Measuring Software Security using MACOQR (Misuse and Abuse Case Oriented Quality Requirements) Metrics: Attacker's Perspective

C. Banerjee[1], Arpita Banerjee[2] and P. D. Murarka[3]

[1]Amity Institute of Information Technology, Amity University,
Jaipur, Rajasthan, India

[2]Department of Computer Science, St. Xavier's College, Rajasthan University,
Jaipur, Rajasthan, India

[3]Department of Computer Science Engineering, Arya College of Engineering and Technology
Jaipur, Rajasthan, India

Abstract: ***In the age of information there is a continuous threat while using any software and the true understanding of its increasing extent is rarely developed. One class of people is involved with development of software and another class of people is involved with use of the same software. Moreover, there is a constant threat to the software from the inside world (inside attacker) and outside world (outside attacker). Hence for proper synchronization of security aspect with the software being developed some mechanism should be in place to judge the type of attacks and attacker. A great number of techniques & technologies are available to safeguard the system from outside attack and attacker. But the issue of tackling the inside attack and attacker is a complex and difficult process for which no appropriate tools or techniques exist. One solution could be to create awareness among the end user who uses the software & development team who develops the software. Since it a continuous process hence its measurement is also necessary to judge whether the process is having any impact on the user and whether the situation is improving. Certain Object Oriented modeling techniques like Misuse case and Abuse cases could be used to incorporate security requirements in the early stages of software development phases i.e., requirement phase and subsequent measurements could also be gather for further analysis leading to improvement in the process. In this paper, we propose MACOQR metrics from attacker's perspective whose aim is to measure the ratio of internal and external attacks be made to the software using the misuse case an abuse case modeling during requirements engineering phase. The measures and ratios obtained may help the security analyst team to take proper and timely action could be initiated for implementation of effective counter mechanism against the internal attacks.***

Keywords: Software Security Metrics, MACOQR, Misuse Case, Abuse Case.

1. INTRODUCTION

Software plays a very important and essential role in today's global economy and it has indeed became an intrinsic part of every one's life; hence its synchronized & secured use is very necessary. Value of any software can be evaluated in form of people's trust. The software when attacked deliberately for stealing highly sensitive official and personal information can result in security breach and can cause harm also to individuals, organizations, nations and the world at large [1]. The attacker generally targets on vulnerabilities or security loop holes available in any software thereby endangering intellectual property and business operation & services resulting in serious financial damages [2] [3].

Security has been a major area of focus since 1977 with incidents of large number of security breach financial loss of millions many cases [4] [5]. The software is entangled with danger and the system is vulnerable both by the outsider and the insider. An outsider is generally an unauthorized and unauthenticated persons or system causing security breach to any enterprise resulting in leaking and manipulating of access rights and permission. In case of inside attack, the attacker is an authenticated and authorized user who misuses their designated access rights and permissions to damage the system. It has been proven theory that an attack caused by an insider to the system is more dangerous than an outsider attack [6] [7]. According to a study conducted by CERT, US Secret Service CSO Magazine & SEI, it was found out that some malicious codes were injected by an ex-employee which modified company's communication protocols resulting in an estimated loss of $691 million [8].

There may be certain security loop left unattended during requirement engineering phases of SDLC. While modeling of misuse cases and abuse cases, if the defects are left uncovered, then the resultant software is bound to be vulnerable and shall experience threats and attack. This in turn will add to the cost as those defects are to be first uncovered and treated properly, bringing down the reputation of the organization [9]. So a sound mechanism needs to be devised for identification, measurement, analysis with suggestions on how the modeling defects left uncovered or undetected during designing of misuse cases & subsequent resultant abuse cases & the best counter measures to deal with them [10].

Analysis of the requirements thus obtained by use and misuse / abuse cases needs to be carried out for designing a secure software system architecture [11]. Further, as the requirements obtained are qualitative in nature hence these requirements need to be converted into quantitative measure by means of some metrics for its proper analysis. Indicators and estimators could be derived from these metrics which in turn could be used by the security analysis team for measurement of software security. Metrics can also be used for analysis of flaws and functionality along with its early detection and further correction [12].

In this research paper, we focus on the defensive perspective of MACOQR metrics. Apart from the introduction, the remainder of the paper is organized as follows: section II describes introduction of proposed MACOQR metrics from defensive perspective, section III presents the set representation of MACOQR metrics from defensive perspective along with metrics to find the ratio of flaw, flawlessness in misuse case model (predicted) and ratio of flaw, flawlessness in misuse case model (observed) during requirements engineering phase. Section IV shows the statistics of data collection for analysis purpose, whereas experimental results and discussions are covered in Section V, conclusion and future work is given in Section VI.

2. PROPOSED MACOQR (MISUSE AND ABUSE CASE ORIENTED QUALITY REQUIREMENTS) METRICS FROM ATTACKER'S PERSPECTIVE

In this work, a security metrics is developed whose aim is to find out the ratio of internal and external attack through analysis of abuse cases reported when the software system is actually implemented in the real world. Through this work the author attempt to highlight the role of insider in attacking the system which results in the increase in abuse cases which potential harm to the system.

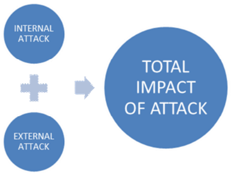


Figure 1 Internal & External Attack is Total Impact

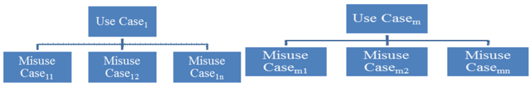


Figure 2 Showing 'n' Use Cases and Corresponding Misuse

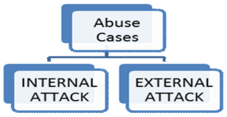


Figure 3 Showing Abuse Cases Scenario from Attacker's Perspective in Relation to Misuse Cases Shown in Figure 2

3. Representation of MACOQR (Misuse and Abuse Case Oriented Quality Requirements) Metrics From Attacker's Perspective

3.1 Set representation of MACOQR Metrics

Consider the following:-

a set of use cases in a model as:

$UC = \{ uc_1, uc_2, \ldots, uc_n\}$ ……………………….. (1)

a set abuse cases reported as:

$AC = \{ac_1, ac_2, \ldots, ac_n \}$ ……………………….. (2)

a set of abuse cases reported as a result of attack using internal IP address as:

$IAAC = \{ iaac_1, iaac_2, \ldots, iaac_n\}$ ……………….. (3)

a set of abuse cases reported as a result of attack from external IP address as:

$EAAC = \{ eaac_1, eaac_2, \ldots, eaac_n\}$ …………….. (4)

3.2 Metrics to find the ratio of internal attack reported through attack as a result of abuse cases reported using internal IP address

Consider (2) and (4) mentioned above

The metrics to determine the ratio of internal attack reported through attack as a result of abuse cases reported using internal IP address can be expressed as follows:

$$R_{IAAC} = 1 \cdot \sum_{i=1}^{n} \left(\frac{EAAC_i}{AC_i} \right) \quad \ldots\ldots \text{(M1)}$$

where

'R_{IAAC}' is the ratio of internal attack found through attack as a result of abuse cases reported using internal IP address

'AC_i' is the number of abuse cases reported

3.3 Metrics to find the ratio of external attack reported through attack as a result of abuse cases reported from external IP address

Consider (2) and (3) mentioned above

The metrics to determine the ratio of external attack reported through attack as a result of abuse cases reported from external IP address can be expressed as follows:

$$R_{EAAC} = 1 - \sum_{i=1}^{n} \left(\frac{IAAC_i}{AC_i} \right) \quad \ldots \text{(M2)}$$

where

'R_{EAAC}' is the ratio of external attack reported through attack as a result of abuse cases reported from external IP address

'AC_i' is the number of abuse cases reported

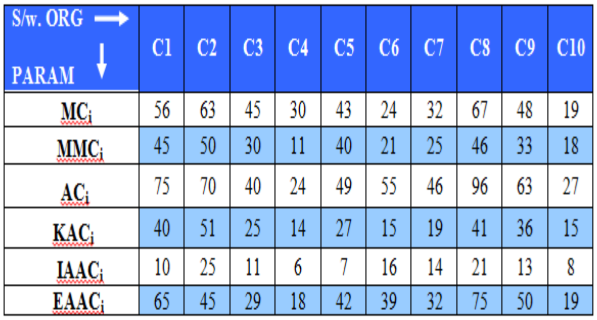
The MACOQR Metrics has been developed and proposed from attacker's point of view for addressing the issues related to software security using metrics. The aim of the MACOQR Metrics from attacker perspective is to measure the ratio of internal and external attack through analysis of abuse cases reported from the software system actually implemented. This measure those collected and analyzed indicate the role of insider in attacking the system which results in the increase in abuse cases which potential harm to the system.

