The authors also analyse several protection acts which have been established to safeguard the privacy of users but have little justification as applicable to the online cloud storage service. Tsai et al. (2012) address security risks as one of the bases of cloud infrastructure from the viewpoint of virtualization technology. Virtualization effects on three different service models are explored by author. Somani et al. (2010) address concerns relating to protection related to the handling of extremely confidential cloud data. When it comes to medical data processing, statutory commitments of a service provider are not sufficient. The paper highlights the usage of data forensics software to better detect cloud problems [28-39].

3. Security threats

The Data Violation Inquiries Study (DBIR) of Verizon 2011 describes types of security risks to which organisations are exposed (Verizon Company, 2011). The study reveals that foreign agents (92 percent) face the greatest security risks. Outside agents involve hackers, organised gangs, and environmental hazards considerations like flood. Insider attacks make upto nearly 18% of data infringements. Company associate infringements make up less than 1% (Verizon Company, 2011). Market associates comprise providers, suppliers, outsourced resources and other external parties interested in the company's business partnership. The DBIR often includes the most prevalent forms of safety violations. The lead are hacking (50%) and malware (49%). In the last couple of years, physical assaults (14%) have doubled. Privileges of violence (17%) such as embezzlement and theft and social strategies (11%), such as solicitations and coercion, fill the two bases for security violations of this nature. Although the aforementioned percentages were not directly applied to the protection risks in the cloud, the study does not monitor the data and properties of an organisation. In comparison to the shared on-demand character of the cloud, this lack of openness not only poses new problems but also amplifies some current concerns. In this segment we speak about some of the cloud protection issues.

3.1 Data confidentiality

Confidentiality of data is about limiting unwanted access to data by consumers. As company data is now processed in the cloud, issues such as, "Is my data protected and who else will access it?"To ensure confidentiality on behalf of clients, the cloud provider should be fully assured. Clients may know the safeguards on their data through the cloud provider.

The health and financial sectors need stringent promises to secure their data against unauthorised entry. Any security infringements may result in sanctions arising from the leak of classified information which may damage the credibility of the organisation. IaaS providers also promote the opportunity to register and continue automatically to utilise cloud resources (Matheus et al., 2019). There are several services of free trial times (Cloud Encryption Partnership, 2012). Attackers can attack online storage providers because secured registration norms enable hackers to stay anonymous and prevent detection. The templates for Iaas and Paas are impacted by such assaults. Access management and privacy capabilities are critical costs in the cloud for data security.

3.2 Insecure interfaces

A collection of interfaces or APIs, handling, orchestrating and tracking the whole user operation, are used to interact cloud users with the cloud provider (Cloud Protection Alliance, 2012). This APIs function as the cloud provider portal. Securing this platform has an immense influence on cloud providers' total security. Unauthorized entry to such gates could jeopardise the security of apps.

3.3 Malicious insiders

It pose a danger to every work. In the cloud world, though, this threat is expanded, since the client cannot monitor personnel procurement procedures. The client is unable, until employing workers particularly those who use his data centres, to monitor the cloud provider infrastructure. To prevent security violations that arise from internal personnel, stringent inspections, tracking and recording of all data accesses are necessary.

3.4 Shared technology issues

Resource sharing in cloud computing achieves scalability. Isolation of tenants is virtual; the hardware and services of the computer are exchanged. In the absence of a clear separation of the basic components of the system, this exchange of resources introduces the ability to allow a tenant to examine the data of another tenant. The form of hardware used in a cloud environment could pose a potential danger. Usually, cloud infrastructure use multi-core and multi-processor. Knowledge may flow between nuclei in such settings. Along with that, the temporary data is usually stored in multi-core processors, which render it easier for a consumer to monitor the machine's memory to retain information in the cache.

Virtualization is one of the cloud's main features. It raises safety hazards, though. Virtualization enables several isolated virtual machines identified as guests to operate on one host simultaneously. The hypervisor, which is also known as the Virtual Machine Monitor, can maintain perfect separation between its visitors (B. Asvija et al., 2017). A virtualized guest setting must not compete with another and must not compete with the host environment either. Virtualization environment including VM escape attacks or VM jumping is sensitive (Owens, 2008). The guest operating system and other virtual machine executing on this system can then be accessed to the intruder once successful. The hypervisor misuse may have drastic repercussions since the hypervisor is privileged. The virtual hopping machine enables one virtual machine to reach another that violates the anonymity, functionality and dignity of the victim.

3.5 Service-Level Agreement (SLA)

An arrangement for cloud service enables the consumer to discuss service levels with a cloud supplier. It explains how programmes can be provided. Typical SLAs provide a service data exchange rate, estimated repair time (MTTR) or jitter attributes, or equivalent, which are observable. Cloud consumers should apply protection to their SLA contracts, so how does protection and secrecy measure? Security and privacy are sadly non-quantitative criteria, which preclude consumers from reaching SLAs. Some testing at the end of the service provider can be achieved so how do we maintain consistency in the measures given by the service provider?

3.6 Denial of service attacks

This attacks focus on distributed application denial attacks target cloud computing vulnerabilities. The cloud provider needs to be well prepared in order for high latency threats and DoS programmes to be detected and acted rapidly (Hedjaz Sabrine., 2019). Cloud services should provide a comprehensive architecture to detect and defend them from DDoS assaults. DDoS prevention methods may at least be in operation, such as connexion restrictions. DoS attacks directed at a shared infrastructure will cause an intruder to use all the physical resources accessible to a computer. The hypervisor is not able to satisfy the resource demand of other VMs (Tsai et al., 2012). According to restrict resources distribution, the hypervisor should be installed. A cloud client profits by ensuring that the SLAs explicitly specify the cloud provider's obligations.

3.7 Availability

Data accessible addresses the avoidance of malware threats, which can prohibit users from accessing those sections or the whole programme. Not only applications and data are accessible but also hardware required. It also includes apps. Given the cloud share of the networks, a small breakthrough may contribute to a cloud outpost that also affects those companies which did not originate the issue or were primary victims (PC Consultancy, 2011). For eg, in 2011 a network breakdown in one of its accessible areas caused Amazon EC2 to fail (Thibodeau, 2011). This outage has plagued many prominent websites such as Netflix and Reddit. In order to stop such blackouts, Cloud systems should be appropriately planned and managed. The concept of negotiating the SLAs and contingency arrangements in the case of a cloud malfunction with the cloud provider is still a smart idea.

3.8 Compliance

It is not trivial to ensure that the cloud provider complies with the rules and conformity criteria defined by specifications such as HIPAA and Sarbanes-Oxley. HIPAA's provisions involve maintaining the protection of personal details in the field of patient health information. Both medical reports must be accurately recorded and tracked. The Payment Card Industry Data Protection Norm (PCI DSS) also accepted by cloud providers as well. In order to ensure cardholder identity security, PCI DSS defines enforcement requirements. Furthermore, the data breach investigation report (DBIR) for 2011 (Verizon Company, 2011), reported in the Verizon 2011, did not follow PCI DSS for 89 percent of victims who experienced a payment card breach.

3.9 Authenticity

For the control of users and organisations, several businesses use the Lightweight Directory Access Protocol. Subashini&Kavitha, 2011: Active Directory is an effective and well recognised method for handling users in SMEs (SMB). Active Directory offers a basic authentication and protection layer, enabling user unified control. If the cloud host functionality allows it impossible to handle user development and deletion as workers go, businesses are losing charge over user accounts management. There is also not well established the protocol for expanding current access management frameworks in an organisation into the cloud.

3.10 Auditability

Both consumer instance accesses in the cloud should be recorded and routinely audited. In eight out of ten cases, malware is commonly used for the intent of assaulting confidential information (Verizon Corporation, 2011). To identify this data breach, it is crucial that the correct indicators are in position. In case of a security violation, trace data should be accessible that will show foul play. A further challenge in the cloud is that cloud users would also have faith in the calculations provided by the cloud provider. The big problem is the data violation inquiry initiative will be delayed if the audit logs needed are not given on time. According to Service level agreements, in case of immediate problems the cloud provider can react immediately. Cloud vendors may deem applications or facilities to be urgent, but a violation of protection may not have the same benefits. An infringement of protection could fall into the category of medium priority. Organizations must also recognise thoroughly guidelines for audit data access in the case of a crisis.

3.11 Data integrity

The confidentiality of data is associated with the prevention of unwanted data adjustments. By offering security, the service provider may advertise data integrity. Encryption can entail quality performance, mainly for DaaS database. With DaaS the penalty can differ if a tuple, link, or whole database was encrypted. Furthermore, the coding programme versus the coding algorithm of the hardware level may have a major output effect. The encryption feature is given by the database in software level encryption. However, the consumer offers the encryption key. This prohibits unauthorised staff, while accessing disc archives, from decrypting valuable details. Encryption is performed on the field level, or on the row level, using Hazigumus, Iyer, & Mehrotra 2002, encryption of the hardware level. Another concern is size of datathat increases fields with the cryptographic techniquefor data encryption with this form of thin-grained encryption. For instance, a keyed 64-bit symmetrical block cypher, Blowfish encrypts and decrypts 64-bit pieces of information. If the field data size is 8 bytes to 64 bytes after Blowfish encryption.

The forfeitfor interaction of cloud frequently asked questions should be regarded with the encryption in the image. The replying time forfeitarises because of two reasons: hardware invocation costs and the execution costs of cryptographic algorithm (Hacigumus et al., 2002). The key management framework needed for data encryption and decryption cannot be stored in the cloud as a further issue with encrypting. This knowledge must be retained by the client. The key management are responsible for the limited base of knowledge for complicated encryption systems, which is not intended to transfer the original database to the cloud.

4. Risk assessment

Modeling threats may help classify the safety hazards an application is prone to, along with the severity of the hazard effect. Unique prevention techniques may be established with this study. The safety danger may be calculated by the likelihood and effect of a hazard. The danger is large because both the likelihood and effect of the hazard are large (Saripalli&Walters, 2010). In order to determine whether or not to step into the cloud operational risk management is necessary. The risk level often differs considerably with the form of cloud infrastructure. Risks are classified into three separate groups by the European Network and Information Protection Service (ENISA, 2009).

4.1 Policy and organizational risks

Generally, no standardisation is offered by the various cloud vendors for service interfaces or data formats. This apparent absence of standards renders it incredibly challenging to switch from house data formats to the format of a cloud service. It also allows porting customers from one cloud service organization to a new one challenging. If possible. Cloud protocols for connectivity remain rather proprietary and are cloud-specific (Littlejohn, 2012). It is necessary to know whether cloud services use standard protocols, as it must be feasible to accept these communication protocols in a layer that defines how multiple structures used by the enterprise communicate. The cloud provider's dependence creates a significant danger whether the provider exits the organisation or when the cloud provider acquires non-binding agreements. There is a strong possibility that there is a shortage of standard technology. It has a medium influence on the company (ENISA, 2009). The lack of contract accountability is another illustration of operational risk. Any of the functionality can be outsourced from a cloud vendor to a third-party supplier. The degree of protection will now rely on the third-party vendor's level of security. Any vulnerabilities in the third-party supplier services may have a detrimental influence on data privacy, security and usability. Unless the cloud vendor holds the client aware of the outsourcing elements of the operation, it will not be feasible for the client to determine the potential cost of going into the cloud.

4.2 Technical risks

Providers commonly utilise dynamic provisioning to project the illusion of infinite services in the cloud, where services such as processing power and storage are exchanged by different users. This design is vulnerable to attacks like Virtual Machine. The attacks depend on the cloud structure: private clouds are poor, whereas public clouds are medium. The effect is strong as it will influence anonymity, credibility and availability of services. Such high effect risks include amalgamation of insiders, data interception possibilities for the delivery and remote access denial. The risk of such risks is moderate (ENISA, 2009). In addition, the multi-rent environment allows cloud vendors to be unreliable and dictates how protection checks are applied, since consumer to consumer security standards differ.

4.3 Legal risks

When data is processed in the cloud in many countries, it must conform with municipal regulations. States and countries not compliant with multinational arrangements risk the security of classified details. The cloud world allows it impossible for consumers to guarantee that their data are actually stored in a way that satisfies these criteria. These clients have to guarantee that they have qualification summaries on how they manage and process data in their cloud provider. One such example (ENISA, 2009) is the qualification of SAS70. Another legal liability includes not disclosing all protection violations by the cloud vendor. The possibility and effect of these risks also raises the overall risk.

5. Risk mitigation and prevention

Suitable protection tests will minimise danger and decrease the chance of attacks. For an enterprise, it is important to consider the danger of going through the cloud and then provide a mitigating plan for any risk found. One crucial factor to bear in mind is that hazard countermeasure will not be cost-effective. There is no means of minimising the danger involved with this hazard. The ever-changing existence of the cloud can contribute to a risk evaluation on a regular basis. New cloud technology can generate new faults. In addition, novel countermeasures may arise to reduce risks not previously discussed (Judith, 2011).

5.1 Intrusion detection

Intruders may obtain information for investigative instruments and procedures that lies as digital proof that helpsmany court investigations (Ahmed & Raja, 2010). Data review of permanent resources in the system log files,Volatile data resources operate throughout the activity of the device.Systems for the identification of attack trends can be used for intrusion detection (IDSs). The implementation of such a deviceCloud users are certain to be confident that the technology of the provider is stable. IDSs will increase protectionUser behaviour, network traffic, request records and connexion records investigative steps. IDS is a move aheadDetects and blocks threats proactively, rather than handling the effects of an incident.Hostage-based and network-based IDSs may be categorised. Capture Network IDSs Network FlowPackages going through them and testing those trends for intrusion detection. Analyze host IDSsLogs, device calls and other host processes (Dhage et al., 2011). It is also possible to verify that operation is only possible through administrative access. Intrusions can be observed by two separate audit techniques: know-how dependent and behaviour-based (C. B. Westphall, Vieira, Schulter, & C. M. Westphall, 2010). From the experience of prior assaults, the knowledge-based approach detects infiltration. It searches for a set of acts that can contribute to an assault. The behavioural approach contrasts the behaviours of consumers with planned actions to find any flaws. Knowledge technology is more popular since it has a low false alarm rate. However, unexplained attack behaviours may only be observed and recorded by behavior-based programmes. The best approach will be to use IDS to catch a wide range of attacks utilising all these methods effectively. An IDS implemented in the cloud vary from the standard business version since internal threats from the cloud itself have to be taken into consideration. Every IDS installed on a node on a cloud-based IDS tracks events for security breaches and warns other nodes to a breach.

5.2 Data center security

Trusted Platform Module (TPM), in particular in IaaS, may be used to protect platforms (Vaquero et al., 2011). It is a secure crypto processor specification. The protection chip is a sophisticated, software-enhanced microcontroller (Parno, 2007). Thisis used to produce encryption keys and covered storage capability where sensitive informationis connected with the platform. It offers remote evidence capabilities to detect the unmodified copy of such programme on the computer. Multiple devices have not been configured to access TPM. IBM built a virtual TPM to address this constraint. Digital TPM can improve the protection of the virtualisation stack at all stages (Vaquero et al., 2011). It helps cloud services to incorporate many authentication levels. The protection of TPM may be built into federated ID management principles. In addition, data in memory and on discs can be secured by encryption. The usage of the cloud provider's TPM allowed elements ensures that the software truly operates on trustworthy resources.

5.3 Authentication and identity management

Multiple service companies are increasingly included in diverse areas of the application. This can contribute to a future nightmare in identity management unless organised between all providers. To enable user authentication and authorization knowledge exchange, the use of Federated IDM solutions is important. Standard protocols should be used to ensure interoperability among communication parties. Assertion of protection.

The XML Open Standard for Markup Language (SAML) enables to log in and share authentication, authorisation details between separate domains and multiple web pages (Zissis&Lekkas, 2012). Confederated such as user-centric IDM are strong option for cloud application. User-centered IDM utilises user identity characteristics. The IDM solution chosen could combine an established IDM solution with companies (Hassan et al., 2010). Be sure the cloud service provides good access restrictions and that the protection practises of the service do not affect what already happens at home. Authentication by token or key may be used to allow protected entry. The solid authentication front is the digital signatures used with Single Sign On and LDAP (Zissis&Lekkas, 2012).

5.4 Shared resources

Data protection may reduce the possibility of knowledge leakage until storage in the cloud. For this reason typical algorithms for symmetric and asymmetric encryption may be used. It is therefore important to encrypt cache and memory data in cloud environments to allow for adjacent node sniffing attacks.The absence of separation between tenants may be abused by malicious parties in the cloud world. In this scenario, the attack 's effectiveness relies on the attacker's willingness to assess another scenario as his co-resident (Ristenpart, Tromer, Shacham, & Savage, 2009). Inhibiting controls for co-residence will deter many attacks like VM Escape and VM Hopping.

The assaults on the hypervisor are another challenge to the network setting. These attacks will jeopardise tenant data security. The assumption that the computer is a virtual machine must be concealed one direction to secure the hyperviewer (Vaqueero et al. 2011).

5.5 Regulatory compliance

Conformity criteria consumers must guarantee that the architecture of the cloud provider complies with these criteria. For example, companies that may comply with HIPAA rules should enable the cloud vendor to support online auditing features that have robust audit ability. A clear interpretation of the liability connected with going into the cloud is the contrast of legislative expectations with the regulatory responsibilities of providers. External evaluations and protection clearance should be available from the cloud vendor (Carroll, van der Merwe, & Kotze, 2011).

5.6 Location

Both potential data positions should be known by customers. Select a service provider who will ensure that data are only processed at the contract-identified geographical locations (Anchises, 2009). Stop utilising internet companies in aggressive countries of data centres. Providers should be willing to show that they conform with policy and legislation, including state regulation.

5.7 Availability

Some weak points may be established through a clear knowledge of service provider networks. Well-managed processes may reduce cloud service operating risk. Data back-up processes and replication practises of the cloud service should be reasonably robust to avoid data failure or degradation. Service level agreements are important for ensuring uptime and operating arrangements in the event of a breakdown. In case of a cloud vendor quitting an organisation or if an operator's service contract expires, the availability of service may be jeopardised. This hazard is counteracted by an assessment of the interoperability requirements of the supplier. The retrieval of data and the duplication of data should be checked to guarantee there there is no nightmare when migrating to another supplier.

5.8 Confidentiality

The compliance unit of the cloud provider should be capable of identifying breaches and countering them promptly. Moreover, consumers can track the notification phase for the cloud services. Clients should guarantee that the compliance reviews of the supplier are adequately clear and the degree of accountability in service level agreements should be reported. Periodic checks by outside parties can be done to check that the protocols and practises according to established requirements are implemented.

Traditional cryptographic algorithms may be used to encrypt data in transmission. Cloud vendors should be able to certify that the security mechanisms were checked by experienced experts. Industry requirements can be followed through main executives. Adequate recovery solutions can minimise main failure or damage. Only approved employees should have keys to key stores (Carroll, van der Merwe, & Kotze, 2011). Furthermore, all facilities and data usage in the case of an audit should be recorded and reproducible.

6. Security practices

In this segment, we discuss some of the key cloud providers' security standards and policies.

6.1 Amazon

Amazon Web Services (AWS), an array of web services integrated on cloud network. Host based firewalls and host-based intrusion detection systems are the main layer of intrusion detection system. A comprehensive background review is carried out by staff with potential access to consumer records. In case of re-approval of access not received, the privileges of access will be checked after 90 days and withdrawn. AWS holds an information about the supply of resources in real time (Amazon Web Resources, 2012). Users may add service via RSS feed and obtain notice of service outputs. AWS helps customers in various regional regions to position instances and to duplicate results (French edition, 2013).

AWS allows consumers to choose the regional area in order to satisfy the location-dependent enforcement criteria. No third party provider resources are outsourced to AWS. To fix network safety concerns, AWS uses SSL-protected endpoints. The hypervisor would only be hurt to send traffic to a virtual instance in order to avoid packet sniffing of attacks by neighbouring occupants. Amazon EC2 uses a tailor-made Xen hypervisor variant, which is tested on a daily basis for new vulnerabilities (Amazon 2012). In order to secure the virtual servers AWS encourages customers to incorporate more protection layers.

6.2 Google

Google Apps is a web-based application of Google-based SaaS software. It utilizes a file system that is distributed to store records. Replication is used to spread data through several networks in order to eliminate single failure points. For unusual activity, Google analyses the internal flow. It also tracks device records for unforeseen operations such as attempting to reach consumer details. Any manual access is regularly logged and reviewed. Google carries out history scrutines as new hires are recruited that involve, but not restricted to, criminal checks, debts, immigration and protection (Google, 2011). The nature of these background checks depends on the position of the work.

By showing an API consumers may use to embed into their home LDAP scheme, Google apps offer single sign-on support, enabling businesses to maintain power over the management of their selected authentication method. Google preserves the OS by utilising patented tools that tracks the Binary Alteration operating systems (Google, 2011). Some discrepancies between an OS and the Google standard of an operating system cause a self-curing procedure that returns the operating system immediately to some standard condition.

6.3 Salesforce

Salesforce provides Force.com, a website for the construction of enterprise software. Until workers are employed (Salesforce, 2012a) there is a comprehensive background review. As a method to restrict things including cut-out / paste and data duplication, safe workstations are used. Force.com scans all network packets with state-of-the-art packet inspection firewalls to protect its networks. In order to encrypt all network traffic, cryptographic protocols Transport Lager protection (TLS) and Stable Sockets Layer (SSL) are often used. Using intrusion detection devices, frequent external threats are observed. The device and data base tracking and generation of relevant notifications (Salesforce, 2012a) utilises event management software to connect user activities to data. Force.com operates a confidence website with RSS feed capability for in real time updates on device efficiency and security (Salesforce, 2012b).

In order to share authentication and authorisation information, Force.com facilitates federated identity management by utilising SAML. Force.com often helps a company to choose its own preferred form of Authentication, for example LDAP, in addition to providing IDM solutions. Network-based encryption is used for straight IP address from which users can access. Force.com rejects permission demands from anonymous emails.

6.4 IBM

IBM is an IaaS solution that provides easy access to virtual Server environments, SmartCloud Business. Tools can be offered by a self-service platform or application programming interfaces (APIs) in the SmartCloud Business setting (IBM, 2011). The endpoints are strictly shielded and all contact with the user using SSL is encrypted using HTTP. Intrusion detection and exploit scanning systems IBM provides monitoring software. The consumer will track and search its simulated world using these services. This is in line with the mutual liability concept of IBM, whereby consumers are liable for all facets of their virtual world security. Through preferring data centres where their services are accessible, consumers may limit their data to those regional areas (Rahul Ghosh et al., 2014).

7. Conclusions

The adoption of the cloud computing services nowadays is rather doubtful. The key contributing factors to these incertities are protection issues surrounding data and application maintenance. Owing to data sensitivity, regulatory enforcement or audit issues, many companies do not choose to preserve their data in a shared space. Cloud vendors are emerging solutions to solve these privacy issues to allow companies more secure with transitioning their data to the cloud. From a consumer viewpoint, it is critical that any protection threats from bringing an organisation into the cloud are proactively analysed and a Risk Management Plan for all defined risks is accessible. Cost of a countermeasure is an important role in choosing the protection standard. In this post, we have described the capabilities of a consumer when choosing a cloud service. Choose a company who will ensure that the data storage practises are open. Design a SLA that specifically shows the liability of the cloud provider in the event that protection thresholds are not reached.

Rerences

[1] Hedjaz Sabrine, Baadache Abderrahmane and Semchedine Fouzi 2019 Comparative Study of Security Methods against DDOS Attacks in Cloud Computing Environment *International Symposium on Networks, Computers and Communications (ISNCC).*

[2] Taous Madi, Mengyuan Zhang and Yosr Jarraya 2018 Quanti C: Distance Metrics for Evaluating Multi-Tenancy Threats in Public Cloud *IEEE International Conference on Cloud Computing Technology and Science (CloudCom).*

[3] Asvija B R Eswari and Bijoy M B 2017 Virtualization detection strategies and their outcomes in public clouds *IEEE Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics.*

[4] Matheus Torquato, Lucas Torquato and Paulo Maciel 2019 IaaS cloud availability planning using models and genetic algorithms *Latin-American Symposium on Dependable Computing (LADC).*

[5] Chaitanya K and Rudrabhatla, 2020 Comparison of zero downtime based deployment techniques in public cloud infrastructure *Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC).*

[6] Ahmed S and Raja M Y A 2001 Tackling cloud security issues and forensics model *High-Capacity OpticalNetworks and Enabling Technologies (HONET)* pp 190-195.

[7] Amazon 2011 Amazon Web Services Overview of Security Processes. Retrieved fromhttp://awsmedia.s3.amazonaws.com/pdf/AWS_Security_Whitepaper.pdf.

[8] Amazon 2012 AWS Risk and Compliance. Retrieved fromhttp://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf.

[9] Amazon Web Services. 2012 Service Health Dashboard. Retrieved from http://status.aws.amazon.com/

[10] Anchises M. G. de Paula 2009 Cloud Computing: Enterprise Risks and Mitigation. Retrieved fromhttp://www.slideshare.net/anchises/cloud-computing-20091124-gts

[11] Balding C 2008 Assessing the Security Benefits of Cloud Computing. Retrieved fromhttp://cloudsecurity.org/blog/2008/07/21/assessing-the-security-benefits-of-cloud-computing.html.

[12] Carroll M, Van der Merwe A and Kotze P 2011 Secure cloud computing: Benefits, risks and controls. Information Security South Africa (ISSA) (pp.1-9), 15-17.

[13] Cloud Security Alliance 2012 Top threats to Cloud Computing V1.0. Retrieved fromhttps://cloudsecurityalliance.org/research/top-threats/.

[14] Dhage S N, Meshram B B, Rawat R, Padawe S, Paingaokar M and Misra A, 2011 Intrusion detectionsystem in cloud computing environment *Proceedings of the International Conference & Workshop onEmerging Trends in Technology (ICWET '11*). ACM, New York, NY, USA, 235-239.

[15] ENISA 2009 Cloud Computing Risk Assessment. Retrieved fromhttp://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[16] Gartner. 2011 Gartner Identifies the Top 10 Strategic Technologies for 2012. Retrieved fromhttp://www.gartner.com/it/page.jsp?id=1826214

[17] Google. 2011 Security Whitepaper: Google Apps Messaging and Collaboration Products.Retrievedfromhttp://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/a/help/intl/enGB/admins/pdf/ds_gsa_apps_whitepaper_0207.pdf

[18] Hacigumus H., Iyer, B., &Mehrotra, S. (2002). Providing database as a service. Data Engineering, 2002.Proceedings. *18th International Conference*, pp 29-38.

[19] Hassan T, James B D J and Gail-Joon, A 2010 Security and Privacy Challenges in Cloud Computing Environments *IEEE Security and Privacy* **8(6)** pp 24-31. http://dx.doi.org/10.1109/MSP.2010.186.

[20] IBM 2011 Security and high availability in cloud computing environments. Retrieved fromhttp://public.dhe.ibm.com/common/ssi/ecm/en/msw03010usen/MSW03010USEN.PDF.

[21] Judith M M 2011 Cloud services: Mitigate risks, maintain availability. Retrieved fromhttp://www.ibm.com/developerworks/cloud/library/cl-cloudservicerisks/cl cloudservicerisks-pdf.pdf

[22] Littlejohn J 2012 Private Cloud Blueprint. Retrieved fromhttp://i.techweb.com/informationweek/nwcdigital/feb12/NetworkComputing_2012_03.pdf

[23] Minqi Z, Rong Z, Wei X., Weining Q and Aoying Z 2010 Security and Privacy in Cloud Computing: ASurvey. Semantics Knowledge and Grid (SKG) *Sixth International Conference* pp 105-112.

[24] Owens K. 2008 Securing Virtual Compute Infrastructure in the Cloud. Retrieved fromhttp://www.savvis.com/en-us/info_center/documents/hos-whitepaper-securingvirutalcomputeinfrastructureinthecloud.pdf

[25] Parno B 2007 The Trusted Platform Module (TPM) and Sealed Storage. Retrieved fromhttp://www.rsa.com/rsalabs/technotes/tpm/sealedstorage.pdf

[26] PC Advisor. 2011 Experts explain greatest threats to cloud security. Retrieved fromhttp://www.pcadvisor.co.uk/news/security/3310229/experts-explain-greatest-threats-cloud-security

[27] Ristenpart T, Tromer E, Shacham H and Savage S 2009 Hey, you, get off of my cloud: exploringinformation leakage in third-party compute clouds. In Proceedings of the *16th ACM conference onComputer and communications security (CCS '09)*, ACM, 199-212

[28] Salesforce. 2012. Secure, private, and trustworthy: Enterprise cloud computing with Force.com. Retrievedfrom http://www.salesforce.com/assets/pdf/misc/WP_Forcedotcom-Security.pdf

[29] Salesforce. 2012 System Status. Retrieved from http://trust.salesforce.com/trust

[30] Saripalli, P., & Walters, B. 2010 QUIRC: A Quantitative Impact and Risk Assessment Framework for CloudSecurity. In Proceedings of the 2010 *IEEE 3rd International Conference on Cloud Computing (CLOUD '10),IEEE Computer Society* pp 280-288.

[31] Somani U, Lakhani K, and Mundra M 2010 Implementing digital signature with RSA encryption algorithmto enhance the Data Security of cloud in Cloud Computing. Parallel Distributed and Grid Computing(PDGC), 2010 *1st International Conference* pp 211-216.

[32] Subashini S and Kavitha V 2011 A survey on security issues in service delivery models of cloud computing *Journal of Network and Computer Applications* **34(1)** pp 1-11. http://dx.doi.org/10.1016/j.jnca.2010.07.006.

[33] Thibodeau P 2011 Amazon outage sparks frustration, doubts about cloud. Retrieved fromhttp://www.computerworld.com/s/article/9216098.

[34] Tsai H, Siebenhaar M, Miede A, Huang Y and Steinmetz R 2012 Threat as a Service?: Virtualization's Impact on Cloud Security. IT Professional **14(1)** pp 32-37. http://dx.doi.org/10.1109/MITP.2011.117.

[35] Vaquero L M, Rodero-Merino L and Moran D 2011 Locking the sky: a survey on IaaS cloud security.Computing **91** pp 93-118. http://dx.doi.org/10.1007/s00607-010-0140-x.

[36] Verizon Business 2011 Data Breach Investigations Report. Retrieved fromhttp://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.

[37] Vieira K, Schulter A, Westphall C B, and Westphall C M 2010 Intrusion Detection for Grid and Cloud Computing IT Professional **12(4)** pp 38-43. http://dx.doi.org/10.1109/MITP.2009.89.

[38] Zissis D and Lekkas D 2012 Addressing cloud computing security issues *Future Generation Computer Syst.* **28(3)**, pp 583-592. http://dx.doi.org/10.1016/j.future.2010.12.006.

[39] Rahul Ghosh, Francesco Longo, Flavio Frattini and Stefano Russo 2014 Scalable analytics for IaaS cloud availability *IEEE Transactions on Cloud Computing* **2**(2).