iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IX **Month of publication:** September 2023

DOI: https://doi.org/10.22214/ijraset.2023.55721

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IX Sep 2023- Available at www.ijraset.com

A Comprehensive Research Study on Cloud Security

Devanshi Bhatt[1], Ishika Desai[2], Kunal Parekh[3]
Department of Computer Science & Engineering, Charotar University of Science & Technology

Abstract: ***With the aid of a significant quantity of virtual storage, cloud computing delivers on-demand services through the Internet. The key advantages of cloud computing are that the customer does not need to build up costly computer equipment and that the cost of its services is lower. Cloud computing has been integrating with the industry and many other fields in recent years, which has encouraged researchers to do research on new related technologies. Individual users and enterprises migrate their applications, data, and services to the cloud storage server due to the availability of its services and scalability for computing activities. Regardless of its benefits, the shift from local to remote computing has created a slew of security risks and hurdles for both consumers and providers. Many cloud services are delivered by a trusted third party, posing additional security risks. The cloud provider offers its services through the Internet and employs several online technologies, which raise new security concerns. This article explored the fundamentals of cloud computing, as well as security concerns, threats, and solutions. Furthermore, the article discusses various essential cloud themes, such as the cloud architectural framework, service and deployment model, cloud technologies, cloud security ideas, threats, and assaults. The report also highlights a number of outstanding research challenges concerning cloud security.***

Keywords: Cloud Computing, Virtual Storage, On-Demand Services, Cost-Efficiency, Technology Integration, Data Migration, Security Risks, Trusted Third Parties, Online Technologies, Research Challenges

I. INTRODUCTION

A computer in the past would use as much electricity as one now and take up the same amount of space as a room. It would also include extravagant electrical components like network devices and processors that produced less computing output. These days, small hard drives replace such appropriate spaces, and expensive electrical components are replaced by cheap network gadgets. The development of a sizable distributed system that pools a lot of resources into one unit and can manage computationally demanding tasks like scientific simulations is possible as a result of the increase in processing power and infrastructure nodes.

Two well-known distributed system components are clusters and grids. Grids and clusters are two different approaches. While grids are made for large dispersed and heterogeneous networks, the cluster paradigm allows for the coupling of homogeneous networks. The cluster strategy is more expensive because to the high cost of central processing units, such as parallel supercomputers. Using middleware, such as MPICH, which is a less expensive solution, standalone resources, such as desktop PCs are connected. The grid, which is produced over the Internet, is the architecture that desktop and home users use the most frequently to create servant computational nodes. One illustration of such a grid is the Large Hadron Collider (LHC) computing grid at CERN. The primary drawback of grid computing is that it makes management more challenging.

We don't consider how electricity is generated or how it enters the channel when we connect an electric gadget to a channel. The virtualization of electricity makes this occurrence possible. Although this electricity can be accessed through a wall socket, it actually hides a power plant and a widely spread infrastructure. This concept forms the basis for researchers' studies when information technology is expanded; these studies involve giving users who are uninformed of how their internals work important data and services. It is believed that the computing environment is entirely virtualized.

High levels of security and privacy for related data and services are attained through the negotiation of a Service Level Agreement (SLA) between cloud service providers and cloud customers. There is no common method for developing a SLA, though. A SLA report for the provided services is described in the study (Kandukuri et al., 2009), which is advantageous to both users and suppliers. These SLA reports, however, might not properly take into account client losses. In order to guarantee that the data of its users is completely protected, several cloud service providers, such as Google, Amazon (2015), and SalesForce, withhold extensive SLAs and omit a number of other service-related variables. The best illustration is Amazon Elastic Cloud Computing (EC2) (Amazon, 2015), which offers its users the virtual hardware abstraction.

II. CLOUD AND SECURITY

Cloud computing is defined by the National Institute of Standards and Technology (NIST) as a model that enables convenient, on-demand network access to a shared pool of reconfigurable computing resources (such as networks, servers, storage, applications, and services) that can be quickly provisioned and released with little management work or service provider interaction. Three cloud service models, four cloud deployment models, and five key features are used by NIST to define cloud computing.

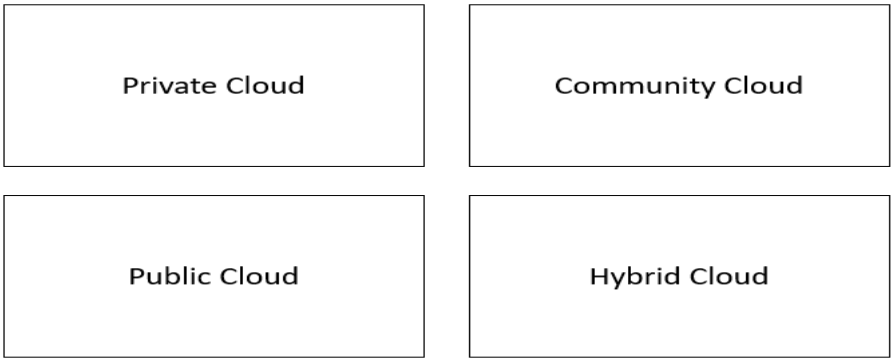


Fig. 1 Cloud Deployment Model

The aforementioned graphic shows that there are three service models, four deployment methods, and five characteristics of cloud computing. Technologies including virtualization, grid computing, distributed computing, web 2.0 technologies, service-oriented architecture, and utility computing have given rise to the cloud.

1) *Private Cloud:* Private cloud, also known as internal cloud, is a type of cloud that companies use internally for their own employees or affiliates only. Private cloud deployment is better suited for large businesses or government agencies with numerous branches. The private cloud will replace public clouds as the primary method of deploying IT systems in these massive corporate data centres. Private cloud installations are within the enterprise itself as opposed to the public cloud, allowing them to have control over data security and system availability. The investment is substantial, particularly for a one-time capital commitment, which is a downside. However, the private cloud behaves well in terms of security.
2) *Community Cloud:* Hybrid clouds combine the benefits of both private and public clouds, enabling them to offer services to both their own users and external clients. When using a hybrid cloud computing approach, agencies should run non-core applications on the public cloud while using the private cloud to support its core programme and store sensitive internal data. In contrast, the hybrid cloud has more complicated security issues and requires a larger deployment cost for providers.
3) *Public Cloud:* Public clouds, often referred to as external clouds, offer services to outside clients; all of their services are offered for usage by others as opposed to just themselves. Third-party providers construct the public cloud in one or more data centres for operation and management. Multiple users can access services through the public infrastructure.

A. *Characteristics of Clouds*

The following are the top five properties of clouds:

1) *Self-service Offered on Demand:* Without needing to speak to a service provider directly, a customer can autonomously provision computer resources like server time and network storage as needed automatically.
2) *Resource Pooling:* Using a multi-tenant approach, the provider pools its computing resources to serve a number of customers, with various physical and virtual resources being dynamically assigned and reassigned in response to customer demand. There is some level of location independence because the client typically has no control or knowledge over the precise location of the resources offered, however they might be able to designate location at a higher level of abstraction (for example, country, state, or datacenter). Storage, computation, memory, network bandwidth, and virtual machines are a few examples of resources. Even private clouds frequently share resources across various departments within the same company.

3) *Extensive Network Access:* In order to encourage use by diverse thin or thick client platforms (such as smartphones, laptops, and PDAs) as well as other conventional or cloud-based software services, capabilities are made available over the network and accessed through normal protocols.
4) *Rapid Elasticity:* Capabilities can be rapidly and elastically to quickly scale out; and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
5) *Measured Service:* Cloud systems automatically control and optimize resource usage by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, or active user accounts). Resource usage can be monitored, controlled, and reported thereby providing transparency for both the provider and consumer of the service

These five essential characteristics differentiate cloud computing from traditional computing approaches. Apart from the above five characteristics, virtualization and multi-tenancy also form important part of cloud characteristics.

B. Cloud Service Models

The three service models—SaaS, PaaS, and IaaS—identified by the NIST cloud computing definition offer customers a variety of service management operations and expose various access points into cloud systems, which in turn gives adversaries a variety of attacking surfaces. Therefore, it is crucial to think about the impact. of cloud service models and the various problems with security implementation and design that they provide.

For instance, SaaS enables consumers to access cloud services over a network connection, typically the Internet and a Web browser. In terms of SaaS cloud system security, Web browser security has received a lot of attention. Since virtual machines (VMs) run on hypervisors on hosts and are given to cloud users of IaaS, hypervisor security for achieving VM isolation has been intensively researched by IaaS cloud providers that use virtualization technologies.

1) *Saas (Software as a Service):* Software as a Service, or SaaS, is a novel method for giving users access to software services. SaaS has also undergone further advanced development as a cloud service. Users of software as a service (SaaS) are not required to buy software products and install them on their own computer or server; rather, they may order the software or utilise a payment model to lease it. Some software is offered for free, but users only have certain rights to use it. Software as a service is essentially processing power that is made available by a software service provider to satisfy a user's need. Online services like email, web conferences, network fax, online antivirus, online games, online videos, and online search are currently the most common SaaS applications, along with management services like online project management and online ordering platforms. Sincere to say, the SaaS model does help consumers and businesses save money on implementation. The future development patterns for the software sector are SaaS. These days, domestic software giants Yong You and Kingdee have also released their own SaaS programmes in addition to Microsoft, Salesforce, and other large software giants.
2) *PaaS (Platform as a Service):* PaaS (Platform as a Service) can offer whole computing environments, including application design, development, testing, and hosting, as a service to clients. The client can create web apps utilising this service mode without installing the necessary hardware and software on their own PC. PaaS is substantially less expensive than software development platforms based on data centres. PaaS offers the most value at the cheaper cost, in fact. The Facebook development platform and the Microsoft Windows Azure platform are typical PaaS application examples. PaaS has a promising future in the industry and can also advance SaaS. PaaS can lower the barrier to entry for providers who want to enter the SaaS market; for providers who already provide SaaS services, PaaS can assist in product diversification and the provision of specialised services. Additionally, PaaS increases development productivity while lowering the cost of SaaS application development.
3) *IaaS (Infrastructure as a Service):* IaaS (Infrastructure as a Service) describes the usage of cloud computing by businesses and people to gain access to remote computer resources, such as computation, storage, and application virtualization-related services. Utility computing is comparable to IaaS mode. The fundamental concept of the latter is to offer computing services in addition to the tools. Users only pay for the processing power, disc space, and other resources that are actually used. The infrastructure services provider can supply the processing capacity that is required for end users, SaaS providers, or PaaS providers without their having to pay the initial investment cost for the foundational IT gear and software. Currently, IaaS services based on hardware can be offered by providers like Microsoft, Amazon, Century Internet, and others.

They are able to pool memory, 1/0 devices, storage, and processing power into a virtual pool of resources using cloud computing technology to offer services to end users and SaaS and PaaS providers. IaaS application is, of course, less developed than SaaS because numerous critical technologies still require research and development.

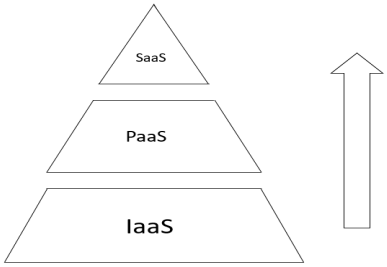


Fig. 2 Cloud Service Model

III.THE DIFFICULTIES OF CLOUD COMPUTING IN SECURITY

Cloud is now a buzzword in the information technology sector, encompassing cloud computing, cloud software, cloud storage, cloud operating software, and cloud security. Through service submission, cloud computing offers a virtual infrastructure and services to outside users. The concept of IT infrastructure as a service, which allows computing services like water, electricity, and other public utilities, to access resources on-demand and pay for use, is reflected in cloud computing. It was therefore viewed as the third revolution in the information business and will serve as the foundation of the information society of the future.

The IT industry's development trend is cloud computing. However, allowing the user to go to the "cloud" also comes with a sizable number of issues. One of the most significant factors impeding the long-term development of cloud is security concerns. Some people think that since data and applications are stored in the "cloud" in the age of cloud computing and both public and private cloud providers provide technical support, centralised control management is advantageous for information security; In general, internal private clouds are more secure, economical, and effective than independent business divisions operating and maintaining systems. Cloud service providers with competent equipment and security professionals can offer full security protection and better and more affordably secure information security through the implementation of centralised cloud computing. The centralised management of cloud computing centres will become the main targets of hacker attacks, and with the system's size and previously unheard-of levels of openness, sharing, and complexity, its security issues are worse than ever.

As widely acknowledged, the era of cloud computing offers cost advantages and, to some extent, certain security benefits. However, it's imperative not to overlook the emerging security challenges that accompany cloud technology. These challenges pose significant obstacles to enterprise security. Reports indicate that cloud computing service providers have faced a multitude of security threats from various sources, each with varying degrees of severity. For instance, in both October 2007 and February 2008, Amazon's EC2 experienced extensive service disruptions. Amazon's cloud computing service, at one point, suffered an outage due to a lightning strike. Additionally, in March 2009, Google encountered a security breach that resulted in the disclosure of customer private information. In July 2009, Amazon's cloud computing services, including EC2, experienced a security failure, rendering their website inaccessible.

1) The first is that there will be more security assaults because of the enormous volumes of user data that are being stored in the cloud system. In contrast, cloud systems give users more open access interfaces in order to ensure flexibility and versatility services provided by the cloud, which also poses greater security risks. If the attacker manages to successfully attack cloud systems, it will result in devastating disaster for both cloud providers and users.

2) The second is virtualization technology, which not only allows for flexible resource configuration on cloud computing platforms but also introduces new security risks. The issue of secure cloud platform deployment based on virtual machine architecture must be resolved. The danger of disclosure rises in a virtualized system since the server is like a file that can be removed quickly. The maintenance of the virtual network environment frequently falls under the purview of the administrator when numerous virtual machines are running on real servers. In that situation, the administrators' privileges grow, necessitating the regulation of their privileges. Virtualization platform introduction has resulted in new security vulnerability. Third, make sure that the cloud platform services are continuous and that user data and company operations are highly available. Events

involving the unavailability of Google's Gmail, Amazon data centres, and others are connected to the accessibility of cloud computing. The aforementioned incidents have a certain effect on the enterprise's excitement for using public clouds. A fault-tolerant mechanism for user data backup must be offered by cloud computing services in order to lessen the effects of lost original data on applications. All of the aforementioned factors considerably enhance the likelihood of service interruption, including the chance that the programme itself contains flaws and the likelihood of numerous hostile attacks.

3) Fourth, make sure user data is secure and private. When hostile assaults target cloud systems, their main goal is to steal user privacy before gaining financial advantage. In this situation, laws, regulations, and procedures are the issues that need to be resolved most urgently. Accordingly, the laws and regulations that are pertinent should be established and improved in order to safeguard third-party security, satisfy the demands listed by businesses, particularly to clearly delineate responsibility division when issues arise, and to offer protection mechanisms as cloud service providers depart. Most domestic organisations are hesitant to store sensitive data with a third party and continue to concentrate on creating private clouds. Only security rules and procedures will be improved over time as security technology develops.

4) Fifth, enhance cloud specifications: Everywhere there are cloud standards because of interest-driven IT development processes. Numerous manufacturers have established their own application standards and data formats, obliging users to implement IT systems and run their own businesses within the parameters established by various service providers. All of this ultimately results in a business environment that is disorganised and unfavourable to user application. The cloud computing security standards and evaluation system offers crucial managerial and technical support. Additionally, interoperability between different cloud service types is crucial to preventing the cloud from becoming isolated in its development and fostering collective advancement. The development of cloud standards will, in part, determine how cloud computing will develop in the future.

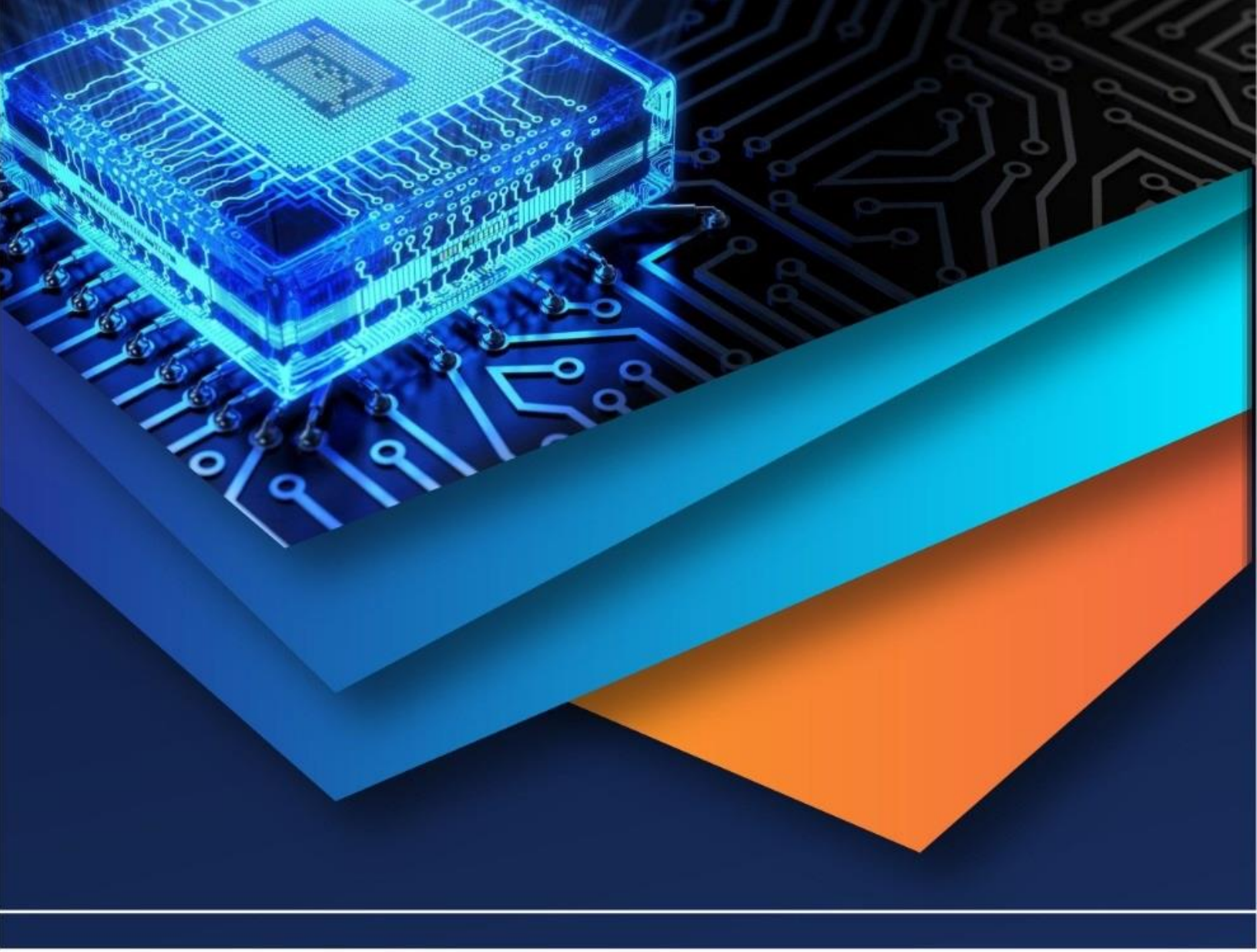
The analysis presented above relies more on public clouds than private ones. Private clouds mostly inherited the benefits of cloud computing in terms of security. Along with the usual security concerns, the private cloud also has internal oversight challenges. Private clouds have more expensive deployment costs despite having tighter security, but major businesses may afford to make the investment. For the vast majority of small and medium-sized businesses as well as individual users, the public cloud is still quite advantageous. In order to increase the security of the public cloud, research into associated security technology solutions should be accelerated. This will give the public cloud a wider market.

IV. CONCLUSIONS

The Cloud computing is a growing trend in the IT sector since it is anticipated to dramatically lower the cost of existing technologies. The cloud computing industry has both positive and negative effects on information security. Whether we can maximise its advantages while minimising its drawbacks will determine the final outcome. Only in this manner will the cloud be able to truly reduce costs while enhancing productivity, efficiency, and security.

REFERENCES

[1] https://ieeexplore.ieee.org/abstract/document/5283911
[2] https://www.sciencedirect.com/science/article/abs/pii/S136341270900 0028
[3] https://www.sciencedirect.com/science/article/abs/pii/S108480451630 2983
[4] PG Shah, X Huang, D Sharma, “Algorithm Based on One's Complement for Fast Scalar Multiplication in ECC for Wireless Sensor Network” , Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference.
[5] PG Shah, X Huang, D Sharma, “Analytical study of implementation issues of Elliptical Curve Cryptography for Wireless Sensor networks”, Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference.
[6] X Huang, PG Shah, D Sharma,"Multi-agent system protecting from attacking with elliptic curve cryptography", Advances in Intelligent Decision Technologies - Smart Innovation, Systems and Technologies Volume 4, 2010, pp 123-131
[7] Kandukuri, B.R. Paturi, V.R. ; Rakshit, A. , “Cloud Security Issues” , Services Computing, SCC '09. IEEE International Conference, 2009
[8] Kaufman, L.M., “Can Public-Cloud Security Meet Its Unique Challenges?” 2010
[9] Sheikh Mahbub Habib, Sebastian Ries and Max Mühlhäuser, “Towards a Trust Management System for Cloud Computing” 2nd IEEE International Symposium on Trust and Security in Cloud Computing



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY