International Journal of Computer Engineering and Technology (IJCET)
Volume 15, Issue 4, July-Aug 2024, pp. 472-480, Article ID: IJCET_15_04_041
Available online at https://iaeme.com/Home/issue/IJCET?Volume=15&Issue=3
ISSN Print: 0976-6367 and ISSN Online: 0976-6375
Impact Factor (2024): 18.59 (Based on Google Scholar Citation)
DOI: https://doi.org/10.5281/zenodo.13304712

CLOUDSTRIKE IMPACT ON GLOBAL OUTAGE AND THE CHALLENGE OF SAAS IN THE FUTURE

Sandeep Reddy Gudimetla
HCL Tech, USA

ABSTRACT

The global business world recently experienced an IT outage, which caused massive disruptions and glitches in business operations. The outage occurred due to a malfunction in CloudStrike's Falcon software. CloudStrike is a leading cybersecurity provider, offering services to over 500 companies in the Fortune 1000 companies. The issue affected key sectors like healthcare, aviation, financial, government agencies, and retail, causing flight cancellations, grounding of flights, and delayed service delivery. This outage exposed the vulnerability of SaaS platforms and applications. Challenges, such as security concerns, vendor lock-in, performance and reliability, and dependency on cloud architecture, have been identified in this paper. Despite the shortcomings, SaaS is affordable, scalable, and flexible. Thus, providers can ensure effectiveness and reliability by adopting various measures, such as establishing multi-region servers, and robust security measures.

Keywords: CloudStrike, Global IT Outage, SaaS Challenges, Cybersecurity, Cloud Infrastructure

Cite this Article: Sandeep Reddy Gudimetla, Cloudstrike Impact on Global Outage and The Challenge of SAAS In the Future, *International Journal of Computer Engineering and Technology (IJCET)*, 15(4), 2024, pp. 472-480.
https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_15_ISSUE_4/IJCET_15_04_041.pdf

INTRODUCTION

On Friday, 18th July 2024, a global IT outage was experienced, causing disruptions across several industries. The most affected sectors were healthcare, financial institutions, aviation, government institutions, small businesses, and media. This failure, which was the largest in the history of IT failures, was caused by faulty software updates. This global outage reportedly arose from an IT company called CloudStrike, which offers software used across various industries. On 18th July, there was an update malfunction on the firm's software (Falcon Sensor). The malfunction affected Windows computers, causing significant tech failures across the globe. This article will explore the impact of CloudStrike on global outages. The cause and the impact of the outage will be discussed, including the challenge of using SaaS in the future.

BACKGROUND

CloudStrike is an American cybersecurity company established in 2011. The company is headquartered in Austin, Texas [1]. Since its establishment, CloudStrike has rapidly grown, offering a range of security services through cloud-based software. The firm currently employs thousands of staff and service businesses in different countries across the globe. CloudStrike protects the network systems of over five hundred Fortune 1000 companies. Over the past decade, the company has experienced immense market growth, where it attained a market value of about $83bn at market close on 17th July 2024. On 18th July, the firm's stock price fell during trading, however, after the outage, its value drastically declined and dropped by 13% [1]. CloudStrike's services and products are usually provided to prevent malware and secure systems from hacking. The firm was also previously hired to investigate key global data breaches, such as the Russian hack on DNC servers in 2016 [1]. Other corporations that have sourced data breach investigation services from CloudStrike include Sony Pictures, which employed it to investigate the 2014 North Korea cyberattack.

HOW CLOUDSTRIKE CAUSED THE GLOBAL OUTAGE

On Friday, July 18th, 2024, CrowdStrike, a leading provider of cloud-based cybersecurity services, faced a major global outage, which affected services that rely on its systems for several hours. The issue arose from the company's efforts to update its Falcon cybersecurity platform [2]. This platform usually interacts with other computer software and systems sections, such as Windows products. When the company pushed for an update on the Falcon software, a malfunction occurred, disabling the systems, including the widely used software pieces [2]. The Falcon update was intended to enhance system performance. Unfortunately, a severe bug was introduced in the process, which triggered a massive failure within CloudStrike's cloud infrastructure. The system's ability to counter such incidents and manage errors was overwhelmed, hence the widespread service disruption.

Generally, the system's main goal is to safeguard vital computer systems from disruptions and crushes. However, it ended up affecting these systems by shutting them down. Nonetheless, the firm's technical team promptly identified the issue and initiated an incident response protocol [3].

The issue was not solved instantly because of the intricacy of the bug, including how it had spread and affected the cloud infrastructure. There was a partial restoration after four hours and a full restoration two hours and thirty minutes later. During the over six-hour outage period, the firm's clients, mainly high-profile organizations in healthcare, government, financial, and technology sectors, experience major cybersecurity risks because of the temporary vulnerability. After the outage, the firm's CEO apologized for the incident and explained that it was not a cyberattack or security incident. The CEO assured the clients that the matter had been resolved and continuous updates would be provided on CloudStrike's website [1].

Time (Hours)	Service Restoration (%)
0	0
1	10
2	20
3	40
4	60
5	80
6	95
6.5	100

Table 1: CrowdStrike Global Outage: Service Restoration Timeline

THE IMPACT OF THE OUTAGE: CASE STUDIES OF AFFECTED COMPANIES

Technology: Microsoft

The global outage massively affected Microsoft's capacity to deliver its services and products. The tech giant relies on advanced cybersecurity measures to safeguard its systems and digital infrastructure. When the outage occurred, the company's internal security operations were disrupted, impacting its ability to protect its cloud services and products. The outage caused a temporary lapse in security, leaving Microsoft's systems vulnerable and highly exposed to possible cyberattacks and threats. The company's customers, especially those who rely on its cloud services to run operations, were also heavily affected by the disruption. Most reported disruptions in their services, leading to operational issues and delays in service delivery [4]. The incident exposed Microsoft to public scrutiny; the company's reputation in delivering secure cloud services was questioned. Critical clients, mainly banking institutions like Nedbank, FNB, and Standard Bank, and media companies relying on Microsoft's cloud services experienced glitches and other issues, alongside the exposure to vulnerabilities.

Aviation: Delta Airlines

Delta Airlines was among the companies hit hard by the global outage. The impact was largely felt in the company's daily operations, resulting in flight cancellations and grounding of airplanes. During the outage, the company's booking, flight management, and check-in processes were affected, leaving thousands of customers stranded in airports for hours [5]. Due to the outage, the company's staff and customers could not access real-time data about flight movements and related activities. Also, the communication systems were down, making it difficult for Delta Airlines to manage flight schedules and respond to the operational issues that arose quickly. This disruption in normal operational activities put the airline's reputation on the line as customers were frustrated and uncertain about their travel plans. The impact also left the company's security systems vulnerable and exposed to cyberattacks. Cybersecurity is essential in critical sectors, such as the airline industry, as it protects customer data and critical IT systems [6]. During the temporary outage, Delta Airline's cyber defense was crippled, which posed a great risk to sensitive customer data and other breaches. The impact was not resolved quickly; days later, normal operations had not resumed at the Airline, raising further concerns, according to [7]. Delta's rivals resumed to normalcy in a day or two. However, Delta took more days, leaving customers frustrated.

Healthcare: National Health Service (NHS)

In the United Kingdom, the National Health Service (NHS) was also affected by the outage. The NHS is the UK's largest healthcare institution, offering comprehensive public health services. The government governs the institution. The CloudStrike outage negatively affected service delivery and normal operations in the institution. Patients suffered as appointment and GP prescription systems were flawed [8]. Other affected critical functions of the NHS included diagnostic services and electronic health record systems. This resulted in delayed patient care, a slowdown in administrative operations, and cancellation of appointments. The events of Friday 18 worsened the strain on the UK's healthcare system, which was already strained. The NHS experienced disruption in usual operational activities, and its security systems were exposed to serious threats during the temporary loss of cybersecurity defense. Healthcare organizations require robust and advanced security systems because of the sensitive patient data and information they store [9]. The sensitive data usually includes people's personal health information and personally identifiable information, which, if exposed to threat actors, may pose legal charges and other issues to the institution. Data breaches have not been reported, and the institution's IT department is back; service delivery is still slow.

FINANCIAL INSTITUTIONS

JPMorgan Chase was among the financial institutions negatively affected by the outage. When the outage occurred, JPMorgan experienced disruptions in processing transactions, which resulted in delays and customer satisfaction [10]. Other financial institutions that were also affected included the Bank of America and the Commonwealth Bank of Australia. In Australia, customers transacting through the country's largest bank (Commonwealth Bank) expressed frustrations as they could not make money transfers. In the UK, the London Stock Exchange was also affected by the technical glitch, resulting in a delayed display of opening trades [11]. Like the healthcare industry, financial institutions keep sensitive customer data, which was left vulnerable during the outage.

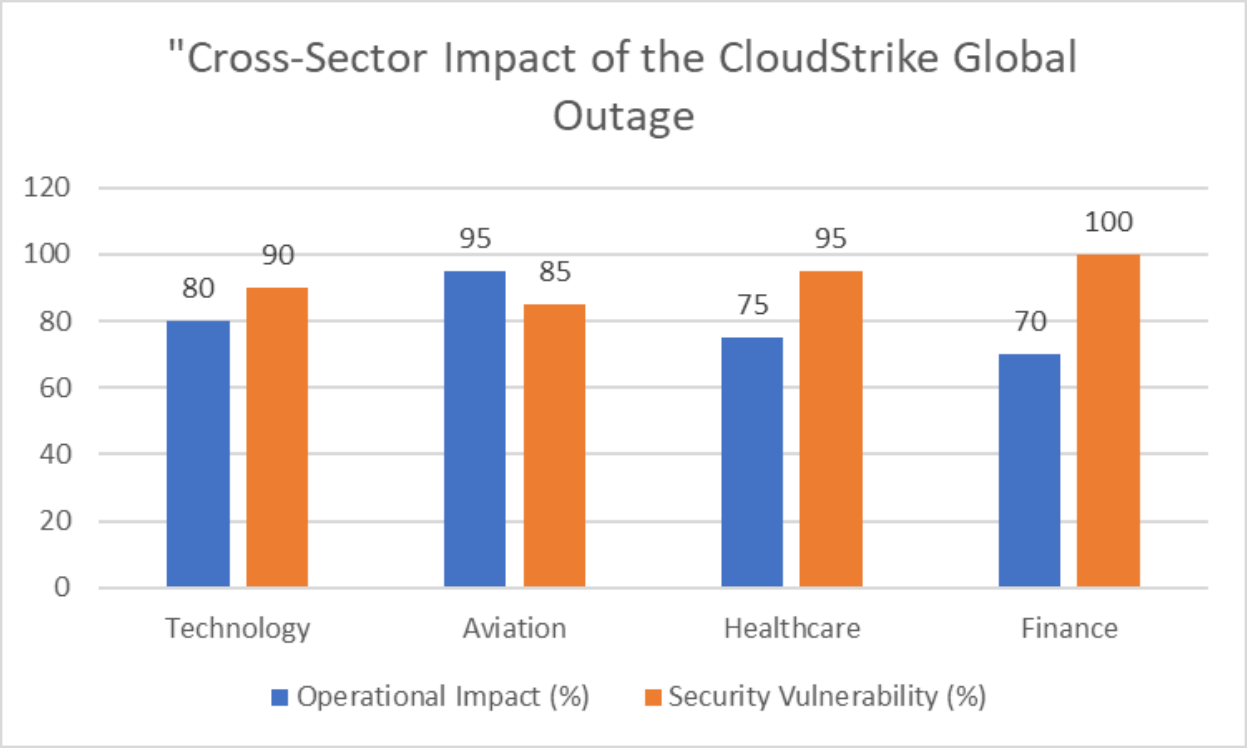

Fig. 1: Comparative Analysis of CloudStrike Outage Effects on Major Industries

THE CHALLENGE OF USING SAAS IN THE FUTURE

The use of SaaS (Software as a Service) applications has increased over the past few years. According to [12], many enterprises prefer this computing model because of its increased ability for hosting and lower costs. One of the cost-effective aspects of this service is that it removes the need for organizations to host their servers [17]. With the servers hosted by the providers, businesses will save the costs needed for the cloud infrastructure, including the associated maintenance costs. SaaS presents numerous user shortcomings, such as dependence on cloud infrastructure, security concerns, integration and compatibility issues, vendor lock-in, and performance reliability.

DEPENDENCY ON CLOUD INFRASTRUCTURE

Using SaaS platforms requires reliance on cloud infrastructure, which is often a single point of failure. For instance, in the CloudStrike event, reliance on cloud infrastructure implies that any disruption or malfunction in infrastructure causes widespread interruptions in service delivery. Generally, there is a high dependency on the providers in SaaS cloud computing models [18]. The main contributing factor is that the providers host the service, and all associated responsibilities lie on them. As a result, organizations become dependent on the services delivered by the providers to run critical business operations [18]. If the provider runs out of business or becomes insolvent, organizations and other service users risk losing access to the application, including their critical data and investments made in the process [18]. The out-of-premises aspect of SaaS platforms gives more power to the providers, leaving users with limited choices in the event of an outage.

SECURITY CONCERNS

Despite being scalable and flexible, SaaS platforms are highly targeted by cybercriminals due to the sensitive data and information they store [13]. Besides, any data breaches in the cloud infrastructure result in massive consequences, such as reputational damage, financial losses, and regulatory fines and penalties; ensuring data security is integral, nonetheless, difficult. Additionally, [17] explains that the dependence on third parties in SaaS cloud computing models increases security risks for users. Generally, SaaS security entails the defense or protection of user's corporate data and other privacy aspects of cloud applications. The SaaS applications also store vast amounts of data, which users can access from any device; this aspect puts critical data and privacy at risk.

Additionally, SaaS popularity has increased, attracting more users and companies to embrace its tools. The downside is that it has raised novel security issues, including phishing attacks, the risk of client data exposure to third parties, and new malware [17]. Further, users have little to no control over SaaS security control; the responsibility solely lies on the providers. These security concerns prompt providers to implement robust SaaS security measures and best practices.

PERFORMANCE AND RELIABILITY ISSUES

SaaS architectures also pose performance and reliability concerns. Generally, the performance of SaaS applications depends on the service provider's infrastructure and network conditions. Businesses relying on a particular provider's infrastructure become affected in the event of a downtown, and their operations are disrupted. This issue is evident in the recent global outage, when businesses relying on CloudStrike and Microsoft's infrastructure experienced disruptions. Performance and reliability issues in SaaS platforms have been explored by [16]. According to this study, Quality of Software (QoS) is a key performance factor for cloud users. This factor greatly impacts user experience and satisfaction. One element that determines the performance of SaaS software is response time; if the time is too long, the user Service Level Objective/Agreements become violated. Usually, this impact results in large economic losses alongside user dissatisfaction [16]. Besides, it is challenging for SaaS providers to examine performance-related issues, such as large data, insufficient information, and complex interaction [16].

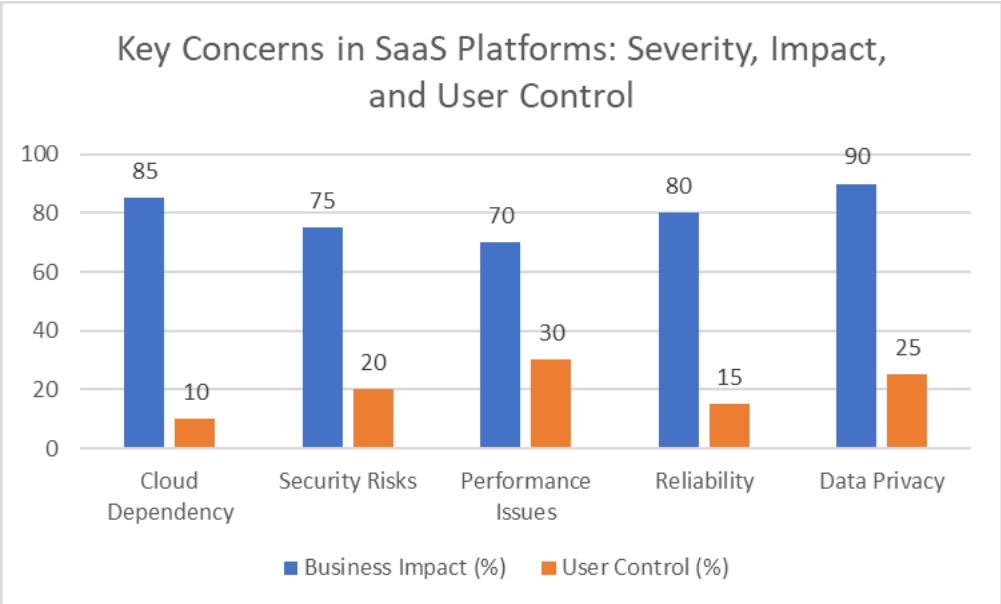

Fig. 2: Comparative Analysis of SaaS Platform Vulnerabilities and Their Business Implications

VENDOR LOCK-IN

Another key challenge of SaaS is that organizations become overly dependent on a single provider, causing a vendor lock-in. This usually limits their flexibility to switch to other providers. Additionally, data portability issues are also likely to arise, affecting migration to other platforms. According to [15], vendor lock-in is a growing concern for businesses operating on cloud platforms. The key issue with vendor lock-in is that it limits the capacity and flexibility of businesses to switch from one cloud provider to another in the future. Generally, switching to different providers is expensive [15]. For a successful switch, businesses must re-architect their systems and retrain their staff, which raises unexpected costs [15]. As a result, in poor service delivery or performance, users must stick with the initial vendors, especially if they are unwilling to spend unexpected additional costs.

MITIGATION STRATEGIES

Organizations can address the dependence on cloud infrastructure issues by implementing failover and redundancy measures. For instance, they can enforce multi-region deployments, which are significant in ensuring that if an issue is encountered in one region, others can step in and slow down the associated downtime. Security concerns can be addressed by deploying comprehensive security measures, such as multi-factor authentication, end-to-end encryption, and continuous monitoring [14]. Performance and reliability can be ensured through establishing Service Level Agreements, which will hold the providers accountable for poor performance and other shortcomings on their end.

Challenge	Impact Severity (1-10)	Cost to Mitigate ($K)	Mitigation Effectiveness (%)
Vendor Lock-in	8	150	70
Data Portability	7	100	75
Cloud Dependency	9	200	85
Security Concerns	9	250	90
Performance Issues	7	120	80
Reliability	8	180	85

Table 2: SaaS Challenges: Impact, Mitigation Costs, and Effectiveness

CONCLUSION

The recent global outage, caused by a software update malfunction, caused glitches and disruptions in businesses relying on the firm's services and products across several sectors. Critical sectors like healthcare, aviation, and finance were largely affected. The outage exposed the shortcomings of relying on SaaS platforms and applications. During the outage, the company's security systems were left vulnerable and exposed to threat actors.

Similar issues can be avoided in the future if providers like CloudStrike and Microsoft establish multi-region server deployments. This will ensure that if servers in one region fail, others in other regions can take over and minimize downtime. Businesses can also take actions like establishing robust security measures and signing Service Level Agreements to hold providers accountable for failures and disruptions.

REFERENCES

[1] N. Robins-Early, "What is CrowdStrike, and how did it cause a global Windows outage?" *The Guardian*, Jul. 19, 2024. Accessed: Jul. 28, 2024. [Online]. Available: https://www.theguardian.com/technology/article/2024/jul/19/what-is-crowdstrike-microsoft-windows-outage#:~:text=An%20update%20to%20one%20of

[2] G. Petras, J. Loehrke, and R. Padilla, "CrowdStrike impact: How a global IT outage unraveled the world's tech," *USA TODAY*, Jul. 19, 2024. https://www.usatoday.com/story/graphics/2024/07/19/crowdstrike-outage-global-effect/74467247007/

[3] E. Rothenberg, "Timeline: How the CrowdStrike outage unfolded," *CNN*, Jul. 20, 2024. https://www.cnn.com/2024/07/20/tech/timeline-crowdstrike-system-outage/index.html

[4] M. Cerullo, "CrowdStrike says more than 97% of Windows sensors are back online," *www.cbsnews.com*, Jul. 26, 2024. https://www.cbsnews.com/news/crowdstrike-outage-microsoft-windows-restored/#:~:text=Microsoft%20estimates%20the%20error%20took (accessed Jul. 28, 2024).

[5] C. Contreras, "Why is Delta still canceling flights when other airlines quickly restored service?" *Northeastern Global News*, Jul. 23, 2024. https://news.northeastern.edu/2024/07/23/crowdstrike-outage-delta-airlines/ (accessed Jul. 28, 2024).

[6] G. Dave, G. Choudhary, V. Sihag, I. You, and K.-K. R. Choo, "Cyber Security Challenges in Aviation Communication, Navigation, and Surveillance," *Computers & Security*, vol. 112, p. 102516, Oct. 2021, Doi: https://doi.org/10.1016/j.cose.2021.102516.

[7] M. Salerno, "What's going on with Delta Air Lines? Why CrowdStrike's still canceling flights in Phoenix," *The Arizona Republic*, Jul. 23, 2024. https://www.azcentral.com/story/travel/airlines/2024/07/23/delta-air-lines-flights-canceled-crowdstrike/74504091007/#:~:text=The%20outage%20caused%20problems%20with (accessed Jul. 28, 2024).

[8] R. Davies, "UK doctors and travel firms warn of backlog after global IT outage," *The Guardian*, Jul. 21, 2024. Accessed: Jul. 28, 2024. [Online]. Available: https://www.theguardian.com/society/article/2024/jul/21/nhs-warns-of-considerable-backlog-in-gp-services-after-global-it-outage

[9] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, "Towards insighting Cybersecurity for Healthcare domains: A comprehensive review of recent practices and trends," *Cyber Security and Applications*, vol. 1, no. 100016, p. 100016, 2023, Doi: https://doi.org/10.1016/j.csa.2023.100016.

[10] L. Noonan, D. Wee, L. Kehnscherper, and A. Narayanan, "Trading Disrupted, Bankers Go Home After Outages Sweep Globe," *Bloomberg.com*, Jul. 19, 2024. Accessed: Jul. 28, 2024. [Online]. Available: https://www.bloomberg.com/news/articles/2024-07-19/some-jpmorgan-employees-unable-to-log-on-amid-global-outages

[11] Aljazeera, "Global IT outage causes chaos, disrupting airlines, banks, media, telecoms," *Al Jazeera*, Jul. 19, 2024. https://www.aljazeera.com/economy/2024/7/19/australia-struck-by-major-it-outage-hitting-banks-media-telecoms#:~:text=Multiple%20other%20sectors%20were%20also (accessed Jul. 28, 2024).

[12] M. Gupta, D. Gupta, and P. Rai, "Exploring the Impact of Software as a Service (SaaS) on Human Life," vol. 10, Jan. 2024, Doi: https://doi.org/10.4108/eetiot.4821.

[13] M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas, and S. U. Rehman, "Cyberattacks and Security of Cloud Computing: A Complete Guideline," *Symmetry*, vol. 15, no. 11, p. 1981, Nov. 2023, Doi: https://doi.org/10.3390/sym15111981.

[14] M. Chauhan and S. Shiaeles, "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions," *Network*, vol. 3, no. 3, pp. 422–450, Sep. 2023, Doi: https://doi.org/10.3390/network3030018.

[15] T. Weldemicheal and S. Johansson, "Vendor lock-in and its impact on cloud computing migration Main Subject area: Informatics," 2023. Available: https://www.diva-portal.org/smash/get/diva2:1787688/FULLTEXT01.pdf

[16] R. Wang, X. Tian, and S. Ying, "Performance issue monitoring, identification and diagnosis of SaaS software: a survey," *Frontiers of Computer Science*, vol. 19, no. 1, 2024, Available: https://journal.hep.com.cn/fcs/EN/10.1007/s11704-023-2701-0

[17] M. Humayun, M. Niazi, M. F. Almufareh, N. Z. Jhanjhi, S. Mahmood, and M. Alshayeb, "Software-as-a-Service Security Challenges and Best Practices: A Multivocal Literature Review," *Applied Sciences*, vol. 12, no. 8, p. 3953, Apr. 2022, Doi: https://doi.org/10.3390/app12083953.

[18] T. Smith, "The Challenges and Considerations of SaaS: A Closer Look," *www.linkedin.com*, May 16, 2023. https://www.linkedin.com/pulse/challenges-considerations-saas-closer-look-tim-smith (accessed Jul. 29, 2024).

Citation: Sandeep Reddy Gudimetla, Cloudstrike Impact on Global Outage and The Challenge of SAAS In the Future, International Journal of Computer Engineering and Technology (IJCET), 15(4), 2024, pp. 472-480

Abstract Link: https://iaeme.com/Home/article_id/IJCET_15_04_041

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_15_ISSUE_4/IJCET_15_04_041.pdf

✉ **editor@iaeme.com**