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

<mark>PART 1:</mark> 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	1. The first sentence of the abstract states "User authentication is <u>the most critical element</u> in the field of information security", while the first sentence of the introduction states "User authentication is one of the most significant issues in computer and information security" (Providing a corresponding reference). The sentence of the abstract (i.e. "the most critical") suggest a strong statement that must either be supported argumentatively, or be rephrased in accordance with the first sentence of the introduction.
	2. Discussing biometrics as an authentication method in the introduction the authors state 1-"users tend to resist its usage because of their intrusiveness and the effect on their privacy", and 2-"Biometrics process is slow, expensive and cannot be revoked". It is suggested that the authors provide sources and information in respect to the soundness of these two arguments.
	3. In section 3.1, an algorithmic representation of the system description/ functionality is recommended. (This can potentially be in addition to the existing textual form).
	4. In section 3.1, It is not clear if three login rounds are required for each authentication request, as stated in section 4.1.1.1.
	5. In respect to the evaluation method:
	  a. The authors state "Recruiting a participant group that would represent the true population was practically impossible",
	    i. What would such a group consist of?
	    ii. Why it was impossible?
	    iii. How does this affect the validity of the evaluation results?
	  b. A more detailed description of the participants attributes is suggested:
	    i. What was their age?
	    ii. Educational level?
	    iii. Technological awareness?
	    iv. etc
	  c. The authors state, "The attacker group participants were <u>briefly introduced to the scheme</u>".
	    i. Why was this approach selected?
	    ii. How did it affect the evaluation results?
	    iii. Does the authors' assumption in respect to the adversarial model suggest that a potential attacker will not be fully proficient to the functionality of the mechanism?
	6. It is not clear if the endpoints for each section of the drawn pattern are the images selected by the user. (This comment must be addressed in conjunction with comments 3 and 5.c.iii) If so:
	  a. Was this information given to the attacker group?
	  b. How this would have affected the evaluation results?
	7. In table 2, a justification is suggested for the "No" in Triangle, Movable frame, Story password, and WIW, similarly to the first six entries.
	8. The authors claim in multiple points across the article that the suggested mechanism covers usability features. Yet, evidence of a conducted usability study are not clearly provided, either as standalone or in comparison to other existing mechanisms:
	  a. What is the "time to learn", and how does it compare with other mechanisms?
	  b. What is the "Speed of performance", and how does it compare with other mechanisms?
	  c. What is the "Repeatability", and how does it compare with other mechanisms?	

	d. What is the "Subject satisfaction", and how does it compare with other mechanisms? e. What is the "User error rate", and how does it compare with other mechanisms? f. What is the "memorability", and how does it compare with other mechanisms? g. etc	
Minor REVISION comments	1. Minor improvements in language are required. (Proofreading is recommended) 2. The quality of figures 2 and 3 must be improved. (They look distorted in a printed version)	
Optional/General comments	1. The discussion of related work is satisfactory. 2. The topic of the article is significant for the scientific community and the field of information security. 3. The suggested solution within this article can constitute a significant contribution after revision.	

Reviewer Details:

Name:	*Vasileios Gkioulos*
Department, University & Country	*Norwegian University of Science and Technology, Norway*