A Study on Blockchain Technology as a Dominant Feature to Mitigate Reputational Risk for Indian Academic Institutions and Universities

Rangi, Pradeep Kumar and Aithal, Sreeramana

College of Management Commerce, Srinivas University, Mangalore, India, College of Management Commerce, Srinivas University, Mangalore, India

31 December 2020

A Study on Blockchain Technology as a Dominant Feature to Mitigate Reputational Risk for Indian Academic Institutions and Universities

Pradeep Kumar Rangi[1] & P. S. Aithal[2]

[1]Research Scholar, College of Management & Commerce, Srinivas University, Mangalore, India
OrcidID: 0000-0002-2052-9054; E-mail: pradeep.rangi@gmail.com

[2]Professor, College of Management & Commerce, Srinivas University, Mangalore, India
OrcidID: 0000-0002-4691-8736; E-mail: psaithal@gmail.com

December 2020

ABSTRACT

The paper-based certification is prone to manipulation and vulnerable to fraud. Instances of fraudulent degrees, manipulation of academic records, or compromised academic programs adversely impact and damage an academic institution's credibility. It also affects the Indian universities' mission and prospects of the students graduating from such a university. What makes reputational risk a unique risk is that it may arise both from the university or institution's failure or the action outside the university. It is, therefore, essential to take an enterprise risk management approach to mitigate reputational risk. Robust credential verification and validation protocols are the most important protections against fake certifications. The legacy certificate verification solutions are highly centralized, i.e., utterly dependent on the issuing authority for certificates. Despite the University Grants Commission (UGC) taking strict measures against individuals, Indian universities, colleges, and associations, we do come across several acts of torts. Some of the technology-savvy institutions have moved to digital certificates and digital signatures. However, this has an inherent weakness, i.e., they still need to rely on a trusted third party. Blockchain technology has three foundational components, data structures based on cryptography that make it secure and tamperproof, consensus protocols that allow it to function truthfully and without any central authority or a third party smart contracts, which provide efficiency and business value transactions. These key features of blockchain, if implemented appropriately, effectively has the potential to mitigate the inherent reputational risk arising from fraudulent academic certificate matters. Niti Ayog is currently developing a blockchain-based proof of concepts to solve traditional educational qualifications related to identity misrepresentation and document forgery. The immutability attribute of the blockchain ensures that tampering and manipulation of the record are not attainable. This paper focuses on the reputational risk Indian universities and institution may face when its certifications are not easily verifiable. Therefore, it becomes easy targets for bad actors to exploit vulnerabilities by issuing counterfeit certificates. Secondary published data, including various scholarly journals, reports, industry publications, and website sources, are utilized to develop this case study. The paper also explores how blockchain technology with specific reference to the proof of concept SuperCert proposed by Niti Ayog for Indian academic institutions may provide effective preventive control to overcome such reputational risk using the ABCD analysis framework as a research case study.

Keywords: Reputational risk, Academic Certification, Blockchain, SuperCert, Enterprise Risk Management, Indian Universities

1. INTRODUCTION :

Reputational risk refers to unfavorable stakeholder perceptions, media coverage, or uncontrollable incidents to harm an academic institution's credibility, thus impacting its mission and prospects of the students graduating from such institutions. What makes reputational risk a unique risk is that it may arise both from the Indian university and academic institutions' failure or the action outside the university. Reputational risks may also arise from conditions outside the sector (academic sector in this case) but still have massive consequences for the industry and stakeholders [1]. To effectively identify and mitigate potential reputational risks, academic institutions must develop, adopt, and illustrate culture to set the tone. The risk framework adopted by the educational institution should also be reviewed periodically and enhanced with a possible technological solution that acts as both a strong deterrent and mitigant and promotes transparency. A Technologically supported risk management framework will provide an efficient and effective means of identifying, evaluating, and mitigating reputational risks. The critical consequences arising from the reputational risk event may include an adverse impact on the institution's ranking and difficulty attracting the best talent, resources, and students [2]. However, the effects may be far-reaching as this damages the institution's reputation and the region, students, and other stakeholders associated with such institutions. An academic institution's reputational risk may arise from several functional areas, including the admission practices, campus environment, scholarship policies, public statements, research initiatives, and the educational program's quality and integrity. This paper mainly focuses on the reputational risk institution may face when its certifications are not easily verifiable. Therefore, it becomes easy targets for bad actors to exploit vulnerabilities by issuing counterfeit certificates.

The Physical examination of records and the appointment of agencies to verify are not very efficient, sometimes resulting in candidates from specific universities not being shortlisted for the number of opportunities. The common critique of the prevailing certificate verification solution has been as follows. The legacy certificate verification solutions are highly centralized, i.e., utterly dependent on the issuing authority for certificates i.e. Indian universities or academic institutions. To ensure additional caution, some entity relying on a certificate seeks to obtain the confirmation or stamping from the Ministry of HRD. Such verification is primarily manual. Therefore, verifications are usually carried out by personal visits, postal systems, e-mails, phone calls, or websites; the process is laborious, inefficient, and time-consuming. And finally, these traditional verification solutions are easily subject to manipulation and tempering [3]. Academic institutions can tremendously enhance their reputation and gain significant goodwill among stakeholders if they can provide an efficient means of verifying credentials and fast-tracking the verification process. In an overly simplified form, A blockchain is a time-stamped sequence of permanent or immutable data records governed by a cluster of nodes or computers (distributed consensus), not handled by any single individual. Every one of these data blocks (i.e., block) is protected and bound by cryptographic rules (i.e., chain) to each other [4]. The renowned, but perhaps not the sole, blockchain is right at the center of modern crypto asset-based currency, i.e., the modern money system of Bitcoin [5],[6],[7]. Blockchain is a system that allows users to know with certainty what has happened, the time, and to validate the same occurrence to others without having an intermediary entity. This very nature of blockchain can solve the fundamental issues of vulnerability, security, and privacy related to the educational certification process and secure records [8] [9]. The very nature of blockchain design includes a complete democratized approach, i.e., a network with no central authority or agency. This fundamental characteristic of blockchain and both shared and immutable records make it transparent; anything, therefore, built on this technology, is significantly enforced transparency and accountability [7]. Therefore, the use of blockchain has multiple benefits; it increases transparency, enforces accountability through smart contracts, and finally incentivizes through efficient risk mitigation.

NITI Aayog, in association with the ISB and Bitgram, has attempted to remediate the complexities and inherent issues with academic credentials through a blockchain-based approach. The solution, SuperCert, has a licensed blockchain infrastructure that involved decentralization, identity encryption, and identity interlinking to address the deficiencies in existing certification verification solutions. SuperCert would

enable creating a hashed version of the student's certificate (i.e., block) and allowing verification of the certificate using the student and the university's public key. The immutability attribute of the blockchain ensures that tampering and manipulation of the record are not attainable [3].

2. RELATED WORKS :

Maintaining academic credentials in a decentralized, distributed, and democratized repository would significantly increase and protect its reputation, lead to an efficient verification process, and provide strong protection against counterfeit certificates. Blockchain technology in education is still primitive; it could provide a critical much-needed medium for restructuring the certification solutions. Academic researchers have significantly impacted this direction and have suggested several new features and changes—some of the scholarly published papers on the blockchain in academics and reputational risk outlined in Table 1.

Table 1 : Related publications on Blockchain in academics and reputational risk by different researchers

S. No.	Themes	Focus Area
1	Enterprise risk management	Enhancing Understanding of risk management in academics and its effect on universities. [2]
2	Reputational Risk	Sources of reputational risk. Though the paper is written with the insurance sector in mind, some of the findings are very relevant for the academic industry. [1]
3	Distributed Tech Ledgers solution for academic record, reputation and reward	Trials of a private blockchain or storing educational records and reputation management for educational systems. [8]
4	Blockchain in academics	It describes case studies of implementations at the Open University UK, the University of Nicosia, MIT and within various educational institutions in Malta [10]
5	Blockchain in academics	Exploring block-chain based projects, underlying protocols, and the services are offered by the existing educational projects using block-chain [11]
6	Blockchain in academics	An approach using blockchain technology implemented in University Fernando Pessoa. [12]
7	Blockchain	Recent academic literature on blockchain primarily in the business and economics. [13]

3. OBJECTIVES OF THE STUDY :

This paper focuses on the reputational risk institution may face when its certifications are not easily verifiable. Therefore, it becomes easy targets for bad actors to exploit vulnerabilities by issuing counterfeit

certificates. The paper also explores how blockchain technology with specific reference to SuperCert proposed by Niti Ayog may provide effective preventive control to overcome such reputational risk.

(1) To identify/explore the impact of reputational risk in relation to certificates in Indian Universities.
(2) To study limitation of existing certificate solution prevalent in Indian universities in preventing certificate counterfeits
(3) To provide an overview of Niti Ayog's SuperCert and other blockchain certification solutions
(4) To review Permissioned blockchain using ABCD in the context of SuperCert

4. RESEARCH METHEDOLOGY :

Secondary published data, including various scholarly journals, regulatory notifications, niti ayog reports, industry publications, and website sources, are utilized to develop this case study and collect published data sources. This article describes and analyses blockchain technology as an effective mitigant for reputational risk for Indian universities. Analysis of determinant issues, affecting factors, and constituent elements of proposed risk mitigants analyzed under four constructs, i.e., as proposed by ABCD model, Advantages, Benefits, Constraints, and Disadvantages are analyzed using the ABCD model [14], [15].

5. REPUTATIONAL RISK VULNERABILITIES :

Reputational risk is one of the strategic stakes for academic institutions. It may arise from primary sources such as policy decisions, the institution's business strategy, or secondary sources such as failure to execute actors outside the institution's educational programs or actions. To effectively manage and mitigate reputational risk, begin with determining the institution's risk appetite. Reputational risk is subjective, and hence it is recommended that stakeholders be segmented to understand the likely impact in an objective manner. Next, find the sources of risk; remember, what makes reputational risk unique is that it may arise both from the university or institution's failure or the action outside the university. Determine controls to effectively mitigate the reputational risk and assess control gaps, both for control design and execution. Finally, periodically evaluate the effectiveness of control and take corrective actions. This paper's scope is a specific component source of reputational risk for institutions, i.e., the threat from counterfeit and fake certificates and inefficient verification process. The key sources of such risk include misconduct internal to the institution or of external actors:

(1) External event - Fake certificate obtained from a diploma mill [16] [17].
(2) External event – Fake certificate is printed by individual with the help of modern printing software to replicate style and security features etc. or deceitful tempering or alteration of legitimate document [16] [17].
(3) Internal event – Institutions faculty misconduct (including bribery, breach of contract) e.g. provides backdated confirmation of assignment submission, update grades to passing marks etc. [17] [18].
(4) Internal event – Institutions administrative staff misconduct e.g. staff corrupts institutions databases for key academic record including enrolments to provide a validity to the fake degree and diplomas [17][19].

6. LIMITATION OF EXISTING CERTIFICATE VERIFICATION SYSTEMS :

The legacy certificate verification solutions adopted by Indian universities and other stakeholders are highly centralized, i.e., utterly dependent on the issuing authority for certificates. An entity relying on a certificate sometimes seeks to obtain the confirmation or stamping from the Ministry of HRD. Such verification is primarily manual. Therefore, verifications are usually carried out by personal visits, postal systems, e-mails, phone calls, or websites; the process is laborious, inefficient, and time-consuming. And finally, these traditional verification solutions are easily subject to manipulation and tempering. Some of the technology-savvy institutions have moved to digital certificates and digital signatures. However, this has an inherent weakness, i.e., they still need to rely on a trusted third party. Thus, the need for a decentralized trust system that is verifiable, fraud-proof, and real-time [3].

7. BLOCKCHAIN :

Blockchain technology has three critical foundational components. Data structures based on cryptography that make it secure and tamperproof, consensus protocols allow it to function truthfully and without the need of any central authority or a third party, and smart contracts, which provide efficiency and business value transactions. [20]. The key features of blockchain, if implemented appropriately, effectively mitigates identified sources of risk in Section 5 and overcome the limitation of traditional verification solutions include:

(1) Protects integrity - Each node on the blockchain network has a copy of the ledger. Any addition or modification to the block or transaction requires every node to validate and confirm transaction validity. If the majority believes it's true, it's submitted to the ledger. This feature of blockchain promotes transparency, which makes it more corruption-proof.
(2) Decentralized - The blockchain is a decentralized network that does not require a controlling authority but is maintained by a community of participants or nodes.
(3) Enhanced Security - Blockchain removes the requirement for a central authority; no one node or participant can easily manipulate any network features to their advantage. On top of that, the blockchain encryption element assures another layer of protection for the network.
(4) Distributed Ledger – Blockchain ledgers do not require control by one participant, instead of managed by network participants. This feature of blockchain ensures computing resources are distributed through machines and provide better performance and integrity of data or blocks.
(5) Consensus – The core at the blockchain is the consensus algorithm mechanisms. Each blockchain has a consensus to help the network make decisions.

The features mentioned above and the immutable design of the blockchain ensure that the tampering of the certificate is not possible, i.e.both the substance of the academic documents and the candidates' identity. The tech stack for the blockchain-based application can be in-house, or more could be in the form of a more efficient solution, i.e., blockchain-as-a-service (BaaS) usage of blockchain components with ease, a cloud provision for blockchain. Through facilitating the distribution, and not just the copy, Blockchain seems to be the cornerstone of a unique conception of the internet [21].

8. SUPERCERT – REVIEW :

Blockchain models can broadly be categorized as permissioned and permissionless blockchains based architecture. Permissioned model is often referred to as private blockchains and requires permission to participate. Permissionless blockchain allows all or anyone to participate and join the network. The model's use depends on several factors, including the eco-system and capabilities one would like to propose [13]. In its latest paper, 'Blockchain: Indian Strategy,' Niti Aayog identifies the four-use cases of blockchain technology in areas such pharmaceutical supply chain, fertilizer subsidies, the verification of university certificates, and the transition of land records. NITI Aayog has designed a proof of concepts in these areas to enhance efficiency and recognize the complexities of implementation. The method presented in the proof of concept for the authentication of university certificates is SuperCert. SuperCert is proposed as a permissioned model-based architecture. The approach requires decentralized and interlinked identification encryption. The process of issuing certificates begins with creating student identity, i.e., Superidentity. A public and a private key assigned to the student, which constitutes or provides a unique blockchain identity (avatar). The process includes the Super certificate issued by the institution or university, linked with the candidate's Superidentity (i.e.creation of a hashed version of the credential) on the blockchain), which can help verify the certificate utilizing the public key of the student and the public key of the university [3]. Table 2 below examines the effectiveness of proposed proof of concept approach SuperCert to mitigate sources of reputational risk identified in section 5 of the paper.

Table 2: SuperCert features assessment against the sources of reputational risk

Sr. No.	Potential Sources of Fraud	Mitigation

1	External event - Fake certificate printed by individual or criminals [16] [17] or obtained from a diploma mill [16] [17]	**Mitigated** **1.** SuperCert is proposed to be permissioned architecture. It may be reasonable to assume that institutes or associations not meeting UGC/ MHRD qualification criteria will not be able to join the proposed blockchain as one of the participant to issue SuperCerts **2.** The solution includes decentralized and intelligent identity encryption. Intelligent identity is interlinked for granting the educational certificates by Indian universities. This feature of the SuperCert mitigates Idneitity impersonation and counterfeit degree related risk
2	Internal event – Institutions faculty or administrative staff related misconduct (including bribery, breach of contract) e.g. provides backdated confirmation of assignment submission or administrative staff corrupts institutions databases for key academic record including enrolments to provide a validity to the fake degree and diplomas [17] [18]	**Not Mitigated** The immutable nature of blockchain provides an opportunity to bring more transparency in tracking students' academic history. Further use cases may be developed to track students' academic records from inception, i.e., entrance, registration, enrollment dates, attendance, projects and assignment submissions, examinations, grades, and pass-out dates.

9. ABCD QUALITATIVE ANALYSIS OF BLOCKCHAIN AS REPUTATIONAL RISK MITIGANT :

ABCD analysis tool provides an opportunity to evaluate the benefits, advantages, constraints, and disadvantages of any proposed solution, mitigant, concept, architecture, technique, product, or service [14], [15], [22]–[24].

8.1 Advantages:

(1) A Certificate verification system based on blockchain technology provides decentralization, immutability, security, and transparency. Blockchains allow interlinking students' identity (SuperIdentity) with certification.

(2) Blockchain provides cryptography to secure the block. The current block is dependent on its adjacent completed block to complete the cryptography process and hence eliminate the risk of redundant and fraudulent entries.

(3) Blockchain use-cases and existing solutions, e.g., Blockcerts, EduCTX, UNIC, Hypercert along with literature in the area provide a reference for institutions to consider blockchain as a potential control design to mitigate reputational risk vulnerabilities

(4) Smart contracts lay for automatic transactions (academic report updates, verifications) triggered when the pre-set conditions are met. This feature of blockchain fosters trust and bring efficiency to the process

(5) Blockchain technology enables transactions to record in chronological order and time hence timestamped. Further, the same can be traced to the origin of the ledger, thereby increases transparency and promotes truthfulness

(6) The blockchain architecture offers both public, private, permissioned or permissionless deployment depending upon business model and use-case

(7) Adoption of such blockchain technology as part of an enterprise risk management approach aligns Indian universities to Niti Ayog's recommendations to enable a strategy for India to become a blockchain hub for research and development.

8.2 Benefits:

(1) Blockchain technology provides robust control design to mitigate counterfeit certificates
(2) Adoption of technology by university significantly boosts universities creditability, i.e., by offering ease of verification of records and add transparency in an academic program
(3) Blockchain provides an efficient means to the university stakeholders (including future recruiters in campus or offline hires) as enhances record verification speed and offers cost effectives means of verification
(4) Smart contracts provide a make verification process seamlessly and on a real-time basis, i.e., once the pre-set conditions are met. It significantly enhances academic institutions reputation among recruiters and will positively impact its ranking
(5) Adopting blockchain technology strengthens the overall risk assessment system of universities by way of automated controls. It positively encourages the institution to explore potential collaborations in the network of higher-trust participants.
(6) Improves efficiency of academic institutions processes, including admission, assignments, examinations, and tracking progress
(7) The solution act as a strong deterrent for the counterfeit academic certificates

8.3 Constraints:

(1) The lack of infrastructure and nascent developer community
(2) The initial cost of implementing the private or permissioned blockchain networks proposed in the Niti Ayogs SuperCert approach may be very high.
(3) Blockchain's immutable feature means there must be a golden source of data before a process is migrated to the blockchain. Several academic institutions may have difficulty in coming up with a single source of truth aminating from traditional database challenges
(4) Integration of blockchain with the existing databases and systems may limit the strategic design decisions.
(5) Legal and regulatory modifications may be required before adopting and piloting a successful blockchain based solution. e.g., easing of existing regulations through sandboxes

8.4 Disadvantages:

(1) Blockchain technology is more stable and secure than any legacy network. This does not imply, however, that it is not stable and secure. Blockchain networks can be targeted using 51 percent attack, Double-spending, DDoS attack, and Cryptographic cracking, to name a few vulnerabilities.
(2) Blockchain network depends on nodes to operate efficiently. The efficiency of the nodes is determined by the quality of the blockchain
(3) Multiple forms of blockchain networks are operating differently. This contributes to interoperability problems where these chains are unable to interact efficiently.
(4) Blockchain offers irreversible transactions, which also a disadvantage that intentional and unintentional errors may have a severe reputational impact
(5) Each blockchain transaction must be digitally signed. This feature certainly enhances transaction security; it also creates a bottleneck in the blockchain process and slows down the processing.

10. CONCLUSIONS :

The threat of potential impairment to Indian universities' or academic institutions' reputation and credibility and consequential impact on students' career opportunities emerging from any affiliation, behavior, or omission that stakeholders could deem unacceptable, immoral, or contradictory should be carefully monitored and mitigated. Isolated incidents of reputational risk will weaken stakeholder's confidence and adversely affect the credibility of the Indian universities. If implemented effectively, blockchain technology's inherent features could provide substantial mitigation against some of the identified reputational risks. As part of the institutes' enterprise risk management plan and institutes strategy, use-

cases may be proposed. Such use-cases may provide for evaluating various scenarios and potential blockchain architectures. Indian universities may adopt an interdisciplinary approach to review, assess, and validate risk institutes' risk profiles and risk decisions. Managing and designing a robust blockchain-based control design solution may require a diverse risk skill as this may impact multiple processes in university. While assessing the risk appetite and proposing and accepting control design, the institute must adopt an enterprise risk approach and carefully assess changes in its risk profile, i.e., is the risk profile modified or new risk introduced, which require careful remediation. The risk appetite of an academic institute usually informs the choice of blockchain and design architecture. A fully embedded enterprise risk management framework clearly defined ownership, and technology selection is foundational to effective risk management. Such an enterprise risk approach goes a long way in mitigating reputational risk and helps Indian universities achieve its long-term mission.

REFERENCES :

[1] Csiszar, E. and Heidrich, G. W. (2006), The question of reputational risk: Perspectives from an industry, *Geneva Papers on Risk and Insurance: Issues and Practice*, *31*(3), 382–394.

[2] Huber, M. (2011), The Risk University : Risk identification at higher education institutions in England, *Centre for Analysis of Risk and Regulation at the London School of Economic and Political Science*, *69*(1), 1-25.

[3] Roy, A. (2020), Blockchain: The India Strategy, *Niti Ayog*, *1*(1), 37–40.

[4] Lin, I. C. and Liao, T. C. (2017), A survey of blockchain security issues and challenges, *International Journal of Network Security*, *19*(5), 653–659.

[5] Nakamoto, S. (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, *Bitcoin: A Peer-to-Peer Electronic Cash System - Bitcoin.orgbitcoin.org*, *1*(1), 1–9.

[6] Sleiman, M. D. Lauf, A. P. and Yampolskiy, R. (2016), Bitcoin Message: Data Insertion on a Proof-of-Work Cryptocurrency System, *Proceedings - International Conference on Cyberworlds, 1(1)*, 332–336.

[7] Cao, S. Cao, Y. Wang, X. and Lu, Y. (2017), A Review of Researches on Blockchain, *57(1)*, 108–117.

[8] Sharples, M. and Domingue, J. (2016), The blockchain and kudos: A distributed system for educational record, reputation and reward, *Springer - Lecture Notes in Computer Science*, *9891*(1), 490–496

[9] Turkanović, M. Hölbl, M. Košič, K. Heričko, M. and Kamišalić, A. (2018), EduCTX: A blockchain-based higher education credit platform, *IEEE Access*, *6*(1), 5112–5127

[10] ALEX, G. F and CAMILLERI, A. F. (2017), Blockchain in Education, *Publications Office of the European Union*, *1*(1), 1–136.

[11] Alammary, A. Alhazmi, S. Almasri, M. and Gillani, S. (2019), Blockchain-based applications in education: A systematic review, *Applied Sciences (Switzerland)*, *9*(12), 1–18.

[12] Vidal, F. Gouveia, F. and Soares, C. (2019), Analysis of blockchain technology for higher education, *Proceedings - International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 1(1)*, 28–33.

[13] Xu, M. Chen, X. and Kou, G. (2019), A systematic review of blockchain, *Financial Innovation*, *5*(27), 1-14.

[14] Aithal, P. S. (2015), Study on ABCD Analysis Technique for Business Models, business strategies, Operating Concepts & Business Systems, *International Journal in Management and Social Science*, *4*(1), 98–115.

[15] Aithal, P. S., Shailashree, V.T. & Suresh Kumar, P. M. (2015), A New ABCD Technique to Analyse

Business Models & Concepts, *International Journal of Management, IT and Engineering (IJMIE)*, *5*(4), 409 – 423.

[16] Grolleau, G. Lakhal, T. and Mzoughi, N. (2008), An introduction to the economics of fake degrees, *Journal of Economic Issues*, *42*(3), 673–693.

[17] Sayed, R. H. (2019), Potential of Blockchain Technology to Solve Fake Diploma Problem, *University of Jyvaskyla, Department of computer science and Information systems*, *1*(1), 1–71.

[18] Osipian, A. L. (2008), Corruption in Higher Education: Does it Differ across the Nations and Why?, *Research in Comparative and International Education*, *3*(4), 345–365.

[19] Osobi, N. (2017), Uganda university awards over 1000 fake degree to Dinka students in 60 days, *South Sudan Liberty*. *1*(1), 1.

[20] Anascavage, R. and Davis, N. (2018), Blockchain Technology: A Literature Review, *International Finance Review*, *20*(1), 131-148.

[21] Bhuvana, R. & Aithal, P. S. (2020), Blockchain based Service: A Case Study on IBM Blockchain Services & Hyperledger Fabric, *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, *4*(1), 94 -102.

[22] Aithal, P. S. (2017), An Effective Method of Developing Business Case Studies Based on Company analysis, *International Journal of Engineering Research and Modern Education (IJERME)*, *2*(1), 16–27.

[23] Aithal, P. S. (2017), Company Analysis – The Beginning Step for Scholarly Research, *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, *1*(1), 1–18.

[24] Aithal, P. S. (2017), Industry Analysis – The First Step in Business Management Scholarly Research, *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, *1*(1), 1-13.

****