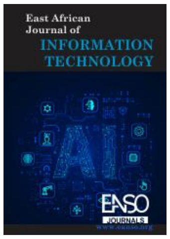


East African Journal of Information Technology
eajit.eanso.org
Volume 8, Issue 1, 2025
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

An In-Depth Analysis of Existing Models for Reconstruction of Events Involved in A Computer Crime

Moses Byaruhanga[1] & Gilbert Gilibrays Ocen[1]*

[1] Busitema University, P. O. Box 236, Tororo, Uganda.
[*] Author for Correspondence ORCID ID; https://orcid.org/0009-0006-8106-1535; Email: mosesbyaruhanga155@gmail.com

Article DOI: https://doi.org/10.37284/eajit.8.1.3208

Date Published:

24 June 2025

Keywords:

Computer Crime Scene, Events Reconstruction Model, Crime Scene Events Reconstruction, Computer Crime.

ABSTRACT

In a research by [1], Crime scene event reconstruction is critical and plays a big role in crime investigation. The consistency and integrity of the crime scene and all corresponding evidence can easily be protected through keeping a clear trail of events that unfolded before, during, and after the crime was committed. Over the years, researchers have developed several models through which the events that led to the crime can be reconstructed. In this paper, we take a clear and a deeper analysis of the most frequently used models to explore their capability in ensuring the accuracy and consistency of results. The study considered a total of twenty-one (21) models and explored each phase outlined by the authors of the model. A mixed method was used in this study, involving both quantitative and qualitative methods interchangeably. The findings were analysed using the statistical package for the social sciences (SPSS) version 22, which is widely used in social science, market research, and data mining among other fields, as noted by [2]. From the results of this paper, it was seen that a standardised model for crime scene event reconstruction is required that can better protect the integrity and the accuracy of evidence during and after crime scene investigation. Finally, the paper proposes a general recommendation to pave the way for further research and investigation regarding crime scene event reconstruction models.

APA CITATION

Byaruhanga, M. & Ