social Informatics Business, Politics, Law & Technology Journal
Vol 5, No 3, September, 2019

Humans in The Clouds: Towards the Analysis of Techniques and Methods used to Counter Vulnerabilities Inherently Embedded in Cloud Computing

Onwodi, G.O.
Department of Computer Science
National Open University of Nigeria
Abuja, FCT, Nigeria
E-mail: gonwodi@noun.edu.ng

ABSTRACT

New vulnerabilities come up every day with cloud computing as more resources and services are migrated to the clouds. Cloud computing has been envisioned as the next generation paradigm in computation. In the cloud computing environment, both applications and resources are delivered on demand over the Internet as services. Cloud is an environment of the hardware and software resources in the data centre's that provide diverse services over the network or the Internet to satisfy user's requirements. In this discourse, we attempt to initiate a research that analyze techniques and methods used to counter vulnerability inherently embedded in cloud computing.

Keywords: Humans, Clouds, Analysis, Techniques, Methods, Counter, Vulnerabilities, Embedding, Computing.

Journal Reference Format:
Onwodi, G (2019): Humans in The Clouds: Towards the Analysis of Techniques and Methods used to Counter Vulnerabilities Inherently Embedded in Cloud Computing. Social Informatics, Business, Politics, L:aw & Technology Journal. Vol. 5 . No. 4, Pp 1-22. www.isteams/socialinformaticsjournal

1. INTRODUCTION

The explanation of "cloud computing" from the National Institute of Standards and Technology (NIST) is that cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. According to the explanation, cloud computing provides a convenient on-demand network access to a shared pool of configurable computing resources. Resources refer to computing applications, network resources, platforms, software services, virtual servers, and computing infrastructure.

Cloud Computing can be explained as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or services provider interaction. Cloud Computing offers various service models as well as deployment models. The service models include; Infrastructure as a service (IaaS),

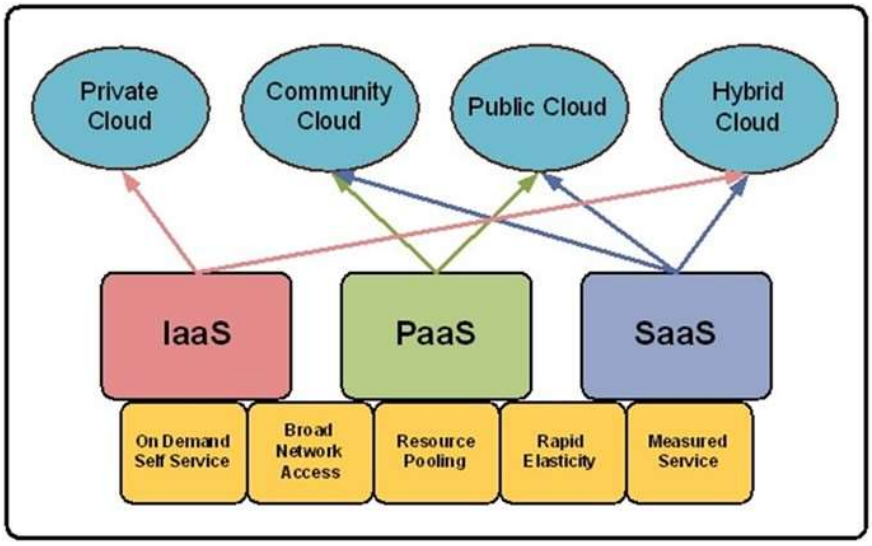

Fig 1: Cloud Services

Platform as a Service (PaaS) and Software as a Service (Saas) whilst the deployment models consist of; Public, Private, Hybrid and Community Cloud.*cloud service models; IAAS, PAAS, and SAAS.*

- **Infrastructure as a service (IAAS)**
  Is one of the models that provides computer infrastructure on an outsourced basis to support enterprise operations. IAAS delivers hardware, servers, data center space, storage and network components. With IAAS, the provider virtualized computing resources over the internet. There is no worries about the underlying physical machine. The clients of IAAS access resources and services through the internet. Clients again make use of cloud provider's services to install the remaining elements of application stack. For instance, users of IAAS can log into the platform to create virtual machines, install operating system in each virtual machine, creates storage buckets for workloads and backups, deploy middleware such as database, and install the enterprise workload into that VM.
- **Platform as a service (PAAS)**
  Is a service model that provides users with computing platform such as; operating system, programming language execution environment, database, web server etc. With PAAS, a third party delivers software and hardware tools mostly those needed for application deployment to users over the internet. Resources that propel you to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise application are made available by the cloud provider. In PAAS, there is no control over the underlying architecture including Operating System, storage, servers etc., the cloud provider gives the ability to the customer to deploy customer created applications using programming languages, tools etc., that are provided by the cloud provider.
- **Software as a service (SAAS)**
  Is a one of the service model where cloud users access software over the internet. In SAAS, access to the software is provided on a subscription basis, with the software being located on external servers rather than on servers located in-house. Meaning a service provider host the application at its data center and a cloud user accesses it through a standard browser. The SAAS describes the distribution of ready to use applications based on this technology model.