4. DATA COLLECTION

In order to measure the comprehensibility and practical applicability of MACOQR Metrics, we have sent the MACOQR Metrics to 10 different software practitioners / organizations (on the request of the software practitioners / organizations, identity is concealed). The data thus collected from the software practitioners / organizations using the MACOQR Metrics are intended to show the evidence to claim that the proposed MACOQR Metrics is valid. The results of the MACOQR Metrics provide important information to support the need for an improvised metrics to be used during the requirements engineering phase of software development lifecycle.

The data is based on the already documented projects which are implemented as application. The software practitioners / organization have been labeled from 'C1' to 'C10' for ease in graphical representation for data validation. The data collected from the software practitioners / organizations using the MACOQR Metrics are listed in Table 1.

Table 1 Parameters values collected from Software Org.



S/w. ORG → PARAM ↓	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
MC_i	56	63	45	30	43	24	32	67	48	19
MMC_i	45	50	30	11	40	21	25	46	33	18
AC_i	75	70	40	24	49	55	46	96	63	27
KAC_i	40	51	25	14	27	15	19	41	36	15
$IAAC_i$	10	25	11	6	7	16	14	21	13	8
$EAAC_i$	65	45	29	18	42	39	32	75	50	19

where

MC_i is total no. of identified misuse cases for 'n' use cases

MMC_i is the total no. of mitigated misuse cases

AC_i is the total no. of abuse cases reported

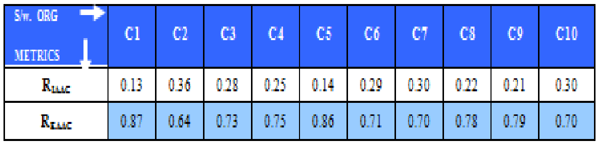
KAC_i is the total no. of known abuse cases in relation to the identified misuse cases

$IAAC_i$ is the total no. of internal attack reported through attack as a result abuse cases reported using Internal IP address

$EAAC_i$ is the total no. of external attack reported through attack as a result abuse cases reported from External IP address

After applying MACOQR metrics on the data gathered as table 1, the ratio analysis of internal and external attack calculated is shown in table 2 as follows:

Table 2 Ratio Analysis of internal and external attack



S/w. ORG → METRICS ↓	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
R_{IAAC}	0.13	0.36	0.28	0.25	0.14	0.29	0.30	0.22	0.21	0.30
R_{EAAC}	0.87	0.64	0.73	0.75	0.86	0.71	0.70	0.78	0.79	0.70

5. RESULTS AND DISCUSSION

The result section contains the observed results and subsequent validation of MACOQR metrics is also provided. From Table 2 it is clearly evident that though the ratio of internal attack to external attack is low in all the cases still it is significant as there are very few mechanism and techniques available to provide counter measure and deal with the issues of internal attack.

Figure 4 to 13 contains the company wise graphical ratio analysis of internal attack and external attack in relation to the abuse cases reported for company 'C1' to 'C10'. Whereas, figure 14 contains the graphical ratio analysis of internal attack and external attack in relation to the abuse cases reported for all company from 'C1' to 'C10'.

The various graphs depicting the ratio analysis of internal & external attack clearly shows that even when software is developed in a secure environment and implemented with technology based defenses by a well-trained security team it does not assure that the software is secure as there is a constant threat from an insider. To safeguard against the attack caused by the insider mechanism and techniques are in place, processes and standards have been laid down but still awareness needs to be create among people about the proper use of secured software with proper monitoring of all users who builds the software and who uses the software.

The proposed MACOQR metrics can be used by the Security Analysis Team to find the ratio of internal attack as well as external attack and proper and timely action could be initiated for implementation of effective counter mechanism. The author after analyzing the data advocates for a collaborative & comprehensive approach which needs to be adopted to deal with the issue of creating proper & sound awareness among the people involved

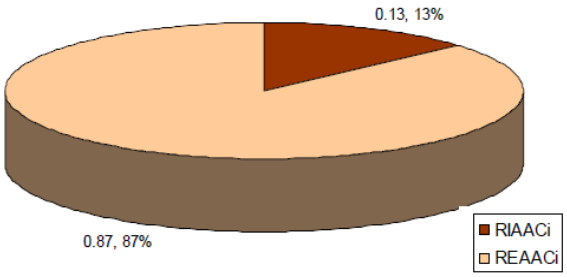


Figure 4. Showing R_{IAAC} & R_{EAAC} for ‘C1’

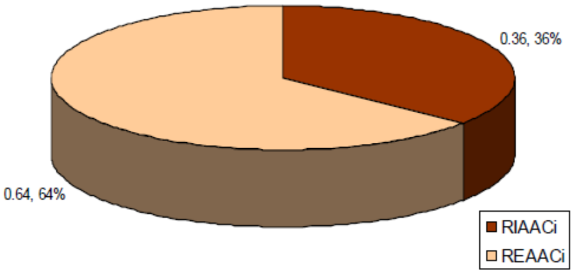


Figure 5. Showing R_{IAAC} & R_{EAAC} for ‘C2’

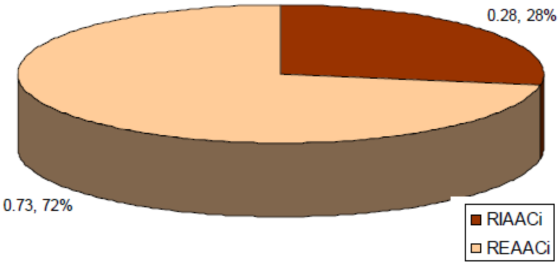


Figure 6. Showing R_{IAAC} & R_{EAAC} for ‘C3’

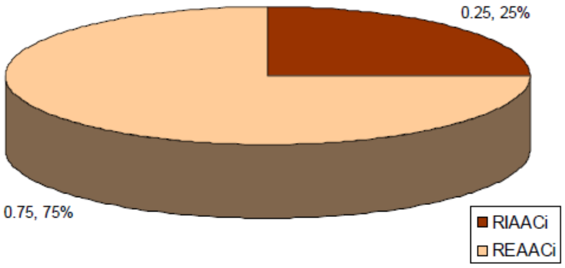


Figure 7. Showing R_{IAAC} & R_{EAAC} for ‘C4’

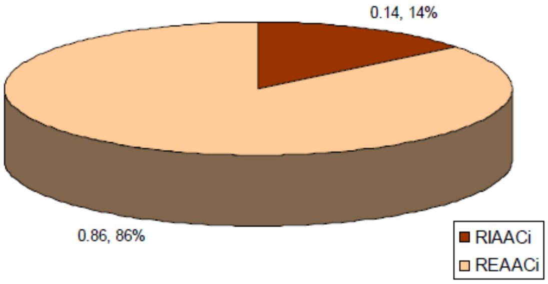


Figure 8. Showing R_{IAAC} & R_{EAAC} for ‘C5’

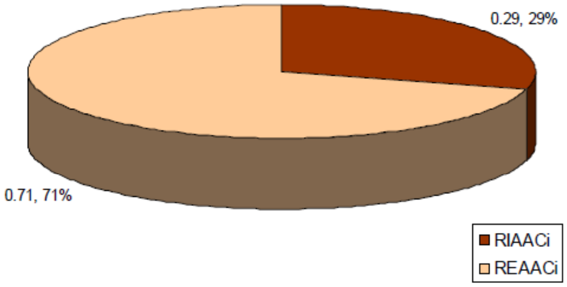


Figure 9. Showing R_{IAAC} & R_{EAAC} for ‘C6’

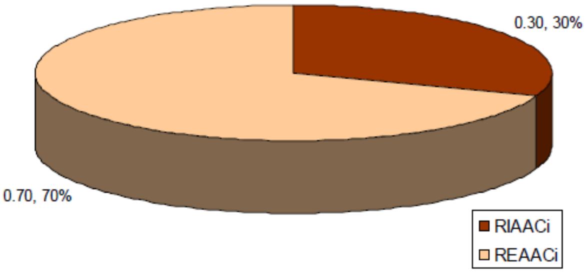


Figure 10. Showing R_{IAAC} & R_{EAAC} for ‘C7’

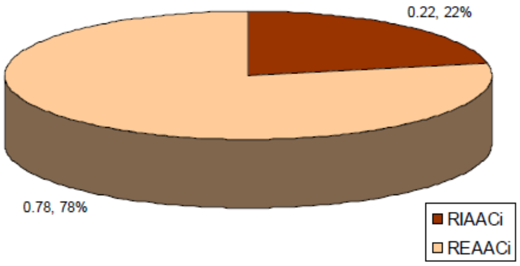


Figure 11. Showing R_{IAAC} & R_{EAAC} for ‘C8’

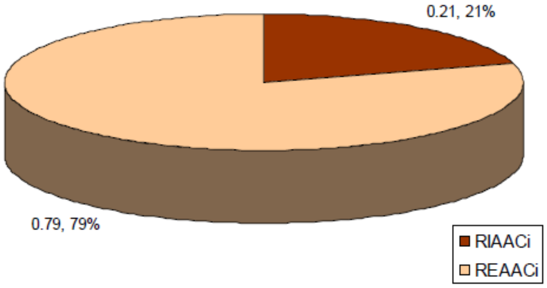


Figure 12. Showing R_{IAAC} & R_{EAAC} for ‘C9’

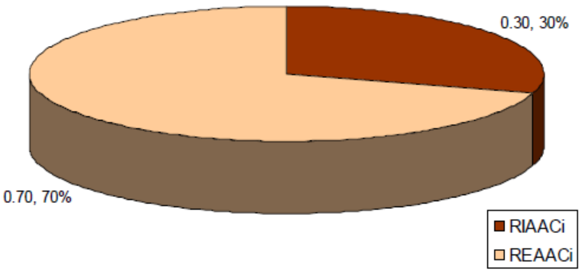


Figure 13. Showing R_{IAAC} & R_{EAAC} for ‘C10’

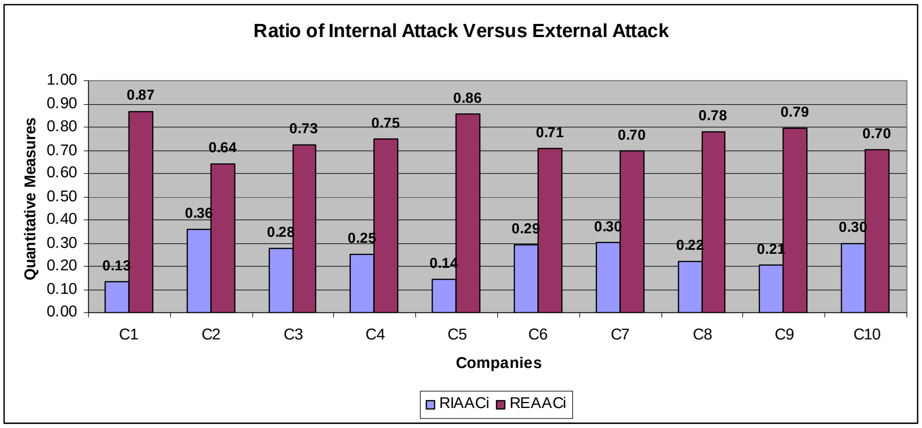


Figure 14. Showing Ratio Analysis of for Companies ‘C1’ to ‘C10’

6. Conclusion and Future Work

The aim of the MACOQR Metrics from attacker perspective is to measure the ratio of internal and external attack through analysis of abuse cases reported from the software system actually implemented. This measure those collected and analyzed indicate the role of insider in attacking the system which results in the increase in abuse cases which potential harm to the system.

The data gathered & analyzed using MACOQR Metrics shows that a collaborative and comprehensive approach in form of education and training needs to be adopted in order to deal with the issue of creating proper and sound awareness among the people involved. Further the education & training should form an essential part as pre-requirement phase in secured software development lifecycle and the quantitative assessment of its effectiveness should be done for further improvement.

From the attacker’s perspective of MACOQR Metrics, future work may include development of a collaborative and comprehensive approach in form of education and training needs to be adopted and incorporated as Pre-Requirements Phase in order to deal with the issue of creating proper and sound awareness among the people involved. Another future work may include the extension of existing proposed MACOQR metrics to include more dimension and factors to the internal attack and external attack and factor analysis could be performed for priority setting based on the type of software being developed and user. A security awareness metrics may also be developed to measure the effectiveness of such training as a future work.

References

[1] Gary McGraw: “Software Security – Building Security In”, Addison-Wesley Professional, 2006 ISBN 0321356705

[2] Elahi, Golnaz, Eric Yu, and Nicola Zannone. "A vulnerability-centric requirements engineering framework: analyzing security attacks, countermeasures, and requirements based on vulnerabilities." Requirements engineering 15.1 (2010): 41-62.

[3] Banerjee, S. K. Pandey (2009): “Software Security Rules: SDLC Perspective”, International Journal of Computer Science and Information Security, IJCSIS, USA, Vol. 6, No. 1, October 2009, pp. 123-128.

[4] Bojanc, Rok, Borka Jerman-Blažič. "A Quantitative Model for Information-Security Risk Management." Engineering Management Journal 25.2 (2013).

[5] Choo, Kim-Kwang Raymond. "The cyber threat landscape: Challenges and future research directions." Computers & Security 30.8 (2011): 719-731.

[6] Banerjee, Arpita Banerjee, P. D. Murarka: “An Improvised Software Security Awareness Model”, International Journal of Information, Communication and Computing Technology, Vol 1(2), July-Dec 2013, ISSN 2347-7202, pp. 43-48

[7] Banerjee, S. K. Pandey: “Research on Software Security Awareness: Problems and Prospects”, ACM SIGSOFT SEN Volume 35 Issue 5, September 2010, pp 1-5

[8] Dawn M. Cappelli, Randall F. Trzeciak, Andrew P. Moore (2006): Insider Threats in the SDLC, A study conducted by CERT, U.S. Secret Service, CSO Magazine, Program, Software Engineering Institute, Carnegie Mellon University, 2006, retrieved on 16/04/2014 from www.cert.org/archive/pdf/ sepg500.pdf

[9] Sindre, Guttorm, and Andreas L. Opdahl: "Eliciting security requirements with misuse cases", Requirements Engineering 10.1, Springer, 2005 pp34-44.

[10] Chun Wei, Sia: “Misuse Cases and Abuse Cases in Eliciting Security Requirements”, System Security: COMPSCI 725, The University of Auckland, New Zealand, 2005 downloadable from www.cs.auckland.ac.nz/compsci725s2c/archive/term papers/csia.pdf.

[11] Joshua Pauli, Dianxiang Xu, "Misuse Case-Based Design and Analysis of Secure Software Architecture", International Symposium on Information Technology: Coding and Computing (ITCC 2005), Volume 2, 4-6 April 2005, Las Vegas, Nevada, USA. IEEE Computer Society 2005

[12] Smriti Jain, Maya Ingle: Review of Security Metrics in Software Development Process, International Journal of Computer Science and Information Technologies, Vol. 2 (6), 2011, ISSN 0975-9646, pp 2627-2631

AUTHOR

Chitreshh Banerjee is currently working as Senior Lecturer, Amity Institute of Information Technology, Amity University, Jaipur. He has also worked as Executive Officer in the Board of Studies, The Institute of Chartered Accountants of India (Set up by an Act of Parliament), New Delhi. He is member in 11 International Societies/Associations. He has an excellent academic background with a very sound academic and research experience. Under the Institute-Industry linkage programme, he delivers expert lectures on varied themes pertaining to IT. As a prolific writer in the arena of Computer Sciences and Information Technology, he penned down a number of books/learning material on Multimedia Systems, Information Technology, Software Engineering, E-banking Security Transactions, System Analysis and Design, Web Technologies, etc. He has contributed 16 research papers in the conferences / journals / seminar of international and national repute. He also provides consultancy in the area of software and project management to a no. of IT companies. He is acting as Editor in four International Journals and Reviewer of 3 International Journals. His area of interest includes software security, software engineering, and e-learning.

Arpita Banerjee is currently working as Associate Professor, St. Xavier’s College, Jaipur. She has a good academic and industry experience in the field of Computer Science & Application / IT. As a prolific writer in the arena of Computer Sciences and Information Technology, she has contributed some chapters in books on Multimedia Systems and E-banking Security Transactions. She has taken a step further in the field of research in software security and has co-authored research papers in 11 journal & conference of national and international repute. Her area of interest includes topics related to Computer Science & Application / Information Technology.

Prof. P. D. Murarka is currently working as Professor, Arya College of Engineering and Technology, Jaipur. He has an experience of more than 45 years with 5 years of industrial experience. He has penned down a number of text and reference books. He has authored many research papers in journal and conferences of national and international repute. His area of interest includes topics related to Artificial Intelligence, Robotics, and Security.