IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307104|

# Identity and Access Management (IAM) in Cloud Environment

**Pooja A, Nagesh B S, Neha M, Raghu Prasad K**

P.G. Student, Department of Master of Computer Applications, RNS Institute of Technology, Channasandra, Bangalore, India

Associate Professor, Department of Master of Computer Applications, RNS Institute of Technology, Channasandra, Bangalore, India

P.G. Student, Department of Master of Computer Applications , RNS Institute of Technology, Channasandra, Bangalore, India

Assistant Professor, Department of Master of Computer Applications, RNS Institute of Technology, Channasandra, Bangalore, India

**ABSTRACT**: The creation and integration of various connected devices into a high-tech cloud that provides services based on demand is known as cloud computing. Cloud computing architecture contains many customizable disseminated systems with different inherent connectivity and usage. Cloud networks is a quickly emerging network technology in business because of its cost-effective, scalable and reliable solution. Even the fact that the major care in the context of cloud computing is promoting, but frankly speaking we are not completely secure from some types of network attack and privacy concerns in a dynamic nature for amazingly performance modern systems. Because of properties such as joint tenancy and third-party managed infrastructure, cloud environments require robust access control and identification processes. Many commercial and intellectual have covered the securitization pertaining to resources of cloud access issues. This paper touches on authentication & authorization, protection problems and hosted services by the cloud setting that has been commented upon [4]. We also compared the current techniques with cloud service suppliers and customers, focusing on identity access management; problems with security and offerings within a cloud environment.

**KEYWORDS**: IAM(Identity and Access Management).

## I. INTRODUCTION

One new paradigm in computing is cloud computing, it is an emerging paradigm in that it combines kinds of re-configurable computer resources such as networks, servers, storage services and applications which provide to clients instant yet simple limited electronic accesses distances on-demand [1]. As of today, cloud computing is a large subject which everyone deliberates upon heavily in almost every business domain. Identity management in cloud environment is done by Cloud service providers (CSPs). Weaknesses in identity management systems, conversly are responsible for certain more notable instances data leakage [2]. The identification and accessibility control (IAC) System should be the most problematic cloud configuration aspect concerning IaC that is key to accepting services. As a result of this CSP-first approach, the current implementation of identity management is ill-equipped to accommodate users with versatile security protocols that policies that are more granular in nature.

## II. AUTHENTICATION MECHANISM

That means allowing one entity to associate itself with another using a process of authentication. This is used to test whether the applicant or the adaptable rules for access control that rights of access and petitions. The authentication process is usually done by software [3]. In network environments, popular authentication techniques are login information(simple text usernames and passwords), multi factor authentication (3D password objects of desire), third-party authentication, graphical password, identification via digital devices and biometrics.

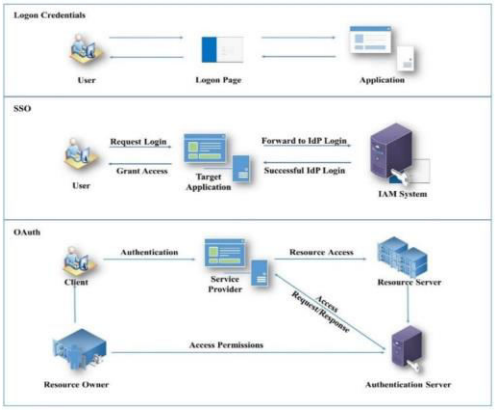
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

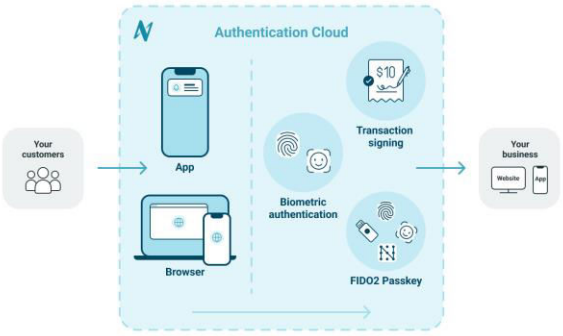
Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307104|




**A. Surveillance Systems**

By providing access control through authentication, physical security systems such as preventing unauthorized access, biometric and access cards safeguard both cloud resources and physical spaces.Because they enable clients to access them almost at will, cloud data centres (CDCs) have caught the interest of or- organizations in recent times. CDCs centrally manage all servers, networks and apps allowing you to have access anytime anywhere. Specific usage & governance standards, data centres and even Physical security in order to stay away from insider source of leaks or unauthorized access.Digital Authentication and Biometric Access control devices currently are provisioned as physical security systems.

**B. Intrusion Detection System (IDS)**

1. Keys and safe Shell credentials: A person's credentials attest to the validity, importance (rank), rights or access of that individual. The one that demonstrates that a user have the rights to use certain resources and services. You generally use this credentials like OTPs, patterns and captcha in order to protect the system from any unauthorized activity. The most common technologies for managing access credentials are user names and passwords.

2. Multi-factor Authentication: Another mechanism for protecting Internet transactions and digital assets, multi-factor authentication adds at least one additional factor to the process (for example a PIN code or your IP address in addition to login / password). Most of the time, a second form of authentication is used with credentials (OTP), Captcha or Pattern. Finally, in addition to the low security multi-factor provides over traditional credential-based authentication. These One-Time Passwords are commonly used in authenticating online transactions. One-time passwords are generated by the server through a certain algorithm according to its settings and provided to an legitimate user via e-mail or registered mobile phone number in online financial transactions.

3. Adapts Chip and Pin: The most prevalent type of securing present or future financial transactions with a physical chip. It allows you to authenticate your organization´s machines and services within the network. Distinct transaction information is provided by the semiconductor microprocessor to help save user information and security keys, in addition to mitigating fraud. Encrypts and signs communications between the client terminal and this with a security key stored in-chip, After confirming the signature, the server decrypts the message using a pair key kept in its possession.

## III. AUTHORIZATION MECHANISM

Some resources can be accessed only to an authorized user who has a right privilege on them. Information regarding user or application identification is utilized in the identification process responsible for deciding on which users / applications are permitted to execute within a system [4]. A user even can use multiple varieties of services simultaneosly over a cloud network which is place for some different environment and witch have range with multi level security. As third-party suppliers authorize specific private data for their programs. These permissions are dangerous because they violate the user's privacy. For instance, outside applications can access cloud- based social network application provided the user permits it [5]. Gathering target intelligence is a lot easier if you are taking hostile action. Permission is achieved through delegating access right. As such, whenever an individual provides permission to

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

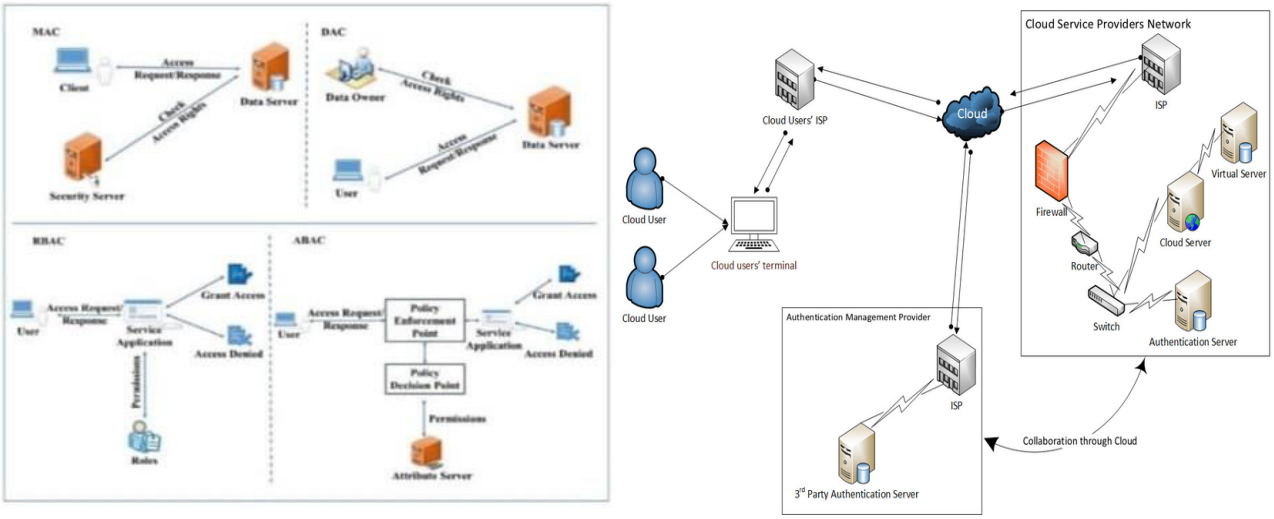
Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307104|

an external app they are able access social network applications in the cloud [5]. It is simpler to gather target intelligence when taking offensive action. Billing is done via allowance in cloud permission.




## IV. IDENTITY AND ACCESS MANAGEMENT

To guarantee that the correct people and organizations have access to the relevant technology resources, Identity and Access Management (IAM) in the cloud is a crucial framework. Digital identity management and resource access control are handled by means of policies, procedures, and technology. The remote nature of cloud services and the need for strong security measures to shield private information and apps from unauthorized access make identity and access management (IAM) especially important in cloud environments. Encouraging security through multi-factor authentication, single sign-on (SSO), and fine-grained access controls, cloud IAM solutions offer centralized management of user identities and access entitlements. Due to their comprehensive reporting and monitoring of all access activities, these systems also make it easier to comply with regulatory standards. Because cloud services are dynamic and scalable, we need flexible identity and access management (IAM) systems that can change with the needs of companies, accommodating varying user roles and permissions. In addition, cloud IAM provides an all-encompassing security posture by integrating with other security measures including encryption, network security, and endpoint protection. Organizations may reduce the risks of data breaches, insider threats, and other security issues by putting efficient IAM methods into place. This lowers administrative costs, streamlines user interface, and guarantees that only authorized users can access key resources.To secure digital interactions and keep control over who can access what resources within a company, identity and access management (IAM) in the cloud is crucial. It is the foundation of cloud security measures and includes identity governance, authentication, and authorization. Minimizing potential security concerns, effective IAM makes sure users have the minimum privilege required to do their tasks. In order to lower the possibility of human mistake and guarantee prompt adjustments to access permissions when roles change, it also allows automated user provisioning and de-provisioning. Furthermore, cloud identity and access management (IAM) systems frequently interface with a range of services and apps, offering a unified and seamless user experience across platforms. Maintaining productivity while adhering to strict security standards depends on this integration.

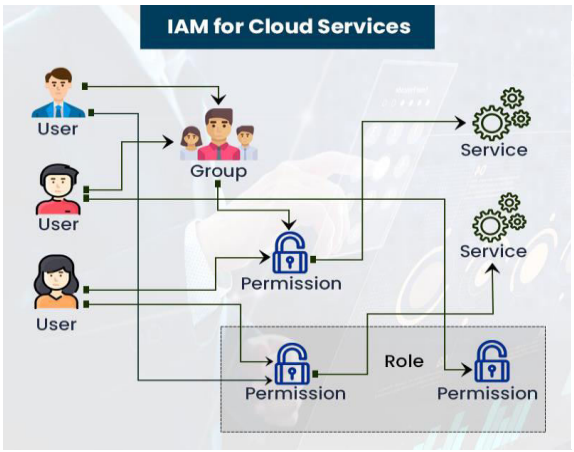
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

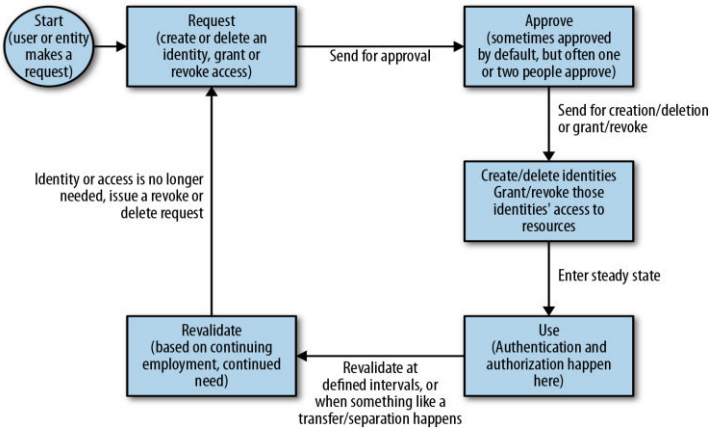
Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307104|

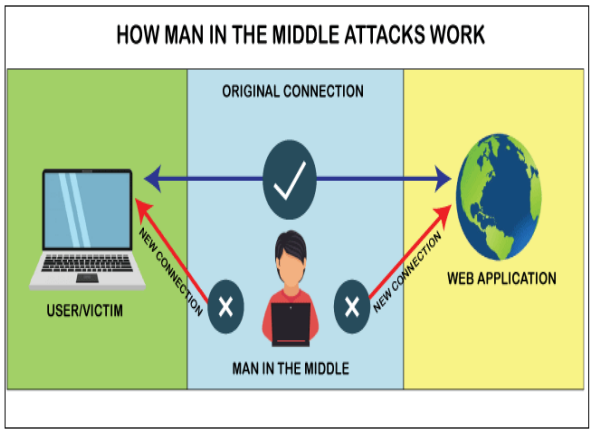



## V. SECURITY ANALYSIS IN CLOUD

### A. Man-in-the-Middle (MITM) attacks

Attacker is a party that intercepts the transfer data of one system and changes it without the knowledge of either provider or dependent part. A man-in-the-middle attack is when an attacker interposes themselves, impersonating among the providers in a interaction with the reliant party. When it comes MITM attacks,such data comprises personally identifiable information (credentials and account details), as well as financial information such as credit card numbers and bank info. If the data is used for further financial transactions illegally, passwords can be changed and identity theft. Solution: Encrypting communication could help to avoid eavesdropping on the line. The right SSL (secure socket layer) settings can actually decrease the possibility of a MITM attack. It is good way of reducing the MITM vulnerability through encrypted tokens for creating trust and one-time access.




### B. Insider attacks

Insider attacks occur when someone within the security perimeter aims to compromise security. Malevolent insider — a business partner of the organization, contractor or current/former employee. These insiders leverage their access to the organization's private and sensitive resources, compromising its availability, integrity, and securi-ty. Insiders in cloud networks are third-party suppliers or even cloud administrators who may use the resources for conducting attacks on the organization infrastructure. Mitigation: Be sure to use strong authentication and authorization in the system. If access governance policies are correctly defined by the organizations insider assaults can be brought down substantially.

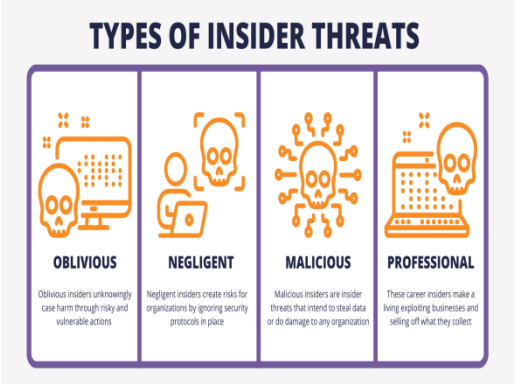
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

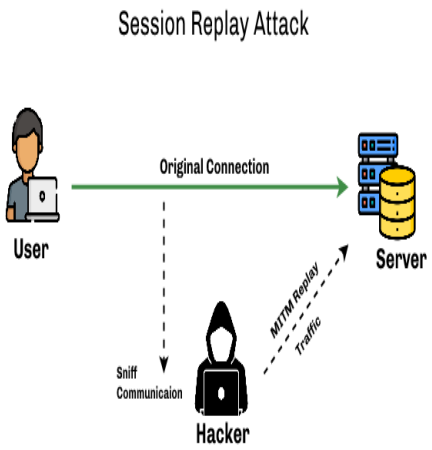
Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307104|




**C. Replay attacks**

Replay attacks, in which a hacker intercepts and re-transmits a legitimate data transmission in order to possibly obtain unauthorized access to cloud resources or data, are a serious security risk in cloud computing. By taking advantage of holes in authentication methods, an attacker can pretend to be an authorized user even though they do not actually have the necessary credentials. Replay attacks have the potential to cause service disruption, unlawful resource usage, and data breaches in the context of cloud services. Cloud providers and users use time-stamped tokens, secure communication protocols (such SSL/TLS), and strong session management techniques to guarantee the integrity and authenticity of communications in order to reduce these risks.




**D. Session/Cookie hijacking**

Session hijacking occurs when the session id is not secured well for user authentication. Note, your local session/cookie is likely embedded with some info about the users credentials. An attacker, after taking over a legitimate session may spoof the attack using this compromised Session id. Such packet sniffing tools are used to fish out userspecies keys by intercept- ing the login mechanism or method This method exploits a cookie that is hijacked, which allows the attacker to log in on some other website with no knowledge of its owner. These include ' a malware or simply an error in the systems, phishing attacks and sniffing tools which all add to session / cookie hijacking. Another idea to defend against client-side session hijack is using safe sessions – Mitigation.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

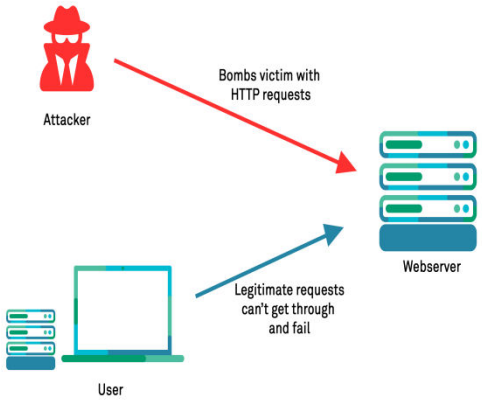
|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307104|


**E. Guessing attacks**

An attacker will try to guess with high probability any newly created hash value by using a password that it had used in the guessing attack, he would simply replace his complicated and unique original string of passwords into something easier or following an easy pattern. These attackers collect generic information about genuine consumers and then attempt to log in using those passwords for thousands of times until they breakthrough. In the offline way, nothing exists on cap on tryings to guess a password so it could be received almost certainly by trying enough. Strong password and then locking the user after a certain number of failed login attempts we can protect against various guessing attacks.




**F. Denial-of-Service attacks (DOS/DDOS)**

This obfuscation holds clues that the server is being flooded with fake service requests intended to keep it so busy responding to phantom ones, legitimate request such as a directory index download command are denied. This is referred toa Denial of Service (DOS) attack; Flood attacks eventually happen when the target host cannot manage all service requests on its own and needs to pass them off (via load balancer system) into another server instance. Distributed Denial of Service (DDoS) attacks are carried out by malware or bots from thousands of compromised systems. Since cloud servers provide IaaS and SaaS models, they are liable to DOS/DDoS attacks. Firewalls stop attacks/mitigate (Mitigation) Cannot do this on large scale Typically done with static rules like I decide what IP subanresses can connect across port 80. It is possible to greatly reduce the impact of DOS attacks on cloud services, when it comes particularly in Dynamically limiting and controlling number of hits from each requesting org -channel (Products like Data Power Gateway for allotting network bandwidth).

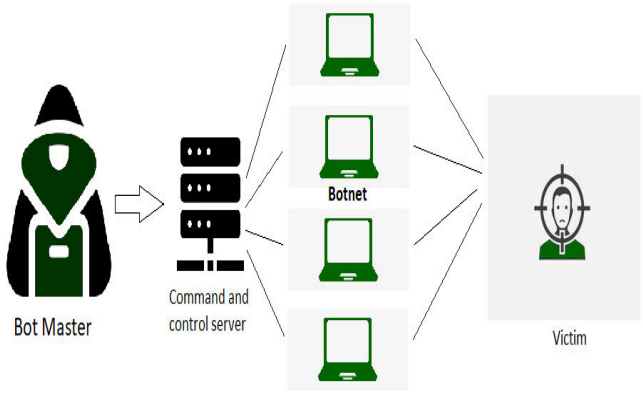
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307104|




**G. Password/Key compromise**

An attacker who steals the login credentials for an attackers online services account or servers can have difficulties with cloud services, which is misusing them. A combination of system weakness, malware attacks and malicious insider makes a password/key compromise truly disastrous. There can be password guessing (because passwords used are weak), brute force assaults, phishing attacks and spoofing attacks whose some examples of a Password breach. Mitigation: Organizations can address the issue could by implementing federation/SSO which would result in an end to using the fixed credentials for web services access.


## VI. CONCLUSION

Cloud service has become an important paradigm for digital solutions, as it reduces the capital investment and operational expenditure of organizations.Security Concern of Public Cloud Privileged Container as a Service It's due to multi-tenancy and depending on the third parties for cloud environment management this technology get high amount of security thread. Focusing on identity, access.,security and services management this research laid down security issues in today's cloud service infrastructure, dangers that they may encounter with corresponding mitigations. This work brings out different themes along with the mechanisms, issues associated with each mechanism in most cases and best practices and suggestions from academia as well as industry perspective. Advanced access management frameworks surface existing identity and need to improve the current identity survey of various mechanisms for

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307104|

security principles , making it sufficiently interesting cloud technology services, indicating a roadmap not only one but furthermore potential practices.

## REFERENCES

[1] Goyal, P., Batra, S., & Batra, P. (2020). Identity and Access Management in Cloud Computing: Advances and Future Directions. *Journal of Cloud Computing*, 9(1), 1-15. https://doi.org/10.1186/s13677-020-00189-w
[2] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud Computing: State-of-the-Art and Research Challenges. Journal of Internet Services and Applications, 1(1), 7-18. https://doi.org/10.1007/s13174-010-0007-6
[3] Takabi, H., Joshi, J. B. D., & Ahn, G. J. (2010). Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security & Privacy*, 8(6), 24-31. https://doi.org/10.1109/MSP.2010.186
[4] Subashini, S., & Kavitha, V. (2011). A Survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications*, 34(1), 1-11. https://doi.org/10.1016/j.jnca.2010.07.006
[5] AlSudiari, M. T., & Vasista, T. G. K. (2012). Identity and Access Management in the Cloud Computing Environment. *Journal of Information Security*, 3(4), 322-328. https://doi.org/10.4236/jis.2012.34038

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details