SCIENCEDOMAIN *international*
www.sciencedomain.org

SDI Review Form 1.6

Journal Name:	**Advances in Research**
Manuscript Number:	**Ms_AIR_37460**
Title of the Manuscript:	**Graphical User Authentication System Resistant to Shoulder Surfing Attack**
Type of the Article	**Original Research Article**

General guideline for Peer Review process:

This journal's peer review policy states that **NO** manuscript should be rejected only on the basis of '**lack of Novelty'**, provided the manuscript is scientifically robust and technically sound.
To know the complete guideline for Peer Review process, reviewers are requested to visit this link:

(http://www.sciencedomain.org/page.php?id=sdi-general-editorial-policy#Peer-Review-Guideline)

SDI Review Form 1.6

PART 1: Review Comments

	Reviewer's comment	**Author's comment** *(if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)*
Compulsory REVISION comments	Graphical user authentication technique is an alternative solution to PIN/Password-based authentication technique suffers from various attacks such as shoulder surfing attack due to its simplicity and graphical user interface. To protect the system from such attack or to improve the performance of graphical user authentication technique author developed a model and compared with existing systems on the basis of graphical space and password entropy. The author claimed that the proposed system is more secure and the approach is balanced the usability and security features in this domain. • Only 30 users participated in the experiment. The subject size is very less. Make it larger. • The author combined two published algorithms: Draw a Secret (DAS) and Story algorithms. The system takes random draws to make a predefined story at login session. It is not cleared that are claim users informed about the story? • Repeated information, some part of Table 3 is repeated to Table 4. • All the formulas are written in an informal way. • A number of used images, number of selecting images and rounds are correlated to Password space consequently password entropy. Therefore it is necessary to discuss the range of these parameters value and the risk associated with it. • Table 1 is unnecessarily inserted. • Research methodology is very poor and not explained properly. • The structure of the paper is not systematically presented. • The approach can use to shoulder surfing attack but may increase the chances of a dictionary or guessing attacks. • The novelty of the study is not good. • Timing parameter, acceleration speed, gyroscope data would be the effective features to reduce the shoulder surfing attacks in any knowledge-based authentication technique such as Graphical PIN or Password.	
Minor REVISION comments	• Illegitimate users must be informed about the story of used 15 legitimate users. • Structure of the paper must be systematic. • Results part is unnecessarily repeated. • Desktop or Android environment, which one is used? Make it clear.	
Optional/General comments	• The novelty of the study is limited. The effectiveness and user experience of the model are not clearly described. To reduce the shoulder surfing attack it increases some guessing attacks. How it must be prevented is to be explained.	

Reviewer Details:

Name:	***Soumen Roy***
Department, University & Country	***University of Calcutta, India***