iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VI **Month of publication:** June 2024

DOI: https://doi.org/10.22214/ijraset.2024.63475

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 12 Issue VI June 2024- Available at www.ijraset.com

Cloud Computing Security Issues

Nishtha Singh

Abstract: ***Cloud computing is an approach to manage limitations or include restrains progressively without setting resources into new structure, preparing new work force or favouring new programming. As information exchange is a noteworthy activity in the current life, information security ends up being a significant issue. Prior to dissecting the security concerns, the importance of distributed or cloud-based processing is examined, and a number of cloud-based security-related challenges have been analyzed. The security issues identified with cloud computing has been investigated here and a local adaptable security solution for the cloud has been proposed. This paper also looks at the cloud security issues in terms of features like ease of adaptability, access, etc. This work is expected to empower scientists and experts to think about various security threats and work on finding out their effective solutions.***

Keywords: Cloud Computing, Security threats, Cloud Architecture

I. BACKGROUND.

Because of these intrinsic qualities, cloud computing has become a very interesting issue in academic fields during the last ten years, providing a distinct viewpoint on the global environment. Various experts from diverse fields, including global energy crisis, climate change, and healthcare, have benefited from the capabilities of cloud computing [4]. Nevertheless, issues including inadequate processing, connectivity, and security capabilities hinder the advancement of cloud computing. In certain contexts, such as real-time secure data sensing, smaller enterprises utilizing their own systems find it nearly impossible [8].

Cloud With its on-demand services that are especially helpful for small businesses with limited resources, cloud computing has emerged as a major force in both the academic and commercial domains [10]. Despite its popularity and benefits, concerns persist, especially regarding security issues. Some view cloud computing as a facilitator of resource management, while others see it as a method for software deployment and data access from the cloud. The flexibility and data availability provided by cloud computing reduce costs through information sharing among organizations. However, issues related to secure access and data storage persist, including vendor lock-in, multi-tenancy, reduced control, service interruptions, and data loss.

While cloud computing has gained widespread attention, security and privacy-related challenges have prevented full acceptance by organizations. Security incidents in renowned companies like Microsoft, Amazon, and Google underscore the need for robust security measures in cloud computing [3]. Cloud computing stores and manages all data, including application data, hardware, and software, in separate cloud domains, in contrast to traditional security methods where consumers guarantee the security of their data. The lack of awareness among customers about the security processes adopted by cloud providers adds to the uncertainty and trust issues between customers and cloud suppliers.

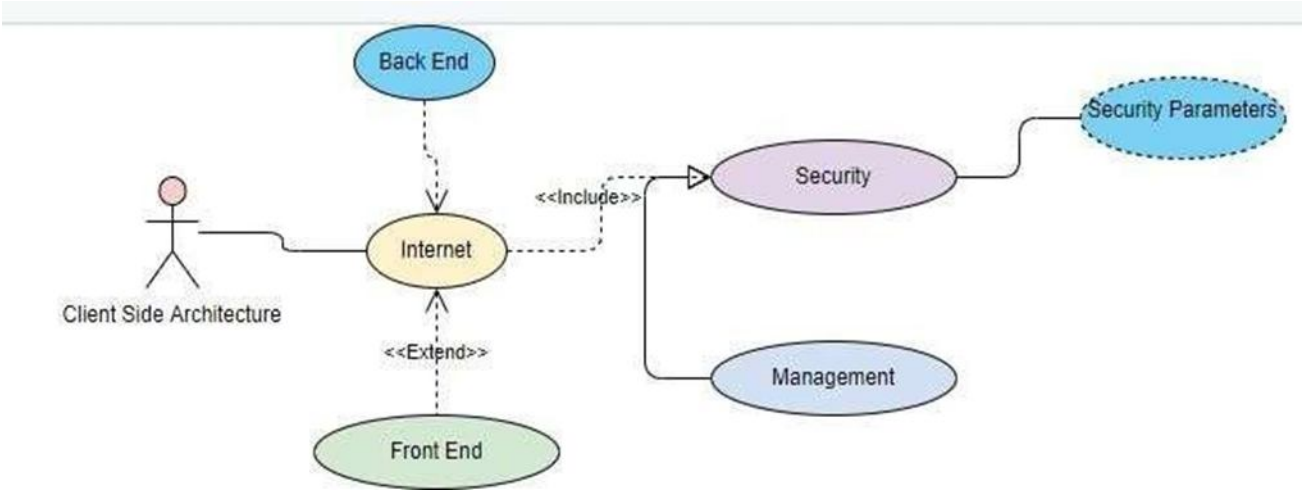


Fig.1. Cloud Computing with security issues

©IJRASET: All Rights are Reserved

II. RELATED WORK

In recent years, there have been two main developments in the concept of cloud computing: renting infrastructure on the cloud and renting various utilities on the cloud. The former involves the utilization of hardware and software, while the latter is focused on availing utilities without necessarily accessing the underlying hardware from cloud service and infrastructure providers [13]. With the development of cloud computing, a number of terms have been developed to describe various combinations of cloud computing, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

One significant aspect of cloud computing that has garnered attention is security. Organizations are increasingly concerned about safeguarding their data and operations in the environment of cloud. Dedicated to promoting best practices for guaranteeing security in cloud computing, the nonprofit organization Cloud Security Alliance was founded. Additionally, it aims to educate on the various applications of cloud computing to secure all forms of computing [5]. The Open Security Architecture is another group that deals with security-related matters and has put forth an open security architecture pattern. This pattern tries to describe essential cloud functions, important roles for supervision and risk reduction, internal organization collaboration, and controls that need more management. Certification, accreditation, and safety assessment series have been significantly enhanced to ensure that operations outsourced to another provider are conducted securely.

Ensuring the security of systems and services is crucial for effective management of service procurement. Figure 2 provides a high-level perspective on cloud computing security, as envisioned by experts. Possibility planning plays a vital role in establishing a response strategy in case of interruptions to service delivery. This planning helps organizations navigate potential disruptions and maintain service continuity.

The security landscape in cloud computing involves a multifaceted approach, considering aspects such as certification, accreditation, safety assessments, and collaboration across internal organizations. These measures are critical in ensuring that cloud-based operations are secure, especially when outsourcing services to external providers. The open security architecture pattern proposed by organizations like the Cloud Security Alliance and the Open Security Architecture provides a framework for understanding and implementing robust security measures in the cloud environment.

The evolution of cloud computing has introduced various perspectives, including renting infrastructure and utilities. Security concerns have prompted the establishment of organizations like the Cloud Security Alliance and the Open Security Architecture, which focus on promoting best practices and providing frameworks for secure cloud computing. As organizations continue to leverage the benefits of the cloud, addressing security issues becomes paramount for the effective and secure operation of cloud-based services.

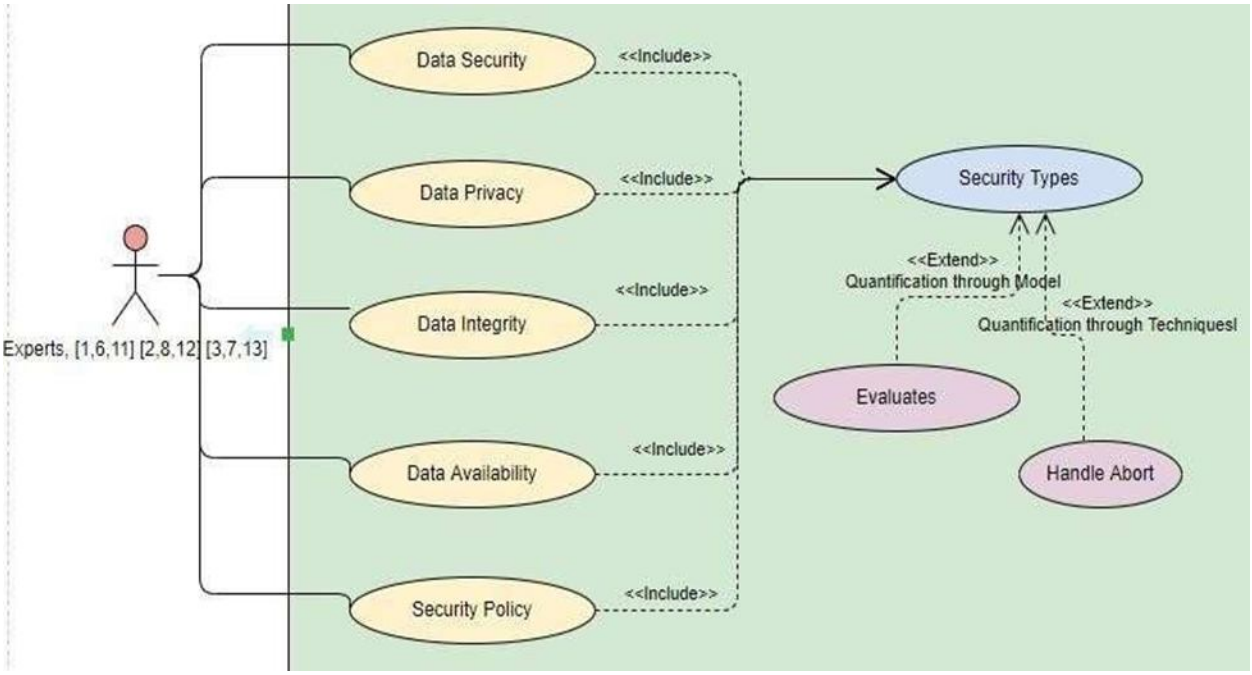


Fig.2. Expert's highlighted concerns about cloud computing

Cloud computing presents a myriad of possibilities and challenges, with security standing out as a crucial hindrance to its evolution as a technology (A. Kundu et al., 2010). The security challenges in cloud computing are diverse and continually evolving in real-time. One significant challenge is data location, where the flexibility of location transparency in cloud computing becomes a security risk. The lack of knowledge about the specific location of data storage can impact the implementation of data protection measures for a particular region, posing a potential threat to data security (G. Thippa Reddy et al.).

In the context of cloud computing, the security of users' personal data is of utmost importance. Merely relying on simple strategic policies or exclusively applying technical security measures is deemed insufficient to address the multitude of security issues and uphold high-quality service standards (L. Wang et al., 2008). It is essential to adopt a comprehensive approach that combines various security measures to ensure robust data protection for both personal and business- related information.

Another critical factor influencing the acceptance and usage of cloud services is integrity or trust (Hyseni et al., 2019). Trust is directly linked to the authenticity, authorization, and accessibility provided by cloud service providers. Establishing trust or integrity becomes a key strategy in developing an effective cloud-based computing system. In the context of cloud computing, a trust model's implementation is essential since it takes into account the interests of all parties participating in a specific cloud computing scenario. In the context of the cloud, trust is influenced by factors such as computer-assisted management, procedures, and approaches (P. Anand, 2016).

The security environment of cloud computing is shaped in large part by security challenges, especially those pertaining to data placement and user protection. Addressing these challenges requires a comprehensive and multifaceted approach, combining strategic policies and technical security measures. Additionally, establishing trust and integrity is crucial for the widespread acceptance and successful implementation of cloud computing services. To ensure that cloud-based computing systems continue to grow and succeed, stakeholders must work together to build effective trust models and security measures.

TABLE.1.
CONTRIBUTION TABLE BY EXPERTS WITH YEAR

EXPERTS	YEAR	CONTRIBUTION	METHODOLOGY
L. Wang et. al.	2008	A study on cloud computing	Theocratically
R.Maggiani et.al.	2009	Cloud computing is discussed with communication	Theocratically
A. Kunduet. al.	2010	Introduced new services	Method based
Akhil Behl et. al	2011	Emerging Security Challenges in Cloud Computing	Evolutions
Gonzalezet. al.	2012	Current security concerns and solutions for cloud computing	Quantitative analysis
V. Inukollue et.al.	2014	A study on security issues associated with Big Data	Theocratically
G. Thippa Reddy et. al.	2015	Framework for Cloud security	Validated
P. Anandet. al.	2016	Threat Assessment	Quantitative Assessment
D.H. Adnaan Arbaaz Ahmedet. al.	2018	Study of Security Issues	Evaluation

III. CRITICAL OBSERVATIONS

After conducting an in-depth study and completing a precise survey of available scholarly works, several critical observations have emerged, outlined below in a point-wise manner.

1) Upgrading cloud computing at the initial phase of the security process has the potential to significantly enhance the cloud framework, providing substantial support to both the infrastructure and the customer.

2) The inclusion of additional features and functionalities, such as considerations related to security, risk factors, and schedule factors, at various phases of security implementation in the cloud environment can positively impact efforts to mitigate risks.

3) Identifying the security factors that influence the cloud framework is crucial. Once identified, a set of variables relevant to information security should be established to effectively address these concerns.

4) Initializing and quantifying security measures in the cloud environment is of utmost importance to ensure a robust and comprehensive security posture

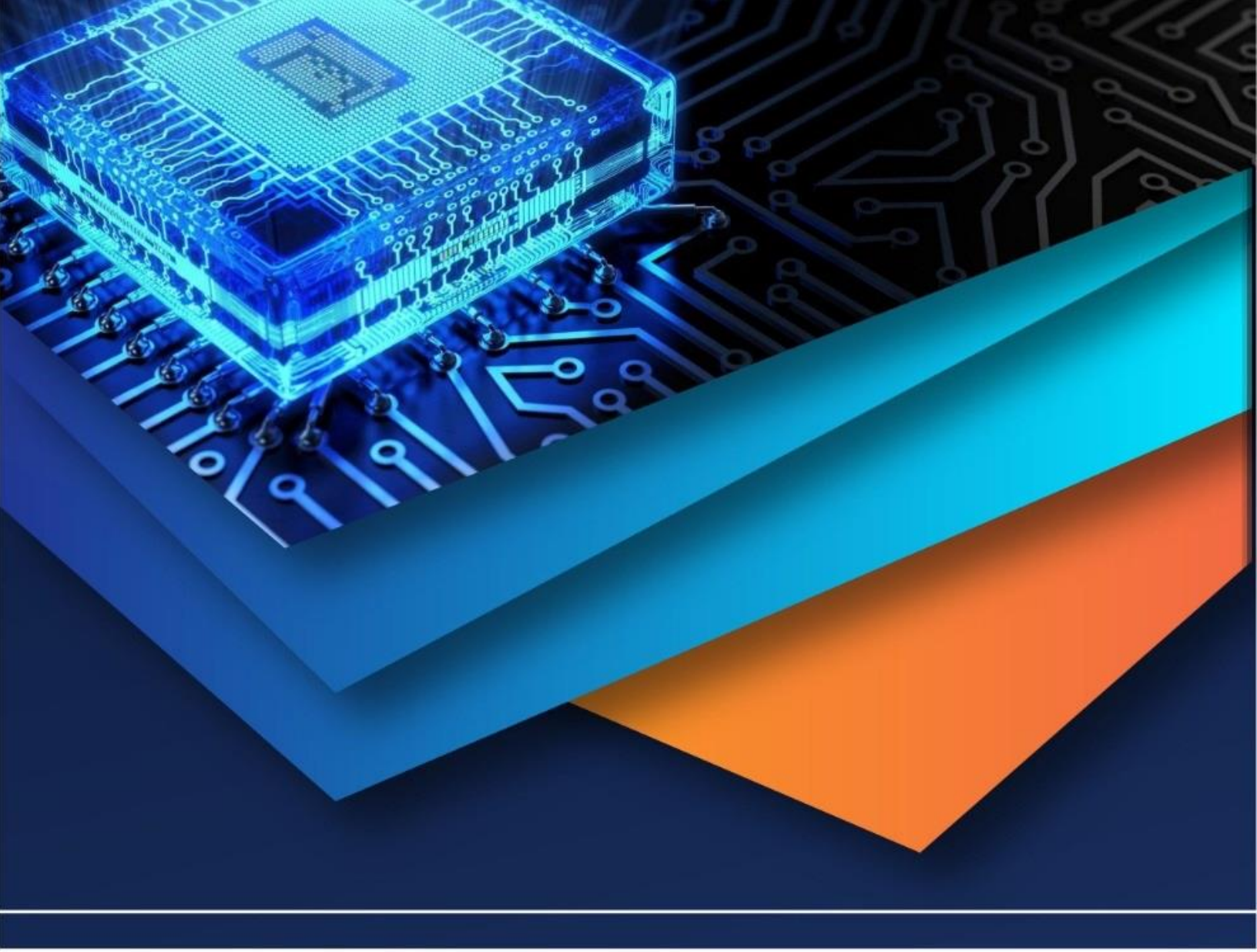
IV. CONCLUSION

Cloud computing has become a prevalent trend adopted by organizations to enhance flexibility in information distribution and exchange, leading to improvements in productivity, interoperability, capacity, and adaptability. Despite the numerous advantages offered by the cloud computing environment, security-related issues pose challenges that can result in a lack of trust, potential breaches of data and user privacy, operational inefficiencies, organizational losses, and uncertainty regarding service provider compliance.

As new models and paradigms are introduced into the cloud computing ecosystem, security considerations get more complex, especially when it comes to data security and user privacy. This study, which focuses on security aspects, the cloud environment, data validation, and data efficiency, identifies the main computational security issues in the cloud at a fundamental level. The results highlight that these problems serve as the foundation for additional study in the field of cloud computing, with the goal of filling in the gaps brought forth by security concerns. Solutions may involve the development of specific methodologies or detailed models to effectively mitigate and reduce these concerns. Addressing these issues is crucial for advancing the field and ensuring the secure and reliable operation of cloud-based systems.

REFERENCES

[1] L. Wang, Gregor Laszewski, Marcel Kunze and Jie Tao, "Cloud Computing: A Perspective Study", New Generation Computing- Advances of Distributed Information Processing, vol. 28, no. 2, pp. 137- 146, 2008.
[2] R. Maggiani "Communication Consultant Solari communication Cloud computing is changing How we communicate", IEEE International Professional Conference IPCC, pp. 1-4, July 2009, ISBN 1-42444357-4.
[3] B. R. Kandukuri, R. V. Paturi and A. Rakshit, “Cloud Security Issues,” 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695- 3811-2.
[4] Ronald L. Krutz, Russell Dean Vines “Cloud Security A Comprehensive Guide to Secure Cloud Computing”, Wiley Publishing, Inc.,2010.
[5] Xuan Zhang, Nattapong Wuwong, Hao Li, etc. Information security risk management framework for the cloud computing environments. In Proc. Of 10th international conference on computer and information technology, 2010.
[6] Special Publication 800-30. Guide for Conducting Risk Assessments. America: National Institute of Standards and Technology, 2011.
[7] European Network and Information Security Agency (ENISA). Cloud Computing: Benefits, risks and recommendations for information security.2009.
[8] Akhil Behl Emerging Security Challenges in Cloud Computing (An insight to Cloud security challenges and their mitigation) , 2011.
[9] Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Naslund, M. and Pourzandi, M. A quantitative analysis of current security concerns and solutions for cloud computing. Journal of Cloud Computing, 1(11), 1- 18, (2012).
[10] Hamlen, K., Kantarcioglu, M., Khan, L. and Thuraisingham, V. (2010). Security Issues for Cloud Computing. International Journal of Information Security and Privacy, 4(2), 39- 51. doi: 10.4018/jisp.2010040103.
[11] Youssef, A.E. (2012). Exploring Cloud Computing Services and Applications. Journal of Emerging Trends in Computing and Information Sciences, 3(6), 838-847.
[12] Zissis, D and Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28, 583–592. doi:10.1016/j.future.2010.12.006.
[13] D. H. Adnaan Arbaaz Ahmed, "Cloud Computing: Study of Security Issues And Research Challenges", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), April 2018.
[14] D. A. L. B. S. a. B. C. Hyseni, "The Proposed Model to Increase Security of Sensitive Data in Cloud Computing", International Journal of Advanced Computer Science And Applications, vol. 9, no. 2, pp. 203- 210, 2019.
[15] G. Thippa Reddy, K. Sudheer, K. Rajesh and K. Lakshmanna, "Employing Data Mining on Highly Secured Private Clouds for Implementing a Security – as a-Service Framework", Journal of Theoretical and Applied Information Technology, vol. 59, no. 2, 2015
[16] V. Inukollu, S. Arsi, and S. Ravuri, “Security Issues Associated with Big Data in Cloud Computing,” Int. J. Netw. Secur. Its Appl., vol. 6, no. 3, pp. 45–56, 2014
[17] P. Anand, J. Ryoo, H. Kim, and E. Kim, “Threat Assessment in the Cloud Environment – A Quantitative Approach for Security Pattern Selection,” in IMCOM ‟16, 2016, p. 1.
[18] A. Kundu, C. D. Banerjee, P. Saha, “Introducing New Services in Cloud Computing Environment”, International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5. pp. 143-152, 2010
[19] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, “On technical Security Issues in Cloud Computing,” Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)