# A Critical Review of Security Threats in Cloud Computing

Mahroosh Irfan, Muhammad Usman
Department of Computing
SZABIST-Islamabad
Pakistan
irfanmahrosh@gmail.com
dr.usman@szabist-isb.edu.pk

Yan Zhuang, Simon Fong
Department of Computer and Information Science
University of Macau
Macau SAR
{syz, ccfong}@umac.mo

***Abstract*—The innovation of Internet has enhanced the use of computers and mobile devices. As a result a large amount of data is being generated on daily basis. Information Technology infrastructure continues to grow with evolving technology and as a result a new business model has emerged known as "Cloud Computing". It is set of resources and services which are obtainable through the Internet. Cloud services are provided from data centers which are located all over the world. It is one of the most electrifying technologies because it has reduced cost related to the computing whereas increased flexibility, scalability, mobility and enhanced storage. The rapid growth in the field of "Cloud Computing" similarly upsurges severe security concerns. Security is actually one of the widely discussed issues in cloud computing; other issues being Availability, Integrity etc. Many research papers have proposed solutions to these problems.**

**This paper provides a critical review of the recent work done in the area of security by doing a thorough review of recent work in this area. Finally, we propose a model to improve security in cloud architecture.**

***Keywords*-Cloud Computing, Cloud Security, Threats, Service Models, and Deployment Models.**

## I. INTRODUCTION

Cloud computing is basically a type of computing which depends on "*sharing computing resources"* instead of having "local servers or personal devices" to handle the applications. It is an Internet Based computing where all the on-demand resources, software and information is provided to the computers and other devices. It works on a basic principle of "You Pay for What You Use". In layman terms, cloud computing uses the internet to access any software which is actually running on someone else's hardware in somebody else's data center and you are only paying for only what you have consumed [11].

"Cloud Computing" simply means "Internet Computing", as internet itself is a collection of clouds. It permits the consumers to access the online resources at anytime from anywhere without worrying about the hardware, software, technical or any sort of physical maintenance issues. Cloud computing is dynamic, scalable and independent computing and that's what make it different from grid computing. A dominant example of cloud is "Google Apps" - it permits the online user to access the services which are deployed on millions of machines spread over the Internet. No maintenance cost involved in cloud computing as it's the service provider's responsibility to make the desired services available, because of this cloud computing is also known as "Utility Computing"

After cloud development, its implementation varies with reference to the service that it intends to serve. The major service models being implemented are: SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). According to Gartner [12], the financial investment on cloud computing in 2016 will be CAGR (Global Compounded Annual Growth Rate) of: SaaS 17.4%, PaaS 26.6% and IaaS 41% [5, 12].

Despite of the service models cloud even consist of the deployment strategies, a cloud can be deployed by using any of the below mentioned strategies:

- Public cloud
- Private cloud
- Community cloud
- Hybrid cloud

Public cloud is open for the public use and it's a cost effective service for applications hosting. Few examples are: Google, Amazon and Microsoft. Mostly Private Cloud is used. It is appropriate for a single organization. Community cloud is used by the group of organizations who enjoy common interests. Hybrid cloud is a combination of Public and Private Cloud model in order to achieve several different functionalities within the same company [8].

The rapid growth in this field has triggered unavoidable security issues. Cloud security is vital concern, as it's the most prominent reason why organizations fear shifting to cloud. The selected papers focus on: Cloud & Network Security, Integrity, Reliability, Performance, Cost, Regulatory Requirements, Bandwidth, Service Quality, Data Limitations and Segregation, Bug Exploitation, and Management of the Console Security. All these issues are hindering the data transition of the big companies to clouds. There are 7 prominent threats in the current era that are enlisted below: [5, 7]

- **Threat#1** Abuse and Nefarious Use of Cloud Computing
- **Threat#2** Insecure Interfaces and APIs
- **Threat#3** Malicious Insiders
- **Threat#4** Shared Technology issues
- **Threat#5** Data Loss or Leakage

978-1-4673-8501-5/15 $31.00 © 2015 IEEE
DOI 10.1109/ISCBI.2015.26

- **Threat#6** Accounts or service Hijacking
- **Threat#7** Unknown Risk Profile

Figure 1 represents the seven threats which were distributed in the 661 publications related to the security issues. Threat# 7 was published and discusses in 377 Papers and the Threat# 4 was present in 335 publications.

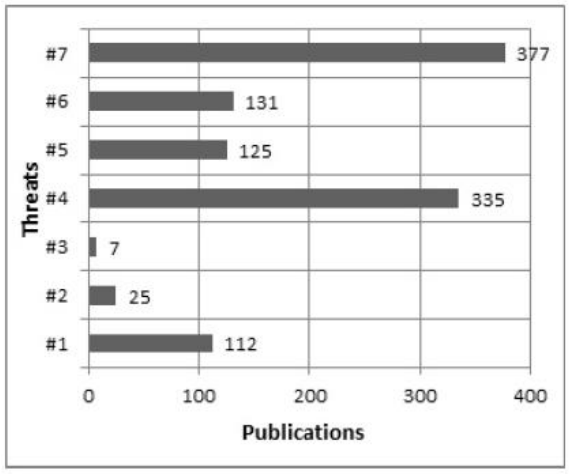



Figure 1. Distribution of publications by threats [5]

This paper is organized as follows: Background is discussed in the 2nd section. Section 3 explores the methodology and inclusion and exclusion criteria. In the 4th section, Literature Review has been discussed. Section 5 comprises of Critical Analysis. The 6th section is about different solutions and recommendations which can be followed to implement data security in cloud. The 7th section concludes everything related to the better security.

## II. BACKGROUND

Cloud computing includes three basic models: SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service).

A. **Software as a Service**: SaaS facilitates the user to access applications and databases. The user does not have to install and execute the application on their local machine. In SaaS, maintenance is easy, hence it is quite cost efficient.

B. **Platform as a Service**: PaaS allows customers to access a processing system or platform to create or coordinate online programs and applications. In PaaS the developer can develop applications, without being concerned about the mediocre service, and deliver it to the users through the servers as well as the web [11, 4]

C. **Infrastructure as a Service**: IaaS is the main cloud service model. It deals with computers and all other resources like VM (Virtual Machines), server, network and storage. Computers can either be physical or virtual machines, for example Google compute engine, Amazon EC2, HP Cloud etc. Now there is no need to purchase the servers and data centers for application deployment. All you need to do is buy all the resources which are required and enjoy application deployment as a fully outsourced service [8, 4]. Figure 2 represents Cloud computing models.

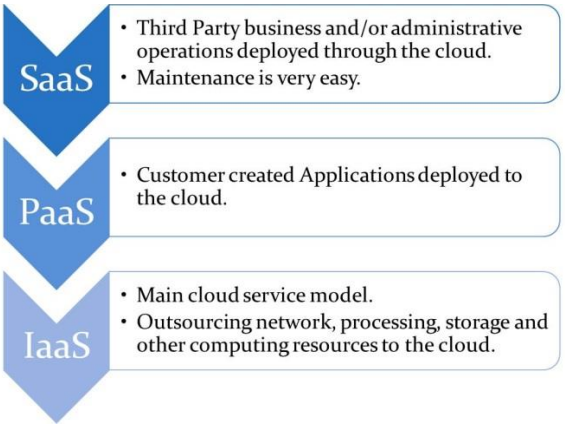



Figure 2. Cloud Computing Models

There are multiple deployment strategies in cloud computing, the basic ones are discussed below.

D. **Public Cloud**: These services are characterized by being available to the clients from actually a third party service provider through the web. As the name "Public" not specifically means "Free" whereas using services of public clouds is equitably inexpensive at time of deploying solutions. Moreover "Public cloud" doesn't mean that there won't be security involved in it, and the data would be publically available. The vendors do provide specific access control mechanism for its users. [1]

E. **Private Cloud**: Private cloud deals with many of the advantages which are provided by the public cloud computing environment for instance service based and elasticity. This type of infrastructure is operated only for a single organization but it can be managed by some other organization or any third party [1, 9]

F. **Hybrid Cloud**: It is a combination of public and private cloud. In this sort of model the users mainly outsource non-critical data and process towards the public cloud, whereas keep the business critical information and the services in their private control [1]

G. **Community Cloud**: This cloud model is managed by a group of organizations which share the same interests. It can also be controlled by a third party [9].

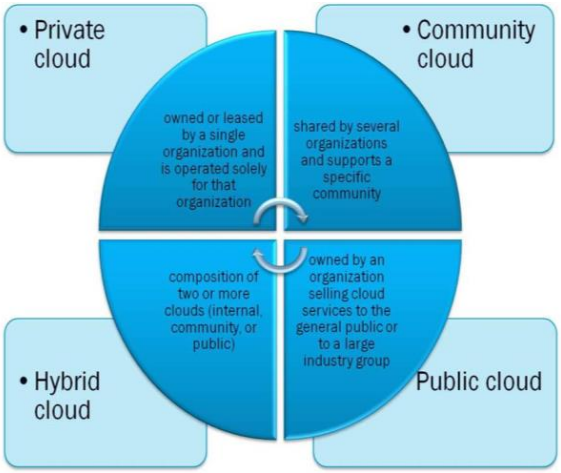



Figure 3. Cloud Deployment model

## III. SYSTEMATIC MAPPING

A. **Definition of Research and Primary Source**: As most of the Research papers are taken from IEEEXplore, so that's the primary source of my work. To start with, we searched for the work which was directly related to the Basics of Cloud Computing, and then moving towards the "Security Threats in Cloud Computing". The keywords which were used while searching for the reference material were: "risk", "threat", and "vulnerabilities". A total of almost 38 research publications were there out of which we choose the best 10 papers. Search string was not refined as there was a chance that many of the relevant research publications might have got excluded, so the Search String was left wide open.

B. **Inclusion Criteria**: The following inclusion criteria were considered at the time of considering the research papers:

- Cloud Computing Security was considered to be the main theme
- Only published (conferences/ journals) papers were considered.
- Papers published between the years 2000-2014 were taken.
- Future work, statistical data as well as if any sort of experiments have been conducted in the papers.

C. **Exclusion Criteria**

- The journals which weren't available online
- The papers which were not published
- Duplication of the material in the journals.
- Papers which didn't had detailed solution proposals.
- Papers that didn't had any sort of proposal of solution.

## IV. LITERATURE REVIEW

**Srinivas, J., et al. [1]** in this paper explores various concepts involved in cloud computing. Cloud is discussed from technical and service aspects and some of the opportunities in cloud computing have been highlighted. Figure: 4 Represents the graph which clearly depict the concerns of clients on cloud computing issues.

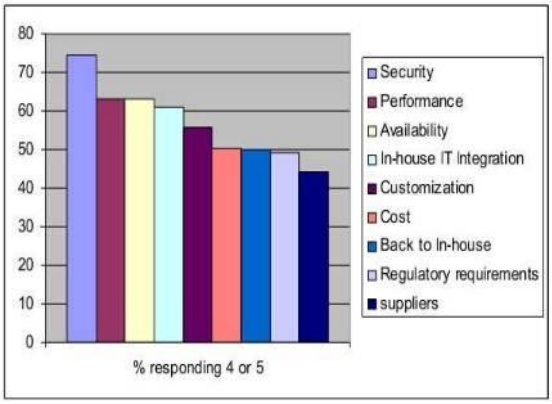



Figure 4. Graph depicting the concerns of clients on cloud computing issues. [1]

The most important question answered in this paper was "Why this technology must succeed". The issues related to cloud computing are discussed as well. The paper is focuses on the enhancement of the Cloud security. It emphasized on the problems, which needed to be fixed like security, load balancing, standardization. Issues such as Security, Performance, Availability, Customization, Cost etc. are discussed in this paper which will definitely be a hot spot for researchers in future.

The strength of their work is in giving a view about Cloud Computing and discussing how one can bring betterment in this era. The faced the limitation by not proposing any model or discussing any threat in detail, they have just covered the Basics. The report's conclusion comprises of Cloud being discussed from technology point of view. There are interesting technical problems to address and from consumer point of view there are essential usability, stability and reliability problems to solve. If the cloud providers are slow to provide safe, secure, reliable data storage and application services, they may miss one of the greatest opportunities of this century

**Sabahi, F [2]** talked about the cloud deployment strategies, delievery models and Cloud RAS (Reliability-Availability- Security) Issues. This paper is all about the cloud RAS Issues in which data Leakage is considered as one of the greatest organizational threats. In SaaS & PaaS DLP (Data Leakage Prevention) is impossible whereas in IaaS client could set in DLP agents for some control over data. The author focused on the DDoS Attacks which are considered to be the flood of packets sent to a web server from multiple sources.Firewalls are vulnerable against DDoS attack. DDoS is part of Network Virtualization layer rather than Server Virtualization. This paper provids a

solution against cloud "**Access Control**" concern. In SaaS and PaaS, the cloud provider is responsible for managing all aspects of network, customers should focus on access control to protect the information for example Authentication using one-time passwords.In IaaS, customers are entirely responsible for managing all aspects of access control to their resources in the cloud. The Strength of the paper is that they have covered RAS Issues and DDoS and proposed a solution against cloud security problem. Whereas the limitations of the paper is that they only focused on a single aspect and did not discovered any further threats. In the Concluding area the author mentioned that the Attacks, such as powerful DDoS attack , have no defense against them and hence it stops people from migrating to Cloud Computing.

**Shaikh, F. B. and S. Haider [3]** has summarized all the security and privacy issues, tools and models proposed against security threats , in a compare and contrast table and has critically analyzed the different security models and tools. A total of 11 Literature Reviews have been summarized with the: Context of Research, Problem Discussed,Technique Used and the Model/Tool Proposed. The claimed contributions of the paper was that Cloud computing is not fully mature and still lot needs to be explored. The strength of the paper was that the framework was clearly mentioned and the table , mentioned in the paper, which was covering all of the summarized reviews, saved a lot of time.Strength/Weakness of every threat was explicitly and mentioned clearly. The Limitation of the paper was that the authors haven't worked on any security standards they have just proposed the idea. In the conclusion section, the author came up with the inference that security is the biggest hurdle in the wide acceptance of cloud computing and he propose to use "Cloud Security Alliance " release of a new governance, risk management for cloud computing.

**Kumar, P. [4]** states that February 2010, Amazon Network Host Service, S3 (Simple Storage Service) was broken down for 4 hours , this AGAIN made people concerned about security of cloud computing. He mentioned the cloud Computing Service Models and the security threats in SaaS, PaaS and IaaS. There isn't any specific research problem that this paper is attempting to address and even no major contribution has been done by the author. Figure:5 Represents all of the security issues which are there in SaaS.

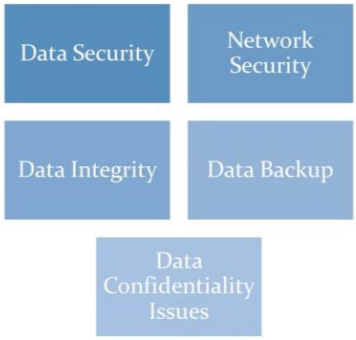



Figure 5. Security issues in SaaS

The strength of the paper is that it covered SaaS , PaaS & IaaS in detail whereas no specific model has been proposed so that's the limitation of the paper Authors haven't discussed any threat in detail in PaaS & IaaS so even that's a weakness of the paper. For offering good service, cloud computing service providers must avoid the threats such as Data security, Network security, Data integrity, Data Backup and Data confidentiality issues.

**Silva, C. M. R. d., et al [5],** aims to catalog studies confirming techniques to the security threats and risks in the cloud computing. This paper is all about the 7 threats which are distributed in 661 publications related to the security threats of cloud computing.

- **Threat#1** Abuse and Nefarious Use of Cloud Computing
- **Threat#2** Insecure Interfaces and APIs
- **Threat#3** Malicious Insiders
- **Threat#4** Shared Technology issues
- **Threat#5** Data Loss or Leakage
- **Threat#6** Accounts or service Hijacking
- **Threat#7** Unknown Risk Profile

Through the sysematic mapping, 661 publications were computed on this subject and it has been clearly recognized that the Threat#7: Unknown Risk Profile is basically the most explored threat in the literature with 377 publications. To minimize the threats, for achieving this goal, the authors have chosen , measure dispersion techniques such as SD (Standard Deviation) & CV (Coefficient of Variation) and came upto and sloution as showed in Figure:6

- CV <= 15% -> Homogeneous
- 16% < CV > 30% -> Medium Dispersion
- CV >= 31% -> Heterogeneous

| Threat | Mean | s | CV | Dispersion Type |
|---|---|---|---|---|
| #1 | 14.00 % | 2.07 % | 14.79 % | Homogeneous |
| #2 | 3.13 % | 3.64 % | 116.56 % | Heterogeneous |
| #3 | 0.88 % | 1.36 % | 154.99 % | Heterogeneous |
| #4 | 41.88 % | 10.23 % | 24.43 % | Average Dispersion |
| #5 | 15.63 % | 23.48 % | 150.25 % | Heterogeneous |
| #6 | 16.38 % | 22.58 % | 137.91 % | Heterogeneous |
| #7 | 47.13 % | 2.90 % | 6.15 % | Homogeneous |

Figure 6. Dispersion Parameters of Proposal Spread for Threats [5]

The author desire to help all those researchers who plan to recommend solutions to some of the problems which are coverd in this research paper. The strength of the paper is that it has clearly mentioned the Selection Criteria and Motivation which no other paper discussed.All threats discussed in other papers, were togetherly discussed in this paper and they even proposed a solution for these threats.No specific limitaion has been identified. In the conclusion part the solutions to the problems related to Threat # 2 , # 3 , # 5 , # 6 have Heterogeneous Variation.Threat # 1 and # 7 , the variation appeared in low dispersion.In Threat # 4 , the protocol identified as Medium Dispersion variation in proposed solutions.

**Sugumaran, M., et al [6],** in this paper benefits of cloud computing are highlighted along with the data

security issues which are related to the cloud services. Cloud computing supports the distributed service oriented architecture as well as the multi-user and multi-domain administrative system. So, that's why cloud computing is more susceptible to the security threats.This paper focuses on the techniques which were implemented for data protection. The strength of paper lies in the propsed architecture, that stores encrypted data in the cloud, using block cipher based cryptogography technique.This algorithm is efficient and secured.

**Behl, A [7]** described how cloud has redefined the the distributed computing. It has changed the entire concept which distributed computing (e.g Grid computing, server client computing) used to present. Despite of the fact, cloud computing provides huge number of benefits, it includes security threats which need to be resolved as the data in cloud needs to be protected in order to earn full benefit from it.This paper focuses on the cloud related security issues and talks about the existing approach to secure the infrastructure and the applications in order to remove the drawbacks. The strength of the paper is that they have discussed numerous security challenges in cloud specially the most critical ones and have given appropriate solutions for that. Limitation of the paper is that, it hasn't proposed any particular model as a solution. In the conclusion part the author tries to entail the whole research and then try to formulate the security strategy which will permit the cloud providers as well as the customers to fight contradiction of emerging security threats.

**Eken, H [8]** in this paper identifies major security threats related to the cloud computing which is a necessary part of all of the companies that are interested in cloud computing and want to use its services. The risk factors specifically related to the cloud are discussed in detail.The purpose of this study is totally anticipated to be a guide for all those who are engrossed in the cloud and want to take benefit from it. The strength of the paper is it's security threat solution deliverence. It's limitation is that it didn't discuss about any new innovation reated to the cloud computing.

**Kulkarni, G., et al [9],** the paper focuses on SaaS (Software as a Service), PaaS (Platform as a service), IaaS (Infrastructure as a service), and on the security threats and how can they be avoided to make this tecnology better as data privacy is one of the most challenging topic in research because of the user's and organization's confidential information being stored online and needs to be protected from unauthorized access. This paper presents a detailed analysis of cloud security issues by emphasisng on its types as well as its service delivery types. The strength of the paper is that it recommends the cloud computing established on various different encryption and decryption techniques from the storage service.The limitation of the paper is that neither they have used any sort of methadology nor they have propsed any model to avoid all the threats and issues they have mentioned in their paper. The author concludes the paper by identifying the major threats and summarizing everything by saying "Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future."

**Jamil, D. and H. Zaki [10],** talks about three main aspects of cloud computing and the popular types of cloud. The main theme of the paper is to highlight the threats in cloud which can be dangerous for it and discussing and providing possible solutions for them. Strength of the paper is that by giving an example realted to the Amazon Virtual Private cloud (VPC) , they showed a possible VPN in order to increase the cloud security and even discussed and presented a potential cloud computing firewall solution. Weakness of the paper is that , they haven't got into detail which was required for proposing a better solution. In the conclusion part the author discusses that cloud technology is still in its early days and created a hype with impressive results and feedbacks so far this will continue to grow.