1.1 Deployment Models

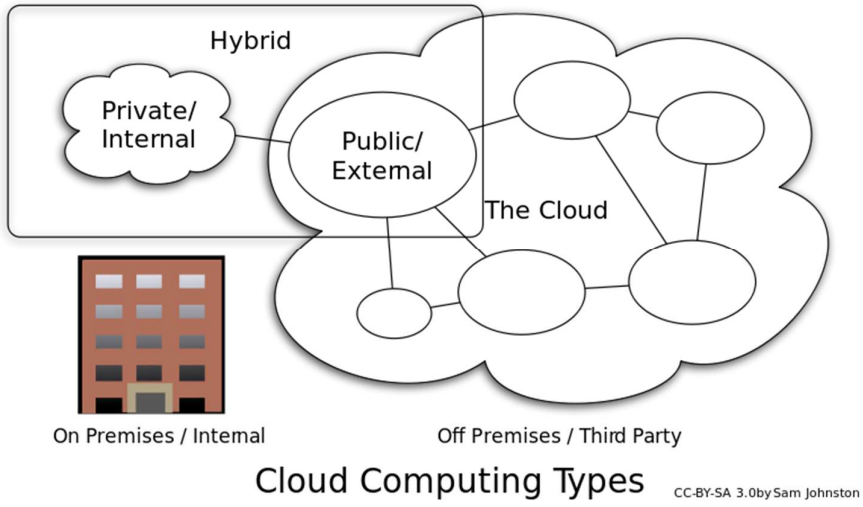

Fig 2: Cloud Computing Types

Public cloud
Is a deployment model in which a service provider makes resources such as storage and virtual machines, applications, etc. available to the general public over the internet. Services provided by Public cloud may be free or offered on pay-per-use model. In public cloud, the service provider manages the cloud solutions core infrastructure, software and other back-end architecture in a multitenant environment in order to free up client or cloud users from these responsibilities.

Private cloud
Is a computing model of cloud computing where IT services are provisioned over Private IT infrastructure for the dedicated use of a single organization. It encompasses a secure and unique cloud environment in which only the specified client can operate. With private cloud, the pool of resources are only accessible by a single organization thereby enshrining that single organization with greater control and privacy. Private cloud is mostly managed through internal resources and offers proprietary environment dedicated to a single business entity

Hybrid cloud
Is a deployment model that integrates private and public cloud by permitting data and applications to be shared between them and utilizing them to perform distinct functions within the same organization. Hybrid clouds gives organization greater flexibility and more data deployment options. It also provides organizations the capacity to seamlessly scale their on-premises infrastructure up to the public cloud to handle any overflow without giving third-party datacenters access to the entirety of the data. This model enable organizations to maximize their efficiencies by using public cloud services for all non-sensitive operations and relying on a private cloud where the need arises, in this regard it ensures all platforms are seamlessly integrated.

Community cloud
Is a cloud deployment model in which the setup of the cloud is shared manually among different organizations that belong to the same community and share similar or common purpose. This model delivers a cloud computing solution to a specified number of organizations that is governed, managed and secured commonly by all the participating organizations or a third-party managed service provider. Communities that come together to embrace this model have similar requirements and their ultimate goal is to work together to achieve their business goals.

Cloud computing encompasses features such a ubiquitous network access, rapid resource elasticity, on-demand self-service, usage based pricing, transference of risk and location independent resource pooling which makes it very attractive to the academia and the industrial world at large. This research looks into data protection and data security which is unarguably the biggest concern for both customers of cloud and the cloud providers. Cloud computing brings to bear various attributes that makes it cumbersome for trusting the system. Several tools have been tested and introduced by researchers for data prevention and protection to eradicate the mistrust of the system yet there are still gaps which needs immediate attention. This paper will review different security techniques and hindrances for data storage security.

2. LITERATURE REVIEW

There are numerous security mechanism that have been proposed by different researchers. In this section we will provide the literature survey of work done in this field.

Rabi Prasad Padhy, Cloud computing is an architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc.

Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data centre of a cloud provider like Google, Amazon, Salesforce.com and Microsoft etc. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. This research paper outlines what cloud computing is, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry. This research paper also analyses the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate.

S. Kumar, Cloud computing is the development of parallel computing, distributed computing, grid computing and virtualization technologies which define the shape of a new era. Cloud computing is an emerging model of business computing. In this paper, authors explore the concept of cloud architecture and compares cloud computing with grid computing. We also address the characteristics and applications of several popular cloud computing platforms. In this paper, we aim to pinpoint the challenges and issues of cloud computing. We identified several challenges from the cloud computing adoption perspective and we also highlighted the cloud interoperability issue that deserves substantial further research and development. However, security and privacy issues present a strong barrier for users to adapt into cloud computing systems. In this paper, we investigate several cloud computing system providers about their concerns on security and privacy issues.

In 2010 S Subashini and V Kavitha proposes a security framework by different methods provided dynamically, that one of the components of this framework refers to provide data security by storage and access to data based on meta-data, which is similar to storing related data in different areas based on meta data, and if the destruction of user data takes place, it can be retrieved. Each part of the framework in "security as a service" is provided for practical applications by providers of security as a layer or multiple layers of required applications.

In 2011 V. Krishna Reddy and DR. L.S.S. Reddy proposed the security problems at different levels of the architecture of cloud computing services have been studied. Security of customer-related data is a substantial need for services which is provided by each model of cloud computing. They have studied matters of on-going security software as a service (SaaS), platform as a service (PaaS) and Infrastructure as a Service (IaaS).This paper focuses on the use of cloud services and security for working cross-domain Internet connected.

In 2011, Jan de Muijnck-Hughes proposed a security technique which is known as Predicate Based Encryption (PBE). PBE represents a family of asymmetric encryption and originates from Identity Based Encryption. This technique integrates Attribute Based Access Control (ABAC) with asymmetric encryption, thereby permitting a single encryptor/multi decryptor environment to be realized using a single scheme. This Predicate Based Encryption focuses its implementation at both Platform as a service and Software as a service. This proposed technique also precludes unwanted exposure, unwanted leakage and other unwanted breaches of confidentiality of cloud resident data. In 2011 Venkata Sravan et.al wrote a paper titled Security Techniques for Protecting Data in Cloud. The aim of this paper is to understand the security threats and identify the appropriate security techniques used to mitigate them in Cloud computing. The research identified a total number of 43 security challenges and 43 security techniques. The most measured attribute is Confidentiality (31%) followed by Integrity (24%) and Availability (19%).

In 2011 Ali Asghary Karahroudy wrote a paper titled Security Analysis and Framework of Cloud Computing with Parity Based Partially Distributed File System. This paper proposed a technique called Partially Distributed File System with Parity (PDFSP) which is a protocol developed as a modification on the existing GFS/HDFS. This PDFSP has four main components; Client Access Machine, User Public Machine, Cloud Management Server and File Retrieval Server. All these components work together to ensure data being transmitted does not get into wrong hands. This paper addressed the three aspects of security which are Confidentiality, Integrity and Availability. In 2012 Punyada M. Deshmukh et. al. wrote a paper. In this paper they have proposed a system which ensures the data storage security using a distributed scheme. A set of Master servers are used which are responsible for processing the users requests. File chunking operation is performed in order to store replicas of file at Slave server providing backup for file recovery. Unlike the previously proposed systems, efficient and dynamic data operations are performed by users. This efficiency is achieved by imparting the data blocks for different users. The functionality is extended to the Android users and the chatting application is included to add ease and comfort to the working environment of users.

In 2013 Nabil Giweli proposed a solution based approach referred as Data Centric Security approach. This approach aims at providing security at the data level hence the data are self-describing, self-defending and self-protecting during their lifecycle in the cloud environments. This approach gives the entire responsibility to the data owner to set and manage the data privacy and security measures. This proposed solution is based on Chinese Remainder Theorem (CRT) and it utilizes symmetric and asymmetric encryption techniques. In this paper, the proposed solution is proven to be very efficient as it does not require complex key derivation methods and the data file does not need to be encrypted more than once.

In 2013 Miao Zhou outlined 5 techniques to provide security and integrity of data in cloud computing. These techniques include; Innovative tree-based key management scheme, Privacy enhanced data outsourcing in the cloud, Privacy preserved access control for cloud computing, Privacy enhanced keyword search in clouds and Public remote integrity check for private data. This paper adopted Keyword Searching Mechanism which enables efficient multi-user keyword searches and hides the private information in the search queries [5]. An encryption scheme for a two-tier system was presented to achieve flexible and fine-grained access control in the cloud. The experimental results indicated that the proposed scheme is efficient especially when the size of the data file is large or the integrity check is frequent.

In 2014 Sudhansu Ranjan Lenka et.al wrote a paper titled "Enhancing Data Security in Cloud Computing using RSA Encryption and MD5 Algorithm. As the title of the paper suggests; they implemented both RSA Algorithm and MD5 Algorithm. In this paper, the RSA Algorithm is used for secured communication and file encryption and decryption purpose whilst MD5 Algorithm is used for digital signature as well as covering the tables for unauthorized users. The two algorithm proposed provides the three (3) aspects of security which are Confidentiality, Integrity and Availability.

In 2014 Aastha Mishra proposed an Advanced Secret Sharing Key Management Scheme. The aim of this paper is to propose a more reliable decentralized light weight key management technique for cloud systems which provide more efficient data security and key management in cloud systems. Security and privacy of user's data is preserved in the proposed technique by the replication of key share among several clouds by the use of secret sharing approach and using a voting method to check the integrity of shares. In this paper, the technique used also brings to bear better security against byzantine failure, server colluding and data modification attacks.

In 2014 Nesrine Kaaniche wrote a paper titled; Cloud Data Storage Security based on Cryptographic Mechanisms. In this paper, Nesrine proposed two (2) techniques to secure data which are ID-Based Cryptography (IBC) and CloudaSec. With the ID-Based Cryptography, the paper proposed to use each client as a private key generator which generates his own ID-Based Cryptographic Public Elements (IBC-PE). These IBC-PE are used to compute ID-based keys and also serve to encrypt the data before their storage and sharing in the cloud [8]. With regards to CloudaSec, there is a public key based solution which proposes the separation of subscription-based key management and confidentiality oriented asymmetric encryption policies.

The CloudaSec aids scalable and flexible deployment of the solution as well as strong security guarantees for outsourced data in cloud servers. It is analysed and understood in this paper that the cryptographic operations at the client side are acceptable compared to the upload operations and do not carry exhaustive computational capacities. For example, a $8*10^5$ bytes of data size requires only 0.1 seconds to be enciphered, compared to 10 seconds to be uploaded. Therefore the encryption procedures involve 1% from the Openstack upload overhead.

In 2014 Afnan Ullah Khan proposed a technique known as Access Control and Data Confidentiality (ACDC) in his paper titled Data Confidentiality and Risk Management in Cloud Computing. The aim of the paper was to develop a novel scheme that would enforce access control policies on cloud computing scenarios. He used a scenario in Medical/Health care where he came out with the following compostions; Data Owner (Medical centre), Data Consumers (patients, nurses, doctors etc.), Infrastructure Provider and Trusted Authority. The paper focused on Infrastructure as a Service as its deployment model whereas data confidentiality and authentication were achieved through the proposed technique. In 2015 Karun Handa et. al. described that Cloud Computing is a technology that readily makes available resources that otherwise may require huge amount of investment. Besides, it increases the availability of resources since anyone can access the data using web. But this advantage comes at a cost.

Firstly, the data is uploaded insecurely which has a high risk of being hacked by some malicious people. Secondly, the data saved at remote servers is under the surveillance of unknown people who can do anything with our data. So, these data security risks are causing a hindrance in the development of the field of cloud computing. Thus, this paper has designed a scheme that can help, solve this issue.

In 2016 Sarojini et.al proposed a technique known as Enhanced Mutual Trusted Access Control Algorithm (EMTACA). This technique presents a mutual trust for both cloud users and cloud service providers to avoid security related issues in cloud computing. The aim of this paper is to propose a system which include EMTACA algorithm which can assure enhanced guaranteed and trusted and reputation based cloud services among the users in a cloud environment. The results of this paper showed data confidentiality, integrity and availability which is the three most important aspect of data security was achieved. In 2016 AL-Museelem Waleed, Li Chunlin assesses how security and privacy issues transpire in the context of cloud computing and examines ways in which they might be addressed. This paper aims to solve privacy and security issues in cloud computing using UEC (Ubuntu Enterprise Cloud). The methodology used involves encrypting and decrypting data to ensure privacy and security in the cloud.

In 2017, Dimitra A. Geogiou wrote a paper to present security policies for cloud computing. The purpose of the security policies is to protect people and information, set rules for expected behavior by users, minimize risks and help to track compliance with regulation. The paper focused on Software as a Service. The paper presented a detailed review and analysis of existing studies as far as security is concern in cloud computing. With Dimitra's review of existing threat, he focused on the once that are not applicable to conventional systems. To be able to identify new rules that supposed to be integrated in the cloud policy, a methodology was proposed for assessing different threats in the cloud. This paper scrutinized the security requirements of a cloud service provider taking into consideration a case study of E-health system of Europe.

3. SECURITY PRACTICES IN CLOUD COMPUTING ENVIRONMENT

Protection Against Internal and External Threats

Security monitoring services help to improve the effectiveness of the security infrastructure of a customer by actively analysing logs and alerts from infrastructure devices around the clock and in real time. Monitoring teams correlate information from various security devices to provide security analysts with the data they require to eliminate false positives and respond to true threats against the enterprise. Usually the skills required to maintain the level of service of an organization is very high. The information security team can assess system performance on a periodically recurring basis and provide recommendations for improvements as needed.

Early Detection

An early detection service detects and reports new security vulnerabilities shortly after they appear. Generally, the threats are correlated with third party sources, and an alert or report is issued to customers. Security vulnerability reports, aside from containing a detailed description of the vulnerability and the platforms affected, also include information on the impact the exploitation of this vulnerability would have on the systems or applications previously selected by the company receiving the report. Most often, the report also indicates specific actions to be taken to minimize the effect of the vulnerability, if that is known.

Platform, Control, and Services Monitoring

Platform, control, and services monitoring is often implemented as a dashboard interface and makes it possible to know the operational status of the platform being monitored at any time. It is accessible from a web interface, making remote access possible. Each operational element that is monitored usually provides an operational status indicator, always taking into account the critical impact of each element.

This service aids in determining which elements may be operating at or near capacity or beyond the limits of established parameters. By detecting and identifying such problems, preventive measures can be taken to prevent loss of service.

Intelligent Log Centralization and Analysis
Intelligent log centralization and analysis is a monitoring solution based mainly on the correlation and matching of log entries. Such analysis helps to establish a baseline of operational performance and provides an index of security threat. Alarms can be raised in the event an incident moves the established baseline parameters beyond a stipulated threshold. These types of sophisticated tools are used by a team of security experts who are responsible for incident response once such a threshold has been crossed and the threat has generated an alarm or warning picked up by security analysts monitoring the systems.

Vulnerabilities Detection and Management
Vulnerabilities detection and management enables automated verification and management of the security level of information systems. The service periodically performs a series of automated tests for the purpose of identifying system weaknesses that may be exposed over the Internet, including the possibility of unauthorized access to administrative services, the existence of services that have not been updated, the detection of vulnerabilities such as phishing, etc. The service performs periodic follow-up of tasks performed by security professionals managing information systems security and provides reports that can be used to implement a plan for continuous improvement of the system's security level.

Continuous System Patching/Upgrade and Fortification
Security posture is enhanced with continuous system patching and upgrading of systems and application software. New patches, updates, and service packs for the equipment's operating system are necessary to maintain adequate security levels and support new versions of installed products. Keeping abreast of all the changes to all the software and hardware requires a committed effort to stay informed and to communicate gaps in security that can appear in installed systems and applications.

Intervention, Forensics, and Help Desk Services
Quick intervention when a threat is detected is crucial to mitigating the effects of a threat. This requires security engineers with ample knowledge in the various technologies and with the ability to support applications as well as infrastructures on a 24/7 basis. MaaS platforms routinely provide this service to their customers. When a detected threat is analyzed, it often requires forensic analysis to determine what it is, how much effort it will take to fix the problem, and what effects are likely to be seen. When problems are encountered, the first thing customers tend to do is pick up the phone. Help desk services provide assistance on questions or issues about the operation of running systems. This service includes assistance in writing failure reports, managing operating problems, etc.

On-demand self-service
The use of cloud computing can be compared to the use light and water. You can use it whenever you need it and pay per use. Is in the form utility computing. This form of storing and accessing your data gives you full control over your resource usage and spending.

Broad Network Access
You can access the cloud services from across the web using any device with internet connectivity. The reason for this is its underlying infrastructure that includes servers on multiple locations. Deployment of services include everything from using business applications to the newest smartphones.

Resource Pooling

Multiple users can share the same space and resources can be assigned, re-assigned and distributed as needed. You can be anywhere in the world and still have the equal access as everyone else provided you have internet access.

Rapid elasticity

Cloud can grow and shrink as much as possible without affecting any of its users or their information. For example; if your business is experiencing peak traffic, the cloud can expand to accommodate all the new requests.

- **Measured service**

You can examine how often people are using the cloud. Cloud used metering for managing and optimizing the service and to provide reporting and billing information. Many cloud providers utilize pay-as-you-go model to ensure their clients are billed for services they are utilizing no more no less.

3.1 Challenges Observed in Literature

Few challenges or issues that were identified during reading and analyzing the research papers have been outlined below;

- Some of the research papers focused their implementation on Platform as a service and Software as a service leaving Infrastructure as a service behind.
- Other papers also concentrated on data Confidentiality without taking into account Integrity, non-repudiation and authenticity.
- Few of the papers were theoretical based meaning actual practical implementation was not done.
- In other papers, though the technique proposed seams reliable, but it looks weird, complicated and cumbersome to implement.
- Some proposed techniques were also not experimentally validated like the Access Control and Data Confidentiality (ACDC)

4. RESEARCH DIRECTION

Our research efforts will revolve around analysing the techniques and methods used to counter the vulnerabilities inherently present in cloud computing and how best to deploy these techniques to improve security and privacy in cloud computing.

To achieve this, we will seek to complete the following objectives

- Review different security challenges to data security and privacy
- Review the different techniques currently available to ensure data security
- Make a comparative analysis of existing research work regarding the techniques for data security in cloud computing
- Provide a simple catalogue for which techniques work best for different applications and technologies.

4.1 Statement of Problem

Cloud computing has been envisioned as the next generation paradigm in computation. In the cloud computing environment, both applications and resources are delivered on demand over the internet. Cloud computing provides a convenient on demand access to a shared pool of configurable computing resources. Resources refers to computing applications, network resources, platforms, software services, virtual servers and computing infrastructure. The merits of cloud computing have attracted interests from both the industrial world and academic research world, however, there are still some problems to solve for personal users and enterprises to store data and deploy applications in the cloud computing environment.

One of the most significant barriers to adoption of cloud computing technology is data security which is compounded by issues including compliance, privacy, trust and legal matters. Data security is particularly important to cloud computing because data are scattered in different machines and storage devices such as wireless sensor networks and smart phones.

To make the cloud computing to be adopted by users and enterprises, there is a need to address the security concerns of the users and make cloud computing a trustworthy environment. In this research work we will review different security techniques and challenges for data storage security and privacy in the cloud computing environment. We present a comparative analysis of the techniques used in the data security aspects of cloud computing as well as data privacy issues and technologies.

4.2 Research Methodology

Our research process will cover:

- An informed research on data security and privacy issues in cloud computing
- In-depth analysis of existing techniques for ensuring data security and privacy
- Selection and review of available and relevant literature
- A comparative summary of techniques for data security and privacy in cloud computing.

REFERENCES

[1] Gartner Inc., "Gartner Identifies the Top 10 Strategic Technologies for 2011." [Online]. Available: http://www.gartner.com/it/page.jsp?id=1454221. [Accessed: 15-Jul-2011].

[2] G. Zhao, J. Liu, Y. Tang, W. Sun, F. Zhang, X. Ye, and N. Tang, "Cloud Computing: A Statistics Aspect of Users," in First International Conference on Cloud Computing (CloudCom), Beijing, China, 2009, pp. 347–358.

[3] S. Zhang, S. Zhang, X. Chen, and X. Huo, "Cloud Computing Research and Development Trend," in Second International Conference on Future Networks (ICFN '10), Sanya, Hainan, China, 2010, pp. 93 –97.

[4] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0." 2011. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[5] A. Marinos and G. Briscoe, "Community Cloud Computing," in 1st International Conference on Cloud Computing (CloudCom), Beijing, China, 2009.

[6] Centre for the Protection of National Infrastructure, "Information Security Briefing 01/2010 Cloud Computing," Mar-2010. Available: http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf

[7] A. Khalid, "Cloud Computing: Applying Issues in Small Business," in International Conference on Signal Acquisition and Processing (ICSAP '10), 2010, pp. 278 –281.

[8] KPMG, "From Hype to Future: KPMG's 2010 Cloud Computing Survey." 2010. Available: http://www.techrepublic.com/whitepapers/from-hype-to-future-kpmgs-2010-cloud-computing-survey/2384291

[9] D. G. Rosado, R. Gómez, D. Mellado, and E. Fernández-Medina, "Security Analysis in the Migration to Cloud Environments," Future Internet, vol. 4, no. 2, pp. 469–487, May 2012.

[10] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy. O'Reilly Media, Inc., 2009.

[11] W. Li and L. Ping, "Trust Model to Enhance Security and Interoperability of Cloud Environment," in Proceedings of the 1st International Conference on Cloud Computing, Beijing, China, 2009, pp. 69–79.

[12] J. W. Rittinghouse and J. F. Ransome, "Security in the Cloud," in Cloud Computing: Implementation, Management, and Security, CRC Press, 2009.

[13] B. Kitchenham, "Procedures for Perfoming Systematic Review," Software Engineering Group, Department of Computer Scinece Keele University, United Kingdom and Empirical Software Engineering, National ICT Australia Ltd., Australia, TR/SE-0401, 2004.
[14] B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering. Version 2.3," University of Keele (Software Engineering Group, School of Computer Science and Mathematics) and Durham (Department of Conputer Science), UK, 2007.
[15] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," Journal of Systems and Software, vol. 80, no. 4, pp. 571–583, 2007.
[16] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0." 2010. Available: https://cloudsecurityalliance.org/research/top-threats/
[17] ENISA, "Cloud Computing: Benefits, Risks and Recommendations for Information Security." 2009. Available: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment
[18] K. Dahbur, B. Mohammad, and A. B. Tarakji, "A survey of risks, threats and vulnerabilities in cloud computing," in Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications, Amman, Jordan, 2011, pp. 1–6.
[19] L. Ertaul, S. Singhal, and S. Gökay, "Security Challenges in Cloud Computing," in Proceedings of the 2010 International Conference on Security and Management SAM'10, Las Vegas, US, 2010, pp. 36–42.
[20] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," IEEE Security Privacy, vol. 9, no. 2, pp. 50 –57, 2011.
[21] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, Jan. 2011.
[22] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On Technical Security Issues in Cloud Computing," in IEEE International Conference on Cloud Computing (CLOUD '09), 2009, pp. 109 –116.
[23] C. Onwubiko, "Security Issues to Cloud Computing," in Cloud Computing: Principles, Systems & Applications, N. Antonopoulos and L. Gillam, Eds. Springer-Verlag, 2010.
[24] M. A. Morsy, J. Grundy, and I. Müller, "An Analysis of The Cloud Computing Security Problem," in Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 2010.
[25] W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," in Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa, Kauai, HI, 2011, pp. 1–10.
[26] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.
[27] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," NIST, Special Publication 800-144, 2011.
[28] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST, Special Publication 800-145, Sep. 2011.
[29] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of Internet Services Applications, vol. 1, no. 1, pp. 7–18, May 2010.
[30] J. Ju, Y. Wang, J. Fu, J. Wu, and Z. Lin, "Research on Key Technology in SaaS," in International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), 2010, pp. 384 –387.
[31] D. Owens, "Securing Elasticity in the Cloud," Communications of the ACM, vol. 53, no. 6, pp. 46–51, May-2010.
[32] OWASP, "The Ten Most Critical Web Application Security Risks." 2010. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[33] Y. Zhang, S. Liu, and X. Meng, "Towards high level SaaS maturity model: Methods and case study," in Services Computing Conference. APSCC 2009. IEEE Asia-Pacific, 2009, pp. 273 –278.
[34] F. Chong, G. Carraro, and R. Wolter, "Multi-Tenant Data Architecture," Jun-2006. [Online]. Available: http://msdn.microsoft.com/en-us/library/aa479086.aspx. [Accessed: 05-Jun-2011].

[35] C.-P. Bezemer and A. Zaidman, "Multi-tenant SaaS applications: maintenance dream or nightmare?," in Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE), Antwerp, Belgium, 2010, pp. 88–92.
[36] J. Viega, "Cloud Computing and the Common Man," Computer, vol. 42, no. 8, pp. 106–108, Aug-2009.
[37] Cloud Security Alliance, "Security Guidance for Critical Areas of Mobile Computing." Nov-2012. Available: https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdf
[38] C. Keene, "The Keene View on Cloud Computing," 18-Mar-2009. [Online]. Available: http://www.keeneview.com/2009/03/what-is-platform-as-service-paas.html. [Accessed: 16-Jul-2011].
[39] K. Xu, X. Zhang, M. Song, and J. Song, "Mobile Mashup: Architecture, Challenges and Suggestions," in International Conference on Management and Service Science. MASS '09, 2009, pp. 1 –4.
[40] R. Chandramouli and P. Mell, "State of security readiness," Crossroads, vol. 16, no. 3, pp. 23–25, Mar-2010.
[41] T. Jaeger and J. Schiffman, "Outlook: Cloudy with a Chance of Security Challenges and Improvements," IEEE Security Privacy, vol. 8, no. 1, pp. 77 –80, 2010.
[42] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a service security: Challenges and solutions," in the 7th International Conference on Informatics and Systems (INFOS), 2010, pp. 1 –8.
[43] A. Jasti, P. Shah, R. Nagaraj, and R. Pendse, "Security in multi-tenancy cloud," in IEEE International Carnahan Conference on Security Technology (ICCST), 2010, pp. 35 –41.
[44] T. Garfinkel and M. Rosenblum, "When virtual is harder than real: Security challenges in virtual machine based computing environments," in Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM, 2005, vol. 10, pp. 227–229.
[45] J. S. Reuben, "A survey on virtual machine security," Seminar on Network Security, 2007.
[46] K. Hashizume, N. Yoshioka, and E. B. Fernandez, "Three Misuse Patterns for Cloud Computing," in Security Engineering for Cloud Computing: Approaches and Tools, D. G. Rosado, D. Mellado, E. Fernandez-Medina, and M. Piattini, Eds. IGI Global, 2013, pp. 36–53.
[47] S. Venkatesha, "Survey of Virtual Machine Migration Techniques," 2009.
[48] P. Ranjith, P. Chandran, and S. Kaleeswaran, "On Covert Channels between Virtual Machines," Journal in Computer Virology, Springer, vol. 8, pp. 85–97, 2012.
[49] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning, "Managing security of virtual machine images in a cloud environment," in Proceedings of the 2009 ACM workshop on Cloud computing security, 2009, pp. 91–96.
[50] K. Owens, "Securing Virtual Compute Infrastructure in the Cloud." SAVVIS. Available: http://www.savvis.com/en-us/info_center/documents/hos-whitepaper-securingvirutalcomputeinfrastructureinthecloud.pdf
[51] H. Wu, Y. Ding, C. Winer, and L. Yao, "Network security for virtual machine in cloud computing," in 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), 2010, pp. 18 –21.
[52] G. Xiaopeng, W. Sumei, and C. Xianqin, "VNSS: A network security sandbox for virtual computing environment," in IEEE Youth Conference on Information Computing and Telecommunications (YC-ICT), 2010, pp. 395 –398.
[53] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," in Proceedings of the 33rd International Convention MIPRO, 2010, pp. 344 –349.
[54] S. Carlin and K. Curran, "Cloud Computing Security," International Journal of Ambient Computing and Intelligence, vol. 3, no. 1, pp. 38–46, 2011.
[55] A. Bisong and S. Rahman, "An Overview of the Security Concerns in Enterprise Cloud Computing," International Journal of Network Security & Its Applications (IJNSA), vol. 3, no. 1, pp. 30–45, Jan. 2011.
[56] M. Townsend, "Managing a security program in a cloud computing environment," in Information Security Curriculum Development Conference, Kennesaw, Georgia, 2009, pp. 128–133.
[57] V. Winkler, Securing the cloud: Cloud computer security techniques and tactics. Elsevier Inc., 2011.

[58] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2009, pp. 199–212.
[59] Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Cross-VM side channels and their use to extract private keys," in Proceedings of the 2012 ACM conference on Computer and communications security, New York, NY, USA, 2012, pp. 305–316.
[60] Z. Wang and X. Jiang, "HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity," in Proceedings of the IEEE Symposium on Security and Privacy, 2010, pp. 380–395.
[61] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in Cloud Computing," in the 17th International Workshop on Quality of Service, 2009, pp. 1–9.
[62] E. B. Fernandez, N. Yoshioka, and H. Washizaki, "Modeling Misuse Patterns," in Proceedings of the 4th Int. Workshop on Dependability Aspects of Data Warehousing and Mining Applications (DAWAM 2009), in conjunction with the 4th Int.Conf. on Availability, Reliability, and Security (ARES 2009), Fukuoka, Japan, 2009, pp. 566 –571.
[63] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards Trusted Cloud Computing," in Proceedings of the 2009 conference on Hot topics in cloud computing, San Diego, California, 2009.
[64] F. Zhang, Y. Huang, H. Wang, H. Chen, and B. Zang, "PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection," in Trusted Infrastructure Technologies Conference, 2008. APTC '08. Third Asia-Pacific, 2008, pp. 9 –18.
[65] Cloud Security Alliance, "SecaaS Implementation Guidance, Category 1: Identity and Access Managament." 2012. Available: https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf
[66] S. Xiao and W. Gong, "Mobility Can Help: Protect User Identity with Dynamic Credential," in Eleventh International Conference on Mobile Data Management (MDM), 2010, pp. 378 –380.
[67] D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Side Channels in Cloud Services: Deduplication in Cloud Storage," IEEE Security Privacy, vol. 8, no. 6, pp. 40 –47, 2010.
[68] J. Wylie, M. Bakkaloglu, V. Pandurangan, M. Bigrigg, S. Oguz, K. Tew, C. Williams, G. Ganger, and P. Khosla, "Selecting the right data distribution scheme for a survivable storage system," CMU-CS-01-120, May 2001.
[69] U. Somani, K. Lakhani, and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing," in 1st International Conference on Parallel Distributed and Grid Computing (PDGC), 2010, pp. 211 –216.
[70] M. Tebaa, S. El Hajji, and A. El Ghazi, "Homomorphic encryption method applied to Cloud Computing," in National Days of Network Security and Systems (JNS2), 2012, pp. 86 –89.
[71] E. Fong and V. Okun, "Web Application Scanners: Definitions and Functions," in Proceedings of the 40th Annual Hawaii International Conference on System Sciences, 2007.
[72] D. Goodin, "Webhost hack wipes out data for 100,000 sites," The Register, 08-Jun-2009. [Online]. Available: http://www.theregister.co.uk/2009/06/08/webhost_attack/. [Accessed: 02-Aug-2011].
[73] S. Berger, R. Cáceres, D. Pendarakis, R. Sailer, E. Valdez, R. Perez, W. Schildhauer, and D. Srinivasan, "TVDc: managing security in the trusted virtual datacenter," SIGOPS Oper. Syst. Rev., vol. 42, no. 1, pp. 40–47, Jan. 2008.
[74] S. Berger, R. Cáceres, K. Goldman, D. Pendarakis, R. Perez, J. R. Rao, E. Rom, R. Sailer, W. Schildhauer, D. Srinivasan, S. Tal, and E. Valdez, "Security for the cloud infrastructure: trusted virtual data center implementation," IBM Journal of Research and Development, vol. 53, no. 4, pp. 560–571, Jul. 2009.
[75] T. Ormandy, "An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments," in CanSecWest Applied Security Conference, Vancouver, 2007.
[76] J. Oberheide, E. Cooke, and F. Jahanian, "Empirical Exploitation of Live Virtual Machine Migration," in Proceedings of BlackHat DC convention, 2008.

[77] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," in Proceedings of the 3rd ACM workshop on Cloud computing security workshop, 2011, pp. 113–124.
[78] W. Han-zhang and H. Liu-sheng, "An improved trusted cloud computing platform model based on DAA and privacy CA scheme," in International Conference on Computer Application and System Modeling (ICCASM), 2010, vol. 13, pp. V13–33 –V13–39.
[79] E. B. Fernandez, O. Ajaj, I. Buckley, N. Delessy-Gassant, K. Hashizume, and M. M. Larrondo-Petrie, "A Survey of Patterns for Web Services Security and Reliability Standards," Future Internet, vol. 4, no. 2, pp. 430–450, Apr. 2012.