Volume: 2 Issue: XII Month of publication: December 2014

DOI:

www.ijraset.com Volume 2 Issue XII, December 2014
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Confidentiality for cloud computing

Vibha Sahu[1], Praveen Shrivastav[2,], Dipti Chhatri[3] ,Dr. S.M. Ghosh[4]
[1,2,3] PHD Scholar, [4]Asso.Prof. [1,2]Dr. C.V. Raman University, Bilaspur, India
[3,4] Rungta College Of Engineering & Technology, Bhilai, C.G., India

Abstract: Cloud computing is a computing paradigm that involves outsourcing of computing resources with the capabilities of expendable resource scalability, on -demand provisioning with little or no sincere IT infrastructure investment costs. This paper discusses to which degree this is justified, by presenting the Cloud Computing Confidentiality Model (CCCM). The CCCM is a step-by-step model that creates mapping from data sensitivity onto the most suitable cloud computing architecture. To achieve this, the CCCM determines first of all the security mechanisms required for each data sensitivity level, secondly which of these security controls may not be supported in certain computing environments, and finally which solutions can be used to manage with the identified security limitations of cloud computing. The most systematic security controls needed to protect the most sensitive data may not be guaranteed in public cloud computing architectures, while they can be realized in private cloud computing architectures. In this thesis I Suggests hybrid cloud model.

Keywords: cloud computing, cloud model, problems, confidentiality, security.

I. INTRODUCTION

Cloud computing is a new term in the computing world. Cloud computing is the collective term for a group of IT technologies which in collaboration are changing the landscape of how IT services are provided, accessed and paid for. Definition of cloud computing is (NIST 2009a)- " Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

A. *Cloud service models*

1) *Software-as-a-Service (SaaS):* The SaaS service model offers the services as applications to the consumer, using standardized interfaces. The consumer can only control some of the user-specific application configuration settings.
2) *Platform-as-a-Service (PaaS):* The PaaS service model offers the services as operation and development platforms to the consumer. "The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations"
3) *Infrastructure-as-a-Service (IaaS):* The IaaS service model offer infrastructure resources as a

service, such as raw data storage, processing power and network capacity. The consumer can use IaaS based service offerings to deploy his own operating Systems and applications. "The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components.

B. *Cloud deployment models*

1) *Public clouds:* In public cloud computing the infrastructure is located on the premises of the provider, who also owns and manages the cloud infrastructure. Public cloud users are considered to be untrusted, which means they are not tied to the organization as employees and that the user has no contractual agreements with the provider.
2) *Private clouds:* Private clouds run in service of a single organization, where resources are not shared by other entities. Private cloud users are considered as trusted by the organization, in which they are either employees, or have contractual agreements with the organization.
3) *Hybrid clouds:* Hybrid clouds are a combination of public, private clouds. Hybrid clouds leverage the capabilities of each cloud deployment model. Each part of a hybrid cloud is connected to the other by a gateway, controlling the applications and data that flow from each part to the other. Where private and public clouds are managed, owned, and located on *either* organization *or* third party provider side per characteristic. The users of hybrid clouds can be considered as trusted and untrusted. Untrusted

users are prevented to access the resources of the private and community parts of the hybrid cloud.

II. PURPOSE OF RESEARCH

Many organizations are uncomfortable with the idea of having their data and applications on systems they do not control. There is a lack of knowledge on how cloud computing impacts the confidentiality of data stored, processed and transmitted in cloud computing environments. The goal of this thesis is to create a Model that clarifies the impact of cloud computing on confidentiality preservation, by making stepwise recommendations on;

How data can classified on confidentiality

How data classifications relate to the security controls needed to preserve the confidentiality of data

How the process of security control selection is negatively influenced in cloud computing environments

How to cope with the negative influences of cloud computing on the protection of data confidentiality

We know how the current processes of IT risk management, data & system classification, and security control selection; will identify security problems in cloud environments. With the identified security problems, the CCCF presents a mapping from data classifications to appropriate cloud architectures, and show how the security problems can be anticipated.

III. CLOUD COMPUTING CONFIDENTIALITY MODEL

we will present the Cloud Computing Confidentiality Model (CCCM), which will enable companies to review the possibilities to engage in cloud based services, based on the confidentiality of the data used within the company.

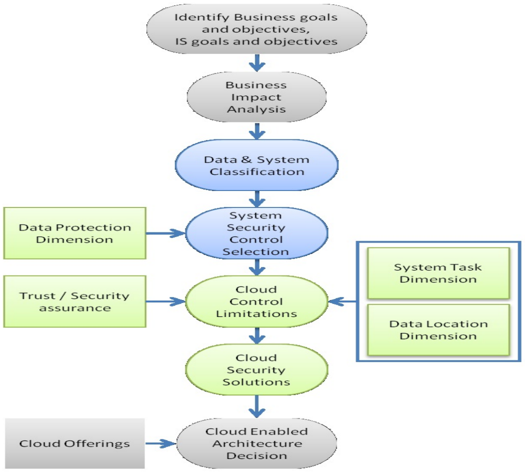

Identify Business goals and objectives, IS goals and objectives
Business Impact Analysis
Data & System Classification
Data Protection Dimension
System Security Control Selection
System Task Dimension
Trust / Security assurance
Cloud Control Limitations
Data Location Dimension
Cloud Security Solutions
Cloud Offerings
Cloud Enabled Architecture Decision

Figure: Cloud Computing Confidentiality Model

The goal of the model is to explain the differences between security in cloud computing environments, and the security in present-day information security practices. The gray boxes are described strategic goals of the business. They are considered to be outside the scope of this research because these processes have no direct relation to cloud computing and are identical in both cloud environments and traditional environments. The blue boxes represent the present-day information security practices, in the form of recommendations concerning data classification and control selection. The green rectangles represent important variables in our Model. These variables either have their effect on the control selection or on identification of cloud control limitations. The possible solutions for the cloud control limitations will be presented in Cloud security solutions. We will present the limitations, which spanned multiple baseline and optional controls. It is important to abstract from limitations on the technical security control level, present the common problems on a higher level.

A. Data & system classification

The main step in our framework is the classification of data and the information systems handling the data. The goal of the classification process is to identify *what* needs to be secured and *how valuable* the data and information systems are. When the data and systems are classified, the appropriate security controls can be selected to protect these assets. The process in the security categorization is to select the security impact levels for the identified information types. "The provisional impact levels are the original impact levels assigned to the security objectives of an information type before any adjustments are made" (NIST 2008a). Impact levels for information types range from *Not Applicable* to *High*.

SECURITY OBJECTIVE	**POTENTIAL IMPACT**		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table: FIPS 199 Categorization of Federal Information and Information Systems on confidentiality (NIST 2004a)

There are a wide range of other factors that may influence the overall system security confidentiality impact level. These factors are:

1) *Aggregation:* Aggregated information can be more sensitive than every piece of information in isolation.

2) *Critical system functionality:* Although a system compromise may be low impact in isolation, dependencies of other systems on the compromised system may have exacerbating effect on overall system impact.

3) Privacy information: When a system handles information that is protected by privacy regulations, such as Personal Identifiable Information (PII), system security categorization must be adjusted accordingly. The confidentiality impact level should generally fall in the *moderate* level.

4) *Trade Secrets:* There are several laws in the United States that prohibit the unauthorized disclosure of trade secrets. Systems that store, process or communicate trade secrets should generally be assigned at least a *moderate* level of confidentiality impact level.

B. System security control selection

The control selection procedure described in this section is based on the NIST SP 800-53, which recommends security controls for Federal Organizations in the USA (NIST 2009b). Security controls, when used correctly, can prevent, limit or deter threat-source damage to organization. Security controls can be placed into three classes:

1) *Technical security controls:* Technical controls can be used to protect against specific types of threats. These controls can range from simple to complex measures and consist of a mix of software, hardware and firmware. Next to standalone controls, technical controls also support the management and operational controls described below.

2) *Management security controls:* Management security controls are implemented to manage and reduce risks for the organization and to protect an organization's mission. Management security controls can be considered of the highest level of controls, focusing on the stipulation of policies, standards and guidelines, which are carried out by operational procedures to fulfill the organization's goals and missions.

3) *Operational security controls:* Operational security controls are used to correct operational deficiencies that might be exploited by potential attackers. These controls are implemented following good industry practices and a base set of requirements in the form of technical controls. Physical protection procedures and mechanisms are examples of operational security controls.

4) *Cloud control limitations:* This presentation will discuss these problems on a more general level. This generalized level is interesting for readers who are not that interested in problems on the control level, but who want to understand what the more general security issues are on cloud computing, when cloud computing is looked upon from a confidentiality point of view. This generalization of limitations is depicted.

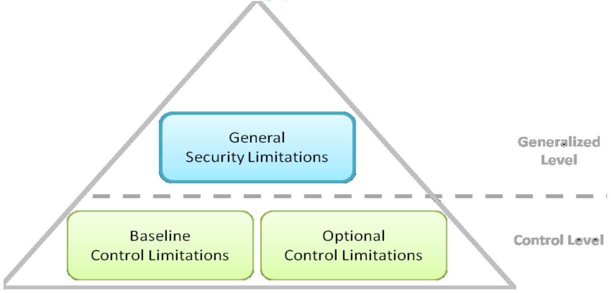


Figure: Control limitation generalization

We identified three problem areas that have their roots in multiple technical controls, and deserve further attention. These three problem areas are:

C. Access related limitations

The first problem area we want to discuss, are the access limitations that occur when the information systems are placed in a cloud computing environment. A very important distinction is the difference between accesses by external or internal networks. If the infrastructure used to access an information system, is not under the control of the information system owner, the security of the transmissions over such infrastructure cannot be guaranteed and as such, it is marked as an external network. There are three options available:

Prohibit access to information systems with Moderate or High impact levels and only allow access to Low impact information systems.

Facilitate encryption to protect the confidentiality and integrity of the information transmitted.

Facilitate the implementation of Virtual Private Network (VPN) technology that not only protects the confidentiality and integrity of the transmissions, but also requires organization controlled end-points of the connection.

These options have a very restrictive manner; both moderate and high impact systems are prohibited, or this requirement produces no limitation on the final answer. The central issue in cloud computing security is the amount of support for encryption and whether both end-points are organization controlled or not. This leads us to the following access related limitation: If the cloud service is accessed via external networks, and no transmission encryption is supported, then cloud computing is limited to low impact and public access systems**.**

D. Security assurance limitations

If organizations want to use information systems hosted by a cloud provider, they want “the assurance that the risk from using the external systems is at an acceptable level, which depends on the level of *trust* the organization places in the external service provider” (NIST 2009b). The level of trust can depend on two factors:

The degree of direct control an organization has on the external provider with regard to the employment of security controls and the effectiveness of these controls.

The security assurance that selected security controls are implemented and are effective in use.

The degree of direct control is traditionally established in the service level agreement with the service provider. The other factor that creates trust of an organization in the security of a system is security assurance, which is the confidence that security controls implemented in an information system are effective in their operation. Organizations interested in cloud services should place security assurance requirements on cloud service providers in order to gain trust in the cloud provider.

E. System separation limitations

The usage of virtualization in cloud computing makes it possible to run development and production systems on the same physical system, while logical separation is performed on the host level in domains. The interesting result of the introduction of virtualization in cloud computing is that demanding physical separation is not as standard as it is in traditional systems. When the NIST recommendations on physical separation of systems and/or components are used as guideline in a cloud environment, there are two options available:

Demand physical separation of systems by the cloud provider. Although physical separation of systems is not part of the standard offerings of cloud providers, the customer demands that the cloud provider supports and implements physical separation of the systems of the costumer. This requirement does involve the security assurance problems described earlier in this subsection, with the possibility that the provider is unwilling or unable to support the physical separation of systems.

Denote the physical separation requirement as obsolete. The required physical separation of systems was designed as a security mechanism in a time it was not perceived that virtualization would become so popular and influential. As a result, recommendations such as physical separation can be seen as standards and regulations that are out of date and not realistic with respect to the fast-paced developments in science and technology.

IV. CLOUD SECURITY SOLUTIONS

In the previous section we discussed the limitations that arise within the security controls and on a more general level, when an information system is hosted in a cloud environment. The goal of this section is to describe the solutions and choices available to either counter these limitations, or accept the limitations. Private clouds are considered to be in the data owner sphere, where there is full control by organization on how the data belonging to the organization is handled. Public cloud can be placed in the joint and recipient sphere, where there may be some, or no control at all. This perception is depicted in Figure:

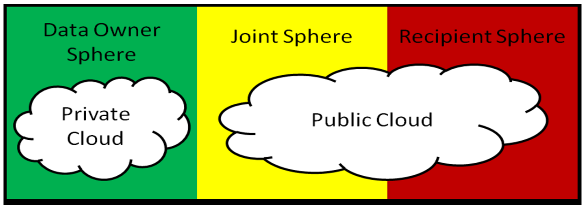


Figure: The common perception of cloud computing

If the additional controls demanded by the organization can be implemented by the cloud provider, the public cloud environment of the provider meets the security requirements set by the organization. In this case, "Public cloud" may be a confusing term, because public is often associated with public access while that is strictly controlled now by both the cloud provider and the organization owning the data.

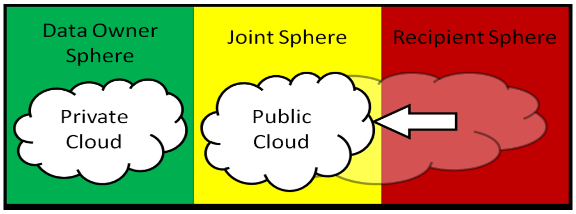


Figure: Perception of public cloud when meeting the security requirements of the data owner

However, if the security gap between what controls the organization requires and what the cloud provider supports cannot be closed by additional controls or supplementing controls, the risk involved must be mitigated by other ways than via contractual agreements.

V. CONCLUSION

Cloud security includes many old and well-known issues – such as network and other infrastructural vulnerabilities, user access, authentication and privacy – and also new concerns derived from new technologies adopted to offer the sufficient resources (mainly virtualized ones), services and auxiliary tools. We use the NIST standards and recommendations as main source of classification and security requirements information. The data classification used in this research project consists of three security objectives and three or four impact levels. The three security objectives are Confidentiality, Integrity, and Availability (CIA), while the impact levels of the data to organizations are High, Moderate, or Low. The confidentiality security objective of data can have the fourth impact level Not Applicable, which relates to no impact to the organization and as such, there is no need for protection of this class of data. The impact level of the whole information system dictates the baseline set of security controls that protect the system. Cloud architectures can be categorized by either the service model or the deployment model.

The service models defined in this thesis are Software-as-a-Service, Platform-of-a-Service, and Infrastructure-as-a-Service, depending on which level of the technology stack the cloud service is offered. The service models are not used in this research. Cloud environments can also be categorized with the deployment model, which describes first of all which party owns the infrastructure, secondly which party manages the infrastructure, and finally at whose location the infrastructure is located.

The security controls implemented in each deployment model differ per cloud provider. The most common cloud deployment models - private and public clouds - are often described with respect to which side of the organization's protective boundary they are. Private clouds are inside the organization's boundary (on-premise), while public clouds are seen as outside the organization's boundary (off-premise).

Construct the Cloud Computing Confidentiality Model (CCCM, see chapter 3), which is a step-by-step Model that creates the mapping from data to the most suitable cloud architecture as computing environment. This Model determines which security is required by the data, which security cannot be guaranteed in which computing environments and which solutions are available for these shortcomings, via the following steps:

A. Identify the information systems used within the organization

B. Identify the data types used in each information system

C. Classify the data types and use the data classifications to classify the information system

D. Select and tailor the security controls, based on the classification of the information system

E. Identify the problems that occur when these security controls are required in cloud computing environments

F. Identify the cloud environment that supports the required security controls and/or copes with the limitations identified in step 5.

VI. RESULTS

The security controls needed to protect data and information systems, have limitations when applied in external cloud environments. Some of these security control limitations are the foundation of the following three major problem areas:

Information systems classified as moderate or high impact level, require extensive security controls that may not be part of the standard set of controls supported by the cloud provider. This lack of supported controls limits the possible information systems that can be run on external computing environments such as public clouds.

Cloud providers have problems gaining the trust of potential customers, because providers are very reluctant in offering customized security plans, and do not offer detailed information on how the security plans are exactly implemented. On the other hand, customers demand provider transparency on security before they denote a service offering as trustworthy and usable.

Security controls exist that require a physical separation of information systems and component, while the focus of cloud computing is on virtual usage of infrastructure, systems and data. It is unclear to which degree public cloud providers support the physical separation requirements.

If the public cloud provider can comply with the security requirements of the data owner, the public cloud is considered to be in joint control of both the cloud provider and the data owner. This is the most ideal situation, in which none of the above security limitations exist.

VII. FUTURE SCOPE

Security is a crucial aspect for providing a reliable environment and then enables the use of applications in the cloud and for moving data and business processes to virtualized infrastructures.

Only technical security controls were analyzed in this thesis. In future research on the topic of confidentiality preservation in cloud computing, the Cloud Computing Confidentiality Model presented in this thesis can be extended by adding the analysis of operational and management security controls. Such an investigation could lead to supplemental controls for limitations that might occur in cloud computing environments.

As discussed in the previous section, *hybrid* cloud computing is a very promising cloud deployment model that can cope with the security limitations occurring in a public cloud environment, while still being able to support many of the economical advantages of public cloud computing. Hybrid clouds depend heavily on the gateway between the private part of the hybrid cloud and the public part of the hybrid cloud. The gateway between the private and public parts of a hybrid cloud is a interesting point for further research. To make this deployment model successful, the following research areas presented as further research:

The gateway must prevent information systems and data to flow from the private part to the public part, if the security for those systems and data cannot be guaranteed by the public cloud part provider. It is possible that automated information flow enforcement, in combination with security attributes on data and information systems, is a vital security control combination for a secured gateway. Internet bandwidth may become the major bottleneck for the hybrid cloud deployment model. Internet bandwidth does not grow exponentially like computing power and storage space, which is known as Nielsen‟s Law (Nielsen 1998). Further research is needed on the impact of this bottleneck and the optimization of data transfers via the hybrid cloud gateway.

REFERENCES

[1] Bardin, J., Callas, J., Chaput, S., Fusco, P., Gilbert, F. et al. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing v2.1, Retrieved January 28, 2010, from Cloud Security Alliance, from http://www.cloudsecurityalliance.org/guidance/

[2] Gartner (2008). Assessing the Security Risks of Cloud Computing, Retrieved December 5, 2009, http://www.gartner.com/DisplayDocument?

[3] Grandison, T., Bilger, M., O'Connor, L., Graf, M., Swimmer, M. et al. (2007). Elevating the Discussion on Security Management: The Data Centric Paradigm. In Proceedings of *2nd IEEE/IFIP International Workshop*, 84-93.

[4] Hoff, C. (2009). Incomplete Thought: The Crushing Costs of Complying With Cloud Customer “Right To Audit” Clauses. *Rational Survivability*, Retrieved September 20, 2009, from http://www.rationalsurvivability.com/blog/?p=877.

[5] NIST. (2004a). FIPS 199: Standards for Security Categorization of Federal Information and Information Systems. Retrieved August 28, 2009, from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

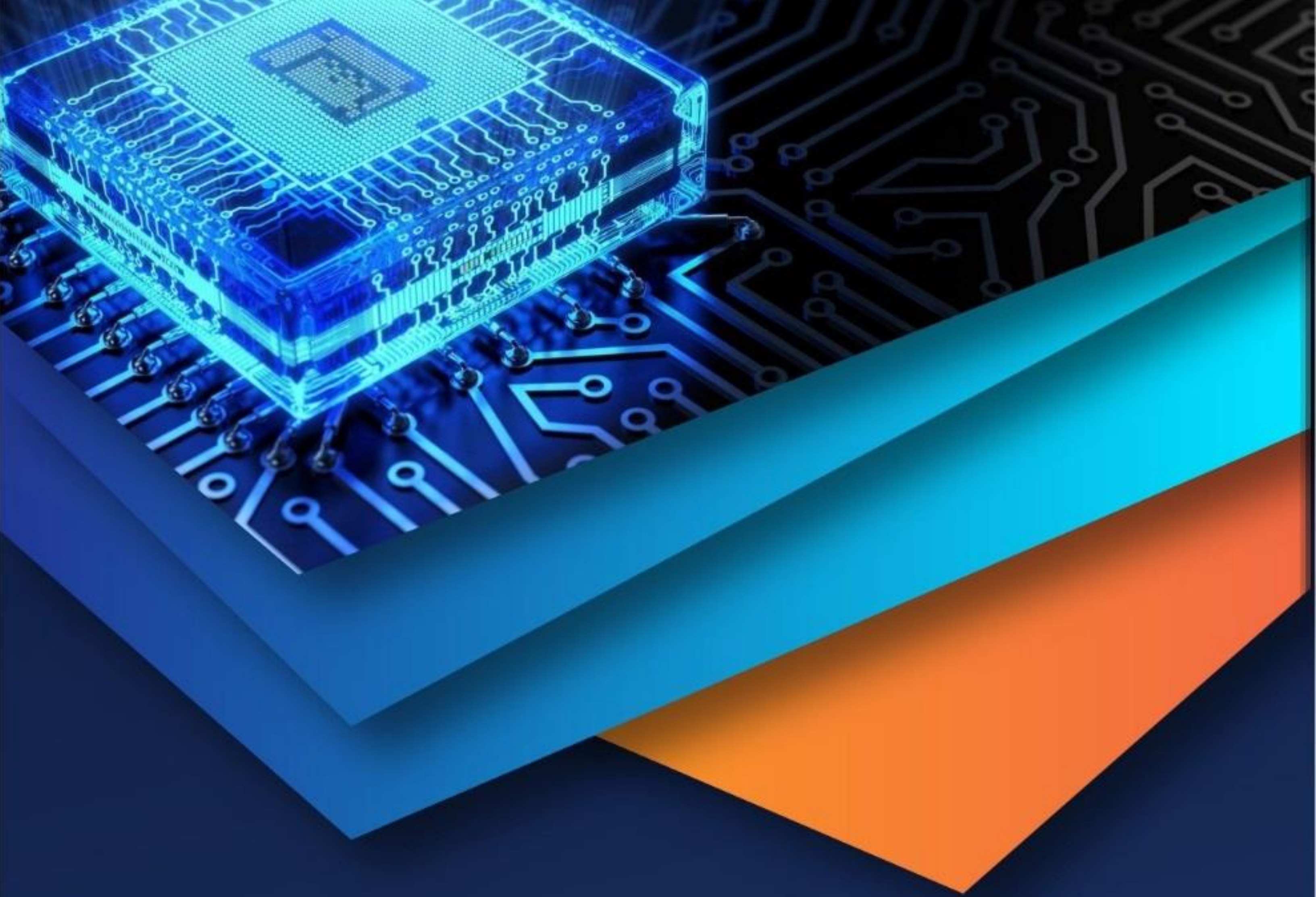
[6] NIST. (2004b). Guide for the Security Certification and Accreditation of Federal Information Systems, SP 800-37. Retrieved January 30, 2010, from http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf.

[7] NIST. (2006). FIPS 200: Minimum Security Requirements for Federal Information and Information Systems. Retrieved December 1, 2009, from http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

[8] NIST. (2008a). Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I, SP 800-60 Rev. 1. Retrieved August 27, 2009, from http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf.

[9] NIST. (2008c). Guide for Assessing the Security Controls in Federal Information Systems, SP 800-53A. Retrieved November 11, 2009, from http://csrc.nist.gov/publications/PubsSPs.html.

[10] NIST. (2009). National Institute of Standards and Technology, main website. from http://www.nist.gov.NIST. (2009a). NIST Working Definition of Cloud Computing v15. Retrieved October 7, 2009, from http://csrc.nist.gov/groups/SNS/cloud-computing/index.html.



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY