International Journal of Scientific Research in Multidisciplinary Studies
Vol.5, Issue.8, pp.148-154, August (2019)

Research Paper
E-ISSN: 2454-9312
P-ISSN: 2454-6143

A Study on Cyber Security Practices and Tips Awareness among E-Banking Services Users of Udaipur, Rajasthan

A. Adholiya[1*], S. Adholiya[2]

[1]Dept. of Management, Pacific Business School, Affiliated to Rajasthan Technical University, Udaipur (Rajasthan), India
[2]Dept. of Commerce and Management Studies, Central Academy Senior Secondary School, Sardarpura, Udaipur (Rajasthan), India

Corresponding Author: asia_1983@rediffmail.com, Tel.: +91-86196-02362

Available online at: www.isroset.org

Received: 26/Jul/2019, Accepted: 16/Aug/2019, Online: 31/Aug/2019

Abstract **–** Cybercrime threats and issues are presenting huge challenge in all the areas and scopes incorporating national security, personal information privacy and security, financial transaction safety and trust, website surfing, and so forth. So, in order to keep away from the cybercrime everybody must think about their own cyber security characteristics and should improve level of awareness for cyber security practices and tips to ensure safety measures for their devices and cyber activities. In order to analyze the familiarity of common e-banking services users with cyber security practices and tips in Udaipur, Rajasthan by concentrating on different security issues and threats associated with the web based activates either financial or non-financial a well-structured questionnaire review technique was used. Users of electronic banking or advanced banking services were the respondents, and their feedbacks were statistically assessed through F-test and regression analysis to identify the significance of level of awareness for cyber attacks and threats, and effect of bank and socio-economic profile on it. Statistics of the test helped to interpret that socio-economic variables plays vital role in driving the customers' level of awareness for cyber security threats and attacks, and tips and practices. Bank customers of Udaipur district are having good set of knowledge of cyber threats and security issues and challenges, tips and practices.

Keywords **-** Cyber Security, Cybercrime, Cyber Threats, Bank, E-Banking, Awareness

I. INTRODUCTION

Internet or web based services under the aegis of fast and integral development of information and communication technology tool and practices in economical, social, political and financial platforms are continuously increasing the number of internet users and the growth is multifold, which leads into new kind of challenges in the technology enabled activities basically in the form of cyber threats. The landscape of accepting the electronically enabled banking activities in the nation is majorly driven through the government schemes and initiatives. New technologies such as artificial intelligence, Big Data, Internet of Things, 3D visualization, Cloud and so forth are evolving the business practices and methods of doing banking for the user and the banks and these all can lead into growing cyber threats.

Cyber or Digital security alludes to the assortment of technological advancements, procedures, and practices intended to protect network systems, electronic gadgets or devices, and data from any kind of service attack, unauthorized information access or tampering, and so forth. Cyber security may likewise be known as data security. Cyber security is very significant on several grounds such as government services and facilities, military, corporate, budgetary, and medicinal associations, and several phenomenal measures of information on PCs and different electronic gadgets. Individual and organizations transmit several confidential information crosswise over systems and to different electronic gadgets, and digital security depicts the control over the transmitted data ensuring that the frameworks used to process or store it is safe and reliable. Cyber security confirms the confidentiality and integrity of the data or the information and mange the reliability of the same with the complex set of configurations. With the advent of information technology in banking and related activities including the electronic payment system services had offered virtual connection to the users with their bank accounts with the permission of banking and resulting into the increasing risks from the customer end as well as the service provider end. As the digital or cyber security may be helpful for the users to manage their several threats related to banking such as loss of personal and confidential information (Account Number, Personal Details, Financial

Details, Passwords, Transaction Details and so forth), denial of services, loss of data, phishing, malpractices with the account, theft of identity and many more. In order to manage the problems and challenges related to internet based activities especially in banking and commerce, technology is becoming more sophisticated and rich; cyber threats are also becoming more complex and unique.

As the banking activities and its users are considered as the most vulnerable profile for the cyber attack and malpractices because of lack of knowledge, awareness and acquaintance for the secure and confidential cyber practices. So, it sought to assess the electronic banking users' level of awareness for the cyber security practices and tips for the Udaipur district as very few studies have been performed focusing on the topic. The present research work evaluated the extent of knowledge and awareness for the cyber security programs, cyber threats, common tips and practices, essentials to be followed for safe banking, do's and don'ts, common mistakes etc among the electronic banking users of Udaipur district of Rajasthan.

Some of the major cyber attacks or threats identified in year 2018 and respondents were asked to rate their level of awareness for them is:

1. Attacks through the underlying Blockchain technologies
2. Supply Chain attacks
3. Attacks through Mass Media
4. ATM malware Intrusion
5. Attack on Cypto Platforms
6. Traditional Card Frauds
7. Internet Banking Trojans
8. PC and Mobile Oriented Banking attacks
9. Theft of Biometric Data
10. PoS attacks
11. Ransomware
12. Social Engineering
13. Identity Theft
14. Synthetic Fraud
15. Phishing

Awareness Issues and Practices to be followed in Online or Internet Banking:

1. Account with two factor authentication
2. Create Strong Password and Timely Update the Password
3. Updated Security Software in PC
4. Access account from Secure Location
5. Remember to Logout
6. App lock to payment and mobile apps
7. No sharing of personal and confidential information especially password, PIN, etc.
8. Always be alert of Fraudulent Calls, SMS etc., do not reply
9. Remember the security codes rather following the practice of saving them
10. Uninstall "Any Desk' app, if not required with immediate effect.

Rest of the paper is organized as follows, Section I contains the introduction of cyber threats and security issues, cyber and digital security, major cyber attacks and threats of 2018, and awareness Issues and Practices to be followed in Online or Internet Banking. Section II contains the related work of cyber security attacks, and awareness, Section III contains research methodology incorporating location, sample size information, scope, objectives and hypotheses, Section IV contains statistical outlook of data analysis and interpretation performed over the dataset, and Section V contains results drawn for the research objectives and recommendation proposed.

II. REVIEW OF LITERATURE

Cyber security is characterized as the protection of internet based services or internet itself, of the substantial or elusive innovations that help the internet, of electronic data, and of the clients in their own, societal and national capacities and boundaries. Customer or User awareness is thought about as containing information, self-view of abilities, real aptitudes and conduct, and mentalities, and the interrelationship among these components [1]. In a research work on assessing the cognitive biasness of the users in cyber security it was mentioned that cyber attackers understands and take advantage of users' inherent cognitive biasness for the cyber activity while using a particular service including lack of understating and capacity to process the information system. So, building knowledge set and being aware of possibilities of errors and mistakes in common cyber activity and how to escape from those is necessary and sometime can act as sufficient to escape from any cyber attack [2].

In a study on "A Study of Cyber Security Awareness in Educational Environment in the Middle East" confirmed the lack of knowledge and awareness for the cyber security events and incidences, and also suggested the need of cyber security awareness programs for the targeted population according to the need and minimum compliance with the law. One of the major idea or assumption of the study is that building the knowledge set or creating the awareness among the users for the cyber security practices and tips may fix all the problems associated with the cyber security especially in the electronic banking and technology enabled banking practices. The core idea of awareness is building the knowledge blocks that can help the users to learn more about the threats and security aspects in banking and can take better decisions [3]. In one of the study research conclusion was focused on building the knowledge block or educating the users and also focused on the interest of the users

encapsulating acquisition retention and quality of transfer of knowledge [4].

Persistence of the poor user behavior for the internet based financial and non financial activities the presents their overall behavior which is found poor or weak as users are not even aware about the basic security tips and practices which is to be followed in any financial activity or baking operation. Addressing the aforesaid poor human behavior for the technologically rich banking and financial activities it was mentioned [5] that only awareness campaigns and education programs are not enough to safeguard the banking activities of the user from cyber attackers. It is also recommended that awareness is must but managing all the frauds and cyber attacks through human based activities is not at all feasible and so that technical enrichment is must for the effective safeguarding of the system from the attackers.

In a study on cyber security problems and issues, a deeper engagement was identified for the problems and issues associated with the cyber security encourage the users with higher cognizance for the cyber awareness programs and also develops their self-efficacy and practices to manage the cyber problems especially in their banking activities and practices. In the cognitive model discussed in the paper encapsulated two major variables such as self-efficacy and perceived vulnerability, also confirmed that these two variables are helpful to predict the protecting behavior of the users at a great extent. So, knowledge and awareness is necessary [6].

This review was directed in the real electronic banking users of Public and Private Banks of Udaipur district of Rajasthan by majorly focusing on different cyber security threats and issues that assaults their banking practices and activities on the web and other electronic banking platforms. This overview presented the electronic bank users' level of awareness about the cyber security issues and practices.

III. METHODOLOGY

In order to assess the public and private sector banks' electronic banking services and practices users of Udaipur, a set of well structured questionnaire encapsulating different question set relating the cyber security and threats was presented to them. The questionnaire was distributed among only those users who were having knowledge about the electronic banking methods. The research process of the study was performed in three different stages which started with the interactions with respondents of research work, questionnaire development, and determination of sample population size. In the stage second of the research work questionnaire distribution and data accumulation process was performed, as the mode of distributing the questionnaire was both in hard copy and through email so several data collection practices were followed. In the last or third stage of the research work systematic analysis over the dataset produced from the responses of respondents was performed, and corresponding results and recommendations were recorded.

A. Study Location - The geographical scope or the study location of the present research work was Udaipur, and the respondents were of public and private sector banks operating in the district area and having good acquaintance with electronic banking and payment system services and practices.

B. Population and Sample Size – As the research work was confined to the e-banking users only, so after interaction with the good number of bank customers a minimum number i.e. 200 respondents from both public and private sector banks were identified as the respondents. A total questionnaire set distributed among the targeted population was 380 in order to get the mark of 200 respondents for the study purpose. So, the data rejection rate was 52.63% as only duly filled questionnaires were incorporated in the research work. This indicated that level of customer awareness for the electronic payment and banking services is not good enough.

C. Data Collection Method – A well structured set of questionnaire was presented to the respondents to assess or to capture their extent of awareness for the cyber security specific to the issues, risks, and tips. Questionnaire was having three different sections, in which section A of the questionnaire incorporated statement related to the personal information or socio-economic profile, section B incorporated questions related to the awareness for the cyber threats and issues especially associated with banking in both hardware and software categories, and section C of questionnaire incorporate questions related to the awareness for the cyber security tips and practices, hardware and software solution, do's and don'ts, common mistakes performed by users in electronic banking.

D. Operational Scope – The operational scope of the research work is limited to the assessment of bank customers' level of awareness or the knowledge for the cyber security pertinent to the electronic banking especially.

RESEARCH OBJECTIVES

- To measure the level of awareness for cyber security practices and tips among e-banking users.
- To measure the effect of socio-economic factors on level of awareness for cyber security practices and tips among e-banking users.

HYPOTHESES

H_{01}: There is no difference in the level of awareness for cyber attacks and threats among public and private bank e-banking users.

H_{a1}: There is significant difference in the level of awareness for cyber attacks and threats among public and private bank e-banking users.

H_{02}: There is no difference in the level of awareness for cyber security practices and tips among public and private bank e-banking users.

H_{a2}: There is significant difference in the level of awareness for cyber security practices and tips among public and private bank e-banking users.

H_{03}: There is no effect of socio-economic factors on level of awareness for cyber security practices and tips among e-banking users.

H_{a3}: There is significant effect of socio-economic factors on level of awareness for cyber security practices and tips among e-banking users.

In order to measure the difference between the public and private sector bank e-banking users' level of awareness for cyber security practices and tips one way ANOVA test was performed and to measure the effect of socio-economic factors on user's level of awareness linear regression analysis was performed.

IV. DATA ANALYSIS AND INTERPRETATIONS

In the present research work population of 200 bank customers (100 Public and 100 Private Bank Customers) of Udaipur district were chosen for the study purpose was of different socio-economic classes and present the good mix of sample population.

Table 1. Sample Distribution Statistics

Type of Bank	Number of Respondents	%
Public	100	50.00%
Private	100	50.00%
Total	200	100.00%

Source: Primary Data

Socio-economic profile of respondents may incorporate several personal and economical characteristics of individual, but for the present research work age (in years), gender, educational qualification, occupation, income or saving (per annum), owning the advanced banking tools, and tenure of using internet or online banking (in years).

Table 2. Socio-economic Profile of Respondents

Age in Group (in years)	No. of Respondents	%
Up to 25	38	19
Between 26-50	117	58.5
Above 50	45	22.5
Total	**200**	**100**
Gender	**No. of Respondents**	**%**
Male	136	68
Female	64	32
Total	**200**	**100**
Educational Qualification	**No. of Respondents**	**%**
Below Graduate	23	11.5
Graduate	41	20.5
Post Graduate	56	28
Professionally Qualified	48	24
Others	32	16
Total	**200**	**100**
Occupation	**No. of Respondents**	**%**
Government Employee	58	29
Private Sector Employee	62	31
From Agriculture	9	4.5
Other Professions	46	23
Not Working	25	12.5
Total	**200**	**100**
Income / Savings (Per Annum)	**No. of Respondents**	**%**
Up to Rs.1,00,000	29	14.5
Rs 1,00,001 to Rs3,00,000	59	29.5
Above Rs 3,00,000	112	56
Total	**200**	**100**
Owns	**No. of Respondents**	**%**
Internet Banking User Account	29	14.5
Debit/ Credit Cards	59	29.5
Mobile Banking Apps	112	56
Total	**200**	**100**
Using Internet Banking / Online Banking	**No. of Respondents**	**%**
Less than 3 Years	107	53.5
3-5 Years	71	35.5
More than 5 Years	22	11
Total	**200**	**100**

Source: Primary Data

The socio-economic statistics of the above table 2 revealed that majority of respondents of the research work are from the age group 26-50 years i.e. 117 (58.5%), male participation 136 (68%) is greater to female respondents participation i.e. 64 (32%), in academic qualification a good mix of qualification was observed as 48 (24%) respondents were professionally qualified, 56 (28%) respondents were post graduate, about the occupation profile of the respondents only 25 (12.5%) respondents were not working anywhere, and remaining are associated with several professions and i.e. 87.5% of the total respondents, for income or saving per month 112 (56%) respondents were having higher income of saving to Rs. 300000 per annum, it was also found that 112 (56%) of the users are using mobile apps promoted by the bank especially by SBI i.e. Yono SBI etc, and about the tenure of using the internet or online banking it was identified that majority of respondents 107 (53.5%) are using it from less than 3 years that is because of the push driven by the government through digital India campaign, and demonetization, cash back offered etc. So, from the statistics it could identify that sample population of the research work has good mix of socio-economic categories of different profiles.

Awareness for Cyber Attacks and Threats in Electronic Banking

Table 3. F-Statistics of Awareness for Cyber Attacks and Threats in E-Banking According to Type of Bank

	Avg. Score	F-Statistics
Attacks through the underlying Blockchain technologies	3.1056	1.2635
Supply Chain attacks	2.1748	1.3189
Attacks through Mass Media	3.3447	3.1125*
ATM malware Intrusion	3.4545	3.2137*
Attack on Cypto Platforms	2.6742	1.7411
Traditional Card Frauds	3.1423	3.5674*
Internet Banking Trojans	2.3709	1.4331
PC and Mobile Oriented Banking attacks	3.6445	3.2115*
Theft of Biometric Data	2.8114	3.6213*
PoS attacks	2.1142	1.7423
Ransomware	3.4916	3.2346*
Social Engineering	3.1122	3.2143*
Identity Theft	3.1021	1.1325
Synthetic Fraud	2.5211	0.9826
Phishing	3.6221	3.2262*

Source: Primary Data (Df =1, Significant at 5 percent)

From the F-Statistics of the above table it was identified that for Attacks through Mass Media, ATM malware Intrusion, Traditional Card Frauds, PC and Mobile Oriented Banking attacks, Theft of Biometric Data, Ransomware, Social Engineering, and Phishing cyber attacks or threats e-banking users level of awareness was found high, the mean score values for the aforementioned variables are 3.3447, 3.4545, 3.1423, 3.6445, 2.8114, 3.4916, 3.1122, 3.6221 respectively.

The significant difference was observed for the public and private sector bank e-banking customers' level of awareness for Attacks through Mass Media (3.1125), ATM malware Intrusion (3.2137), Traditional Card Frauds (3.5674), PC and Mobile Oriented Banking attacks (3.2115), Theft of Biometric Data (3.6213), Ransomware (3.2346), Social Engineering (3.2143), and Phishing (3.2262) since their F values were found significant at 5 percent significance level. So, for the aforesaid cyber threats or attacks the H_{a1} is accepted i.e. "There is significant difference in the level of awareness for cyber attacks and threats among public and private bank e-banking users. For remaining cyber threats or attacks H_{01} is accepted i.e. "There is no significant difference in the level of awareness for cyber attacks and threats among public and private bank e-banking users".

Awareness for Cyber Security Tips and Practices of E-Banking

Table 4. F-Statistics of Awareness for Issues and Practices of E-Banking

	Avg. Score	F-Statistics
Account with two factor authentication	2.5644	1.3584
Create Strong Password and Timely Update the Password	3.7421	3.5612*
Updated Security Software in PC	3.4419	3.2214*
Access account from Secure Location	3.1136	3.1128*
Remember to Logout	3.5724	3.1234*
App lock to payment and mobile apps	3.2442	3.6475*
No sharing of personal and confidential information especially password, PIN, etc.	3.4718	3.3114*
Always be alert of Fraudulent Calls, SMS etc., do not reply	3.4467	3.1154*
Remember the security codes rather following the practice of saving them	2.7406	2.1364
Uninstall "Any Desk' app, if not required with immediate effect.	2.2141	1.8942

Source: Primary Data (Df =1, Significant at 5 percent)

From the F-Statistics of the above table it was identifies that for Create Strong Password and Timely Update the Password, Updated Security Software in PC, Access account from Secure Location, Remember to Logout, App lock to payment and mobile apps, No sharing of personal and confidential information especially password, PIN, etc., and Always be alert of Fraudulent Calls, SMS etc., do not reply cyber security tips and practices e-banking users level of awareness was found high, the mean score values for the

aforementioned variables are 3.7421, 3.4419, 3.1136, 3.5724, 3.2442, 3.4718, and 3.4467 respectively.

The significant difference was observed for the public and private sector bank e-banking customers' level of awareness for Create Strong Password and Timely Update the Password (3.5612), Updated Security Software in PC (3.2214), Access account from Secure Location (3.1128), Remember to Logout (3.2115), App lock to payment and mobile apps (3.6475), No sharing of personal and confidential information especially password, PIN, etc. (3.3114), and Always be alert of Fraudulent Calls, SMS etc., do not reply (3.1154) since their F values were found significant at 5 percent significance level. So, for the aforesaid cyber security tips and practices H_{a2} is accepted i.e. "There is significant difference in the level of awareness for cyber security practices and tips among public and private bank e-banking users". For remaining cyber security tips and practices H_{02} is accepted i.e. "There is no difference in the level of awareness for cyber security practices and tips among public and private bank e-banking users".

Effect of Socio-Economic Variables on In Level of Awareness for Cyber Security Tips and Practices

Table 5. Coefficient of Variables – Socio-Economic Variables Effect on Awareness for Cyber Security Tips and Practices

Model		Coefficients			t	Sig.
		Unstandardized		Standardized		
		β	Std. Err.	β		
1	Constant	1.719	0.287		7.235	.000
	Age	0.562	.044	.289	4.524	.000
	Gender	-.143	.056	-.179	-1.087	.058
	Educational Qualification	0.745	.049	.374	4.266	.000
	Occupation	0.523	.061	.319	4.112	.000
	Income / Savings	0.498	.036	.416	3.896	.009
	Owns	0.516	.054	.337	3.916	.002
	Using E-Banking	0.617	.037	.402	4.233	.000

Source: Primary Data

According to the statistics of the coefficient table presented above, it was identified that for the composite effect of the socio-economic variables on the bank customers' level of awareness for the cyber security tips and practices t value 7.235 was found significant at .000. For the individual variables effect on bank customer' level of awareness for cyber security tips and practices except gender (-.143) for all the other variables such as Age (0.562), Educational Qualification (0.745), Occupation (0.523), Income / Savings (0.498), Owns (0.516), and Using E-Banking (0.617) their beta values were found positive. About the significance of the effect measured through the t value it was found that for all the variables such as Age (t=4.524, 0.000), Educational Qualification (t=4.266, 0.000), Occupation (t=4.112, 0.000), Income / Savings (t=3.896, 0.009), Owns (t=3.916, 0.002), and Using E-Banking (t=4.233, 0.000) t value showed significance except gender (t=-1.087, 0.000).

So, from the above statistics it was identified that alternate hypothesis H_{a3} presenting that "There is significant effect of socio-economic factors on level of awareness for cyber security practices and tips among e-banking users" is accepted for age, educational qualification, occupation, income / savings, owns, and using e-banking. For gender null hypothesis H_{03} is accepted that confirms that "There is no significant effect of socio-economic factors on level of awareness for cyber security practices and tips among e-banking users".

V. RESULTS AND RECOMMENDATIONS

Based on the statistical outputs, it is obvious that public and private sector bank customers of Udaipur district are well-exposed to cyber threats and security issues and challenges and about their level of awareness for the common cyber attacks and threats in electronic banking is good for attacks through mass media, ATM malware intrusion, traditional card frauds, PC and mobile oriented banking attacks, theft of biometric data, ransomware, social engineering, and phishing. About respondents level of awareness for the issues and practices in electronic banking it was noticed that most of the customers are quite aware of tips such as create strong password and timely update the password, updated security software in PC, access account from secure location, remember to logout, app lock to payment and mobile apps, no sharing of personal and confidential information especially password, PIN, etc., and always be alert of fraudulent calls, SMS etc., do not reply. However, it was also noticed while integrating with the respondents that all the online banking activities should be monitored by the customers frequently and closely and also should keep updated them about the new advancements, including the development of the behavior of reporting of cyber threats. It was also identified that all the socio-economic variables plays vital role in the maintaining or driving the level of awareness of customers for cyber security threats and

attacks, and tips and practices. The research findings and the statistics of the research work can be used for developing the teaching and learning modules for the public and private sector bank customers. The research findings had offered valuable and deep approach to the obtainable level of information set of the on cyber security, threats and attacks, and tips and practices in electronic banking among the academicians, bankers, and other researchers.

The research work points out that most of the e-banking users have good level of awareness or knowledge about the cyber security threats and issues, and tips and practices to deal with the potential cyber crime in their electronic or online banking. But, how frequency they follow the guidelines of the banks and at what extent their approach of building the complete awareness is influenced by their socio-economic profile may lead into formulating the effective online banking services usage policies for the bank customers on the basis of their socio-economic variables. Continuous exposure for the safe banking practices and habits score helps to know about the possibilities of the improvement, and lead into identifying the set of practices and habits that need more confined focus of banking personnel on raising the awareness among the bank customers.

The study recommended that more awareness programmes should be proposed by the banks for the bank and other common public for boosting their level of awareness for the contemporary cyber threats and challenges and how they can practice over them not to be a victim of it. Banks should continuously make interaction with the electronic banking customers to prepare the log of the risk and challenges they identified in their continuous banking practices either performed through website, mobile apps, ATM or any other channel of electronic banking.

REFERENCES

[1] R. Chandarman, B.V. Niekerk, "Students' Cyber Security Awareness at a Private Tertiary Educational Institution", The African Journal of Information and Communication (AJIC), Vol. **20**, pp. **133-155**, **2017**.

[2] D. J. Krawczyk, M. Bartlett, K.M. Hamlen, B. Thuraisingham, "Measuring Expertise and Bias in Cyber Security using Cognitive and Neuroscience Approaches," In the 2013 IEEE International Conference on Intelligence and Security Informatics, pp. **364–367, 2013**.

[3] S. Al-Janabi, S. A. I. AlShourbaji, "A Study of Cyber Security Awareness in Educational Environment in the Middle East", Journal of Information & Knowledge Management, Vol. **15**, Issue **1**, pp. **1650007-1 - 1650007-30**, **2016**.

[4] P.S. Kumaraguru, S.A. Acquisti, L.F. Cranor, J. Hong, "Teaching Johnny not to Fall for Phish," ACM Trans. Internet Technol. TOIT, Vol. **10**, Issue **2**, pp. **7**, **2010**.

[5] J. Nielsen, "User education is not the answer to Security Problems," **Alertbox**, **2004**.

[6] Y. Sawaya, M. Sharif, N. Christin, A. Kubota, A. Nakarai, A. Yamada, "Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior," presented at the Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, pp. **2202–2214**, **2017**.

AUTHORS' PROFILE

Dr. Ashish Adholiya, is right now an Assistant Professor at Pacific Business School, Affiliated to Rajasthan Technical University, Kota, completed is Ph.D. in the area of Database Flexibility from JRN Rajasthan Vidyapeeth (Deemed to be University, NAAC –A Grade). Has a total experience of 12 years in academics and 3 years of IT companies. He guides and assists students pursuing MBA, MCA and Ph.D. programs in their Dissertation's research methodology and statistical section. He has authored 15 research articles for international journals and 23 for national journals with impact factor. He has been conducting Management Development Program to various organizations like IOC. He is managing editor of two national journals published by Pacific University, Udaipur since last 3 years.

Shilpa Adholiya, is right now a Research Scholar in Faculty of Commerce and Management Studies, and working as Sr. Lecturer (PGT) in nationally reputed senior secondary school Central Academy, Udaipur, Rajasthan. She acquired her MCA with A grade from SMU, M.Com. (ABST) from VMOU, M.A.(Economics) from VMOU. Her area of the research work is Artificial Intelligence and Cloud Computing, and also had several research contributions in Social Sciences topics. She has authored 6 research articles for international journals and 10 for national journals with impact factor. She has been awarded by Best Teacher Award by Times Group in 2016-17. She has presented research articles at various National and International conferences, and participated workshops.