## V. CRITICAL EVALUATION

Table1, shows feature wise & Table2 represents sloution oriented critical analysis of all the papers.

TABLE I. FEATURE-WISE CRITICAL ANALYSIS

| Authors Name | Srinivas, J., et al. | Sabahi, F | Shaikh, F. B. and S. Haider | Kumar, P. | Silva, C. M. R. d., et al | Sugumaran, M., et al | Behl, A | Eken, H | Kulkarni, G., et al | Jamil, D. and H. Zaki |
|---|---|---|---|---|---|---|---|---|---|---|
| Abuse & Nefarious use of Cloud Computing | | | | | ✓ | | | | | |
| Availability | ✓ | ✓ | | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Bandwidth | ✓ | | | | | | | | | |
| Cost | ✓ | | | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Data Backup | | | | ✓ | | ✓ | ✓ | ✓ | | |
| Data Client Trust | | | ✓ | | | | | | | |
| Data Confidentiality | | | | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Data Integrity | | | | ✓ | | ✓ | | ✓ | ✓ | ✓ |
| Data Leakage | | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | |
| Data Loss | | | ✓ | | ✓ | | ✓ | ✓ | ✓ | ✓ |
| DDoS attack | | ✓ | | | | ✓ | ✓ | | ✓ | ✓ |
| Hijacking of Account | | | | | ✓ | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Hijacking of Service | | | ✓ | | ✓ | | ✓ | | ✓ | ✓ |
| Hijacking of Sessions | | | ✓ | | | | | | ✓ | |
| Insecure Interfaces API's | | | | | ✓ | | | ✓ | | ✓ |
| Malicious Insiders | | | | | ✓ | | ✓ | | | |
| Malicious User | | | ✓ | | | | | | | |
| Network Security | | | | ✓ | | | | ✓ | ✓ | ✓ |
| Performance | ✓ | | | | | | ✓ | ✓ | ✓ | |
| Reliability | | ✓ | | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Security | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Shared Technology Issues | | | | | ✓ | | | ✓ | | |
| Unknown Risk Profile | | | | | ✓ | | ✓ | ✓ | ✓ | ✓ |
| User Authentication | | | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ |

TABLE II. SOLUTION-ORIENTED CRITICAL ANALYSIS

| Literature References | Context of Research | Model Proposed | Critical Analysis and Observation |
|---|---|---|---|
| **Srinivas, J., et al.** | Cloud Computing Basics | **NO** | Just the basics .. Only discussed the problems. |
| **Sabahi, F** | Cloud Computing Security Threats & Responses | **YES** Solution: Against cloud security problem | Only covered RAS issues and DDoS attacks |
| **Shaikh, F. B. and S. Haider** | Security Threats in Cloud Computing | **YES** Model: To use "Cloud Security Alliance " release of a new governance, risk management for cloud computing | Critical Analysis about the different security models and tools proposed. |
| **Kumar, P.** | Security Threats to Cloud Computing | **NO** | Covered SaaS , PaaS & IaaS in detail. |
| **Silva, C. M. R. d., et al** | Security Threats in Cloud Computing Models: Domains & Proposals | **YES** | Covered all threats |
| **Sugumaran, M., et al** | An Architecture for Data Security in Cloud Computing | **YES** Architecture: To store encrypted data in the cloud | Encrypted Data is stored with better speed using block based symmetric cryptography algorithm |
| **Behl, A** | Emerging Security Challenges in Cloud Computing | **NO** | Discussed security challenges |
| **Eken, H** | Security Threats and Solutions in Cloud Computing | **YES** Information Security solutions for enterprise and service providers for the cloud computing deployment | Discusses solutions for Enterprises and Cloud Hosting Providers related to the Data and Information Security |
| **Kulkarni, G., et al** | A Security Aspects in Cloud Computing | **NO** | Author's Primary focus was on SaaS, PaaS and IaaS, and the cloud related security threats |
| **Jamil, D. and H. Zaki** | Cloud Computing Security | Solution: Basic potential cloud computing firewall | Discussed Cloud Data Secuity referring to Amazon Virtual Private cloud (VPC) |

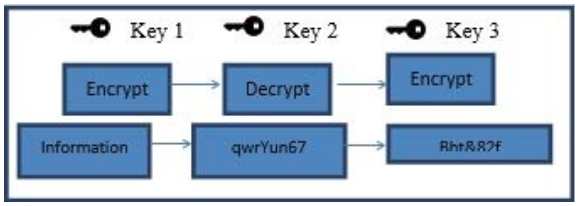
## VI. Proposed Solution

The technical winds of the current times are much advance than just a bunch of Tokens and Passwords. Everybody is talking about the QR (Quick Response) Codes. Ubiquitous little square that uses four standardized encoding modes (numeric, alphanumeric, byte / binary, and kanji) to efficiently store data.


Figture 7. QR Code

My proposed solution is the **Merger of "QR Codes" and "Triple Data Encryption Standards Algorithm"**.

Proposed Methodology: 3DES uses a three-key package say Key1, Key2 and Key3. My proposal is to use the personalized QR Code as the Key1, Combination of QR Code and an 8-digit passcode as Key2 and then again the QR Code and another 8-digit passcode as Key3.




Figture 8. Proposed Security Solution Mode

QR code is unique for every user of the world; hence the Keys will be unique as well and there will be a less chance of accessing the stored personal information.

3DES Encryption Algorithm is as follows:

***Cipher*** text = ***EKey3 (DKey2 (EKey1 (plaintext)))***

The above can be explained in layman terms as: The Application Encrypts the PlainText with Key1, it then decrypts the encrypted PlainText with Kay2, and then the final encryption is done using Key3.

Decryption is the reverse of encryption

***Plaintext = DKey1 (EKey2 (DKey3 (cipher text)))***

When the user creates his cloud account, the three key combinations will be stored in the database and nobody, not even the cloud owner will be able to see the data as it will be in the encrypted format.

Once the registration process is completed, cloud space will be allocated to the user carrying all the information encapsulated in the QR code – which will always be a unique username. The whole data (files, audio, video, images etc.) of the user is maintained securely in the provided space.

The security is maintained when the user download its files from the cloud. The downloaded file is available in the encrypted format. This secures the information from unauthorized access. If an unauthenticated user downloads the file, it can be seen in the encrypted form only and hence the precious data is not at stake. The authenticated user will be aware that the downloaded file needs to be decrypted using the same key and encryption algorithm, as implemented at the time of upload

## VII. Conclusion

Due to the rapid development in the field of Information Technology and Cloud Computing, Security Threats, to personal information, have earned priority. The challenges in privacy protection are sharing data while protecting personal information. This paper focuses on the safety issues of present cloud computing data security mechanisms and proposes an enhanced data security model for cloud computing to ensure security in each cloud layers. With the help this new security model, we can remove the security flaws of existing data security model in cloud environment and hence ensure the data security in cloud environment.

## Acknowledgment

The authors are thankful for the financial support from the research grant "Building Sustainable Knowledge Networks through Online Communities," Grant no. MYRG2015-00024-FST, offered by the University of Macau, FST, and RDAO.

## References

[1] Srinivas, J., et al. (2012). "Cloud Computing Basics." International Journal of Advanced Research in Computer and Communication Engineering, 1 (5).

[2] Sabahi, F. (2011). Cloud computing security threats and responses. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, IEEE.

[3] Shaikh, F. B. and S. Haider (2011). Security threats in cloud computing. Internet technology and secured transactions (ICITST), 2011 international conference for, IEEE.

[4] Kumar, P. "Security Threats to Cloud Computing."

[5] Silva, C. M. R. d., et al. (2013). Security Threats in Cloud Computing Models: Domains and Proposals. Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on, IEEE.

[6] Sugumaran, M., et al. (2014). An Architecture for Data Security in Cloud Computing. WCCCT, 2014 World Congress on, IEEE.

[7] Behl, A. (2011). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. WICT, 2011 World Congress on, IEEE.

[8] Eken, H. (2013). Security threats and solutions in cloud computing. WorldCIS, 2013 World Congress on, IEEE.

[9] Kulkarni, G., et al. (2012). A security aspects in cloud computing. ICSESS, 2012 IEEE 3rd International Conference on, IEEE.

[10] Jamil, D. and H. Zaki (2011). "CLOUD COMPUTING SECURITY." International Journal of Engineering Science & Technology 3(4).

[11] da Silva, C. M. R., et al. (2013). "Systematic Mapping Study On Security Threats in Cloud Computing." arXiv preprint arXiv:13