International Journal of Engineering Research & Management Technology ISSN: 2348-4039

May- 2015 Volume 2, Issue-3

Email: editor@ijermt.org www.ijermt.org

Cloud Security Issues, Challenges And Their Optimal Solutions

Vinay Kumar Pant
M.Tech. (CSE)
Subharti Institute of Technology and Engineering
Meerut, India

Mr. Anshuman Saurabh
Assistant Professor (CSE)
Subharti Institute of Technology and Engineering
Meerut, India

ABSTRACT—
Cloud computing is a new revolution of IT industry, that is improvement of Grid computing and Network Computing. It is a flexible, cost-effective, and modern way to delivery platform for business or consumer IT services over the Internet. The major concern of cloud computing to provide the services by using internet (web). Even with the potential gains achieved from the cloud computing, the industries or organizations are slow to adopting it, due to the security issues and challenges associated with it. However, cloud Computing deal with risk because essential services are often provided by outsource (third party), which makes it difficult to maintain cloud services related to shared resource, applications or data security and privacy. Different people provide the different view on cloud security. Some believe it is safe to use or some neglect the use of cloud services. Security is a major issue, which restricts the growth of cloud computing. This paper represents detail study and analysis of the cloud computing security issues and challenges with some simple method to secure cloud.
Keywords— Cloud computing, Security, SPI model (SASS, PASS, IASS), SLA (Service Level Agreement).

1. INTRODUCTION

The word cloud computing define as delivering host services over the web (internet). It provide to storing, accessing and sharing computer resources over internet, instead of local server or personal devices to handle application (programs). Some research defines cloud computing as a virtual server available over the internet. The word 'cloud computing' define as "A type of web (network) based computing" [1].

Cloud is an Internet based Service provided on-demand to a User who doesn't need to worry about implementation details or maintenance. In the last few years, cloud computing has grown, one of the fast growing area of the IT industry. The importance of Cloud Computing is increasing and it is receiving attention in the organizations and scientific communities.

Fig. 1. Simple view of cloud computing [1]

According to Gartner's study Cloud Computing consider as one of the most important technologies and with a better prospect in successive years by companies and organizations. Cloud Computing authorize universal, on-demand, appropriate network access to a shared computing resources (e.g., applications, servers, storage, and services) that can be expeditiously provisioned and absolved with minimal management effort or service provider interaction. The cloud has different architecture based on the services they provide. The data are organized at one centralized place called data centers, keeping a large size of data storage. That data processed using online servers. So, the customers have to trust the vendor on the availability as well as data security. The cloud enhances collaboration, agility, scalability, availability and ability to adapt to fluctuations according to request, potential and speed up development work for cost decrement through accomplished and optimized computing [2]. Even if there are so many benefits to opt Cloud Computing, there are also some limitation to adopt it. One of the most significant problem with cloud is security, followed by issues regarding compliance, privacy and legal matters. We divide security issue into two categories:-Security issue faced by provider (SASS, PASS, IASS related) and security issue faced by customers (organizations, companies and personal user who host applications and store data on cloud). Cloud Computing describes relatively a new computing model, there is a great deal of incertitude about how we put security at all levels (e.g., network, application, host, and data levels) and how applications security is drive to Cloud Computing [3]. According to IDC survey conducted by IT executives and business associates, the top issue in cloud computing is Security.

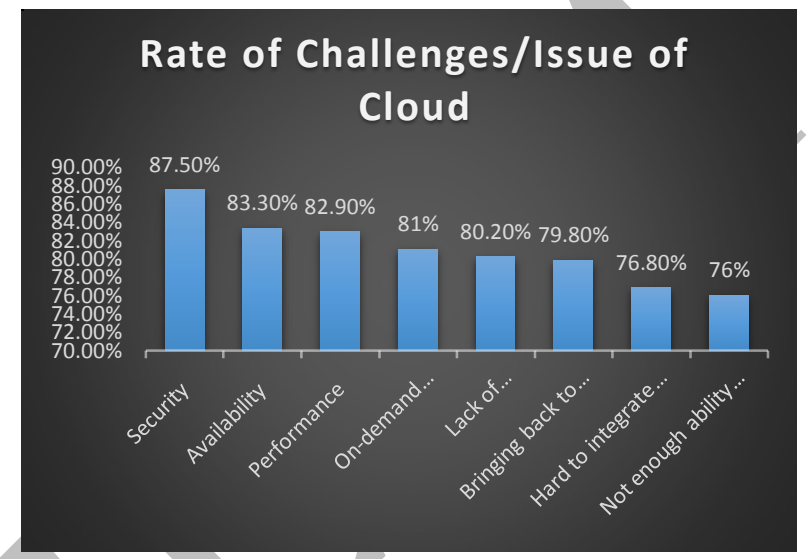

Fig. 2. Diagrammatic representation of IDC Enterprise panel report

We focus here to classified security issues for Cloud Computing according their reference model and identifying the main security challenges with cloud computing. We also work on some simple methods that help to solved security issue of cloud computing.

2. CLOUD REFERENCE MODEL

We study cloud model in two form. (1)- Cloud service model, (2) - Cloud deployment model.

2.1. Cloud service model[1, 4, 15]

Basically cloud computing has been consider as "Software-Platform-Infrastructure" (SPI) model. Cloud service model has following three types of services:

2.1.1. Software as a Service (SaaS)

SaaS model provide software application through internet services on the user demand. SaaS is an ultimate level of abstraction. The services are accessible from various client devices through a web browser (e.g., web email, office 360). Their service oriented architecture based on the web service technologies.

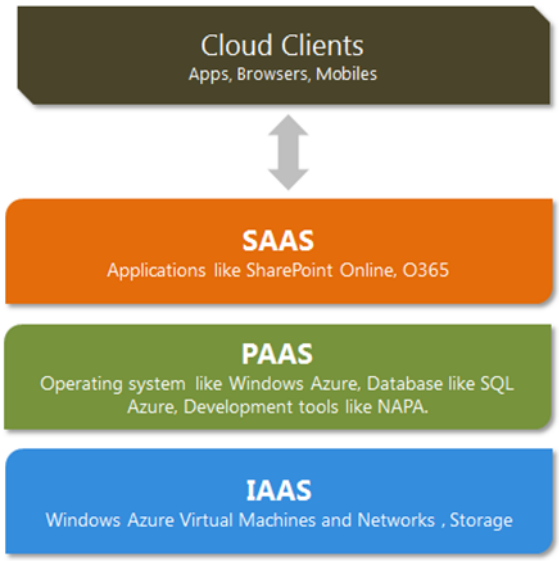

Fig. 3. Cloud Service Model [1]

2.1.2. Platform as a Service (PaaS)

PaaS provide an environment and platform to developers or programmer to build application and services over the web. It also allows user to create software applications using tools provide by provider. PaaS is a way to send hardware, Operating system, storage, and network capacity over the internet. Yet user does not control and manage the cloud infrastructure including server, O.S, or storage, but control over the deployed application on hosting environment.

2.1.3. Infrastructure as a Service (IaaS)

IaaS is the sometime refers as a hardware as a service (HaaS). IaaS service model denote to facilate out sourcing the equipment that help to user to perform operation (tasks), such as storage, hardware, servers and network components.

2.2. Cloud deployment model[1, 15]

Deployment model are define in following types.

2.1.4. Private cloud

Private cloud is operated and managed by a single company and provider. It is only accessible by a single organization, though managed internally or by a third-party, and it can be hosted internally or externally. Private model can improve the alllocation of resources, that allocate resource individually to organization or departments according their functionality on demand basis.

2.1.5. Public cloud

Public clouds model services are available for general use over the web. In which user don't need to purchase hardware, software and supporting infrastructure, all things managed and provide by provider. In public cloud no wasted of resources because user pay for per use. All the user of public cloud share the same infrastructure pool with limited configuration, availability variances and security protection. Ex. Amazon AWS

IJERMT

2.1.6. Hybrid cloud

Hybrid Clouds are a combination of two or more clouds (private, community or public).The goal is to combine services and data from a variety of cloud models to create a unified, automated, and well-managed computing environment. Ideally, the hybrid approach allows a business to take advantage of the scalability and cost-effectiveness.

2.1.7. Community cloud

This is a hybrid form of private clouds build and directed specifically for a targeted group. Community cloud is a multi-tenant cloud service model that is shared among several organizations and that is administered and secured commonly by all the participating institutions or a third party managed service providers.

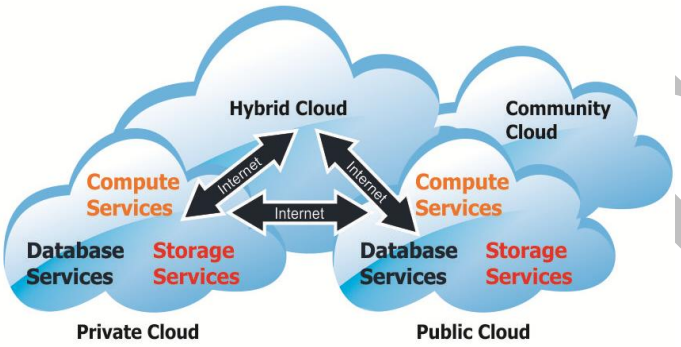

Fig. 4. Types of Deployment model [1].

3. SECURITY ISSUES WITH SOFTWARE-AS-A-SERVICE (SAAS)

SaaS provides application services on demand such as email, conferencing software, and business applications such as ERP, CRM, and SCM [5]. SaaS consumer has less control over security then other fundamental delivery models in the cloud. The use of SaaS applications is limited cause of security concerns.

3.1. Identity thefts and Access management issue

Managing identities and access control for enterprise applications one of the biggest challenges deal with IT industry today, according to research from the Cloud Security Alliance [2]. An enterprise may be able to leverage several cloud computing services without a good identity and access management strategy, in the long run dispersion an organization's identity services into the cloud is a necessary requirement for strategic use of on-demand computing services.

3.2. Data security issue

Data security is a common issue, but it becomes a major challenge when SaaS users have to rely on their providers for proper security [4]. The SaaS vendor is the one responsible for the security of the data until is being processed and stored [5]. Many cloud service providers provide very few details about their data centers and operations. Hence customer or user does not known about data security.

3.3. Accessibility issue

We access SaaS application anywhere, from any network device easily, including public computers and mobile devices. But most important things is internet connection, without internet we can't be able to access application. So we are fully dependent on web and are no longer access our application offline. Other thing is we use mobile devices that are not fully secure to access application. Some vulnerability found in the device OS and official applications that cause of hacking.

IJERMT

3.4. Application security issue

SaaS applications are typically delivered via the Internet through a Web browser. However, errors in web applications can create vulnerabilities for the SaaS services. Hackers have using the internet to understanding user's system and perform malicious activities such as steal sensitive data. Security challenges in SaaS applications are not different from any web application technology, but conventional security systems do not effectively protect it from attacks, so we need to new approaches for protection of application [4].

3.5. Multi-tenancy issue

Multi-tenancy is one of the major feature of cloud computing. As a result of multi-tenancy, multiple users can store their data in a single instance server using the applications provided by SaaS [6]. This is the approach where we use resources very efficiently but scalability is limited. Since data from multiple bearers is likely to be stored in the same database, the risk of data leakage between these bearers is high. We need to the some security policies that ensure one customer data are hold separate from other customers.

3.6. Cloud standards issue [1]

Cloud customer use various applications on cloud services, so compatibility between these services and applications are very important to stability and security. To manage the application and services we need a good Cloud standard organization. For keeping their customer, cloud venders introduce sticky services, which create difficulty for the customers if they want to swap from one provider to the other. In present a large numbers of standard councils are working with different interests, e.g. IEEE Cloud Computing Standard Study Group, Cloud Security Alliance (CSA), ITU Cloud Computing Focus Group, Open Cloud Consortium, Distributed Management Task Force, Storage Networking Industry Association, Open Grid Forum and Organization for the Advancement of Structured Information Standards, and so on. To promote the wide use of cloud computing, these standards bodies need to sit down and work together to establish common standards.

3.7. Backup issue

The traditional backup methods used with earlier applications and data centers, which were primarily designed for web and consumer applications, are not optimally designed for the applications running in the cloud. The SaaS vendor needs to ensure that all sensitive enterprise data is regularly backed up to facilitate quick recovery in case of disasters. Also the use of strong encryption schemes to protect the backup data is recommended to prevent accidental leakage of sensitive information.

4. PLATFORM-AS-A-SERVICE (PAAS) SECURITY ISSUES

PaaS facilitates deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers [4]. As with SaaS and IaaS, PaaS depends on a secure and reliable network and secure web browser. PaaS application security comprises two software layers: Security of the PaaS platform and Security of customer applications deployed on a PaaS platform [7]. PaaS providers are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications. PaaS also brings some security issues that are described as follows:

4.1. Resource Pooling and Rapid Elasticity issue [1]

Different types of hardware and software resources are integrated for efficient use in cloud environments. This heterogeneity may cause faults as security settings may differ for different kinds of resources. Information leakage is another problem caused by shared resources.

IJERMT

4.2. Development Life Cycle issue

In application development, developers face the complexity of building secure applications that may be hosted in the cloud. At the way where services and data will change or move in the cloud will affect both the System Development Life Cycle (SDLC) and security [8]. Developers have to keep in mind that PaaS applications should be upgraded frequently, so developers have to confirm that their application development processes are flexible and adequate with changes [9]. The Secure system development life cycle (SSDLC) is new till now and not widely used. Improper use of code and design rise the issue of insecure SSDLC.

4.3. Third-party relationships issue

Moreover, PaaS does not only provide traditional programming languages, but also does it offer third-party web services components such as mashups [7]. Combination of more than one source element into a single integrated unit are known as mashup. Mashup is one of the most critical security issues with PaaS models, for data and network security. PaaS customers are dependent on the web-hosted development tools and third-party services for the security of data and networks.

4.4. Underlying infrastructure security issue

In PaaS, developers do not have rights to access the main layers, so vender are responsible for protecting the underlying infrastructure and also the applications services [6]. Even when developers are responsible for the security of their applications, they do not have to belief that development tools provided by a PaaS vender are secure. Cloud server is used to store PaaS applications and user's data. The security of this data in time of processing, transferring and storing depends on the vendors.

5. INFRASTRUCTURE-AS-A-SERVICE (IAAS) SECURITY ISSUES

IaaS provides a number of resources such as servers, storage, networks and some other computing resources that are connected in the form of virtualized systems, they are accessed via the web [8]. Users are enable to run any software with full control and management on the resources allocated to them [10]. However, the underlying computation, network, and storage infrastructure is controlled by cloud providers. IaaS vendors put their sufficient effort to secure their systems in order to minimize threats that result from creation, communication, mobility, monitoring, and modification [11]. IaaS also deal with some security issues.

5.1. Access control and management issue

Most IaaS provider offers a basic firewall service, allowing the users to filter special Internet Protocol (IP) address ranges and specific port. Cloud vender provides default configuration which offering minimal access.

5.2. Data leakage protection and usage monitoring issue [1]

Data stored in an IaaS infrastructure in both public and private clouds needs to be monitored. We need to know who is accessing the information, how the information was accessed or what type of device, the location from which it was accessed, and what happened to that information after it was accessed? These are some critical issue that force to user thinks about the uses of cloud services.

5.3. Network monitoring issue

In IaaS model, providers are responsible for network monitoring to sustain acceptable level of QoS. The network monitoring involves a process that keeps track the status of troubleshooting, malicious activity and fault detection. In cloud, Network monitoring is not easy compared with traditional monitoring because cloud is geographically distributed and depends significantly on resources sharing [12].

IJERMT

5.4. Storage resources issue

IaaS provider perform important role to store user's data and providing resources [12]. Sometime companies use untrusted storage device that cause of data loss. Encryption would be a good Solution, but it might prevent the other user's accessibility to the data. Cloud have multi-tenancy feature, so provider need to provide encrypted key to every user. This approach increases traffic and degrade performance.

6. CLOUD COMPUTING SECURITY RISK AND CHALLENGES

6.1. Isolation failure

Shared resources and Multi-tenancy are characteristics of cloud computing. In this category we study the failure of procedure separating the usage of storage, routing, memory and even reputation between different tenants (e.g., guest-hopping attacks) [14].

6.2. Privileged user access [1,16]

Data process outside of organization is very risky work, because outside services bypass the physical, logical and personal control. So manage the application, user need administrative control upon the application. In cloud deployments, consumers necessarily give control to the cloud provider over a number of issues that may affect security.

6.3. Regulatory compliance [16]

However consumer is responsible for security of their data in back and front both end. Traditional service provides the external security certification. But cloud provider refuses this concept it provide the facilities to use their application and services. It is the responsibility of the cloud consumer to check that the cloud provider has valid certifications or not. It is also important for the cloud user to be knows about the division of security responsibilities between the consumer and the provider. Service level agreements (SLA) in a cloud may not take a responsibility to provide such capabilities on the part of the cloud provider, thus leaving gaps in security defenses.

6.4. Malicious behaviour of insiders

Damage caused by the malicious actions of insiders (person) working within an organization that compromises information confidentiality, integrity or availability. Differences may arises due to trust between insider and their organization. The problem related to insider attack (security) in cloud environment occur within either or both the consumer organization and the provider organization.

6.5. Vendor lock-in [14]

In this technique the consumer dependent on vendor services. The user want independence to move their application and data from one provider to another, but these services does not support portability of applications and data to other vendors that increase the risk of data and service unavailability. Thus customers are effectively prevented from swapping and integrating to alternate vendors.

6.6. Data protection

Cloud computing poses several data protection challenges for cloud consumers and providers. In case of data security we face different risk related to data integrity, data stealing, data location, or data loss. The exposure or prevention of sensitive data is more important, but it also concerns damage or unavailability of data. In some cases, it may be difficult for the cloud consumer to effectively check the data proceeding services of the cloud provider and thus indeed that the data is handled in a secure way [14].

IJERMT

6.7. Management interface vulnerability

Consumer management interfaces of a public cloud provider are usually accessible through the Internet and mediate access to larger sets of resources than traditional hosting providers. And this situation increased risk, especially when we combined remote access and web browser vulnerabilities.

6.8. Service unavailability

This could be caused by a host of factors, from software (Application) or equipment failures in the vender's data center, from error of the communications between the consumer systems and the provider services.

7. SOLUTION OF SECURITY ISSUES

Cloud security architecture is powerful only when we use specific method or policy to according their architecture. We systematically analyze cloud security issues, challenges and risk. For each malware and threat, we identify which cloud service model or models are affected by these security problems. There is some simple way or method, which help to secure cloud.

7.1. Identity and access management guidance

CSA (Cloud Security Alliance) is a non-profit organization that promotes the use of best practices in order to provide security in cloud environments. CSA has issued an Identity and Access Management Guidance which provides a list of recommended best practiced to assure identities and secure access management [2]. This report comprise user access certifications, identity management, centralized directory, access management, role-based access control, privileged user and access management, separation of duties, and identity and access reporting.

7.2. Digital signatures

Digital signature is a technique use to validate authentication and integrity of data and software. Many researchers propose to secure data using digital signature with RSA algorithm while data is being transferred over the Internet. Researcher gives advice to use RSA that is very recognizable algorithm and it be able to protect data in cloud environments.

7.3. Use of Encryption Technique

Encryption techniques are used form a long time to secure sensitive data. Software developers need to develop the application that provides encrypted data for the security. We will ensure that data is secure when it is encrypted in time of Sending or storing in the cloud. We have some well-known encryption techniques such as Advanced Encryption Standard (AES). Also, SSL technology can be used to protect data on cloud [16].

7.4. Virtual network security

A virtual network framework to protect the communication between virtual machines presents by Wu and et al. [13]. This framework proposed two configuration variants (“bridged” and “routed”) for virtual networks which is based on Xen. Most of virtual network models are consists three layers: firewall, shared networks and routing layers, which can prevent VMs from sniffing and spoofing.

7.5. Proper understanding of SLAs (Service Level Agreements)

In cloud computing all services like software application, storage, hardware and networking are provided by third party provider using web. So trust between customer and provider is necessary. Service level agreement represent agreement between the service provider and the service user in term of scope, quality and responsibilities [1]. The performance level must be observed regularly by the both sides. According to SLA every provider and user having some responsibility that is necessary to follow to secure cloud.

IJERMT

7.6. Recovery Facilities

Cloud providers should provide good recovery facilities. Hence data are fragmented or lost due to any disaster, they can be recovered and continuity of data can be managed as well as [16].

7.7. Use of Better Enterprise Infrastructure

Enterprise must have infrastructure which facilitates installation and configuration of hardware resources such as routers, servers, proxy servers, firewalls and software like operating system and so many [16]. We need an infrastructure who prevents malicious activity and cyber-attacks.

7.8. Control the consumer access devices

The consumer's access devices or points such as Personal Computers, virtual terminals and mobile phones should be secure. The damage of server and an endpoint access device by an unauthorized user can cancel even the best security protocols use in the cloud. Be sure that the user computing devices are managed properly and secured from malware functioning and supporting advanced authentication features.

CONCLUSION

Cloud Computing is a new concept that presents number of benefits for its users. However it also raises some security problems, which may slow down its progress. Understanding of vulnerabilities in Cloud will help organizations to move towards the Cloud. We have described security issues for cloud models: SaaS, PaaS, and IaaS, which vary depending on the model. This paper also describe the security risk and challenges which held the progress of cloud computing. Here we distinctly study security issue with cloud service models and challenges associated with provider and user in cloud computing. Also, discus some solution methods, that help to secure cloud. We need some new security techniques and redesigned traditional techniques that can work with cloud architectures. Every organization, who use cloud (online) services their first question about security of information (data), application or infrastructure that provided by venders. We have discuss every point of view of security. This paper may help service provider and customer to understanding security issue and challenges associated with cloud computing. It also provide the information about their optimal solution that help to secure the cloud.

REFERENCES

1. WWW.WIKIPEDIA.ORG/WIKI/CLOUD_COMPUTING/(WEBOPEDIA)
2. Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0.. Available:https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf website
3. Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. Future Internet 4(2):469-487
4. Subashini S, Kavitha V (2011). A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 34(1):1-11
5. Ju J, Wang Y, Fu J, Wu J, Lin Z (2010) Research on Key Technology in SaaS. In: International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), Hangzhou, China. Washington, DC, USA: IEEE Computer Society. pp 384-387
6. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez1 (2013) An analysis of security issues for cloud computing. In: Journal of Internet Services and Applications.
7. Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. Sebastopol, CA: O'Reilly Media, Inc..
8. Morsy MA, Grundy J, Müller I (2010) An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop. Sydney, Australia: APSEC.
9. Ertaul L, Singhal S, Gökay S (2010) Security challenges in Cloud Computing. In: Proceedings of the 2010 International conference on Security and Management SAM'10. Las Vegas, US: CSREA Press. pp 36-42
10. Dahbur K, Mohammad B, Tarakji AB (2011) A survey of risks, threats and vulnerabilities in Cloud Computing. In: Proceedings of the 2011 International conference on intelligent semantic Web-services and applications. Jordan: Amman. pp 1-6

IJERMT

11. Dawoud W, Takouna I, Meinel C (2010) Infrastructure as a service security: Challenges and solutions. In: the 7th International Conference on Informatics and Systems (INFOS), Potsdam, Germany. Washington, DC, USA: IEEE Computer Society. pp 1-8
12. Wesam Dawoud, Ibrahim Takouna, Christoph Meinel (2012)- Infrastructure as a Service Security: Challenges and Solutions.In: International Journal of Advanced Research in Computer Science and Software Engineering(ijarcsse).
13. Wu H, Ding Y, Winer C, Yao L (2010) Network Security for virtual machine in Cloud Computing. In: 5th International conference on computer sciences and convergence information technology (ICCIT). DC, USA: IEEE Computer Society Washington. pp 18-21
14. Security for Cloud Computing (2012) by Cloud Standards Customer Council
15. Mell P, Grance T (2011) The NIST definition of Cloud Computing. Gaithersburg, MD: NIST, Special Publication 800–145.
16. Pradeep Kumar Tiwari, Dr. Bharat Mishra (2012) Cloud Computing Security Issues, Challenges and Solution. In: International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 8, August 2012).

IJERMT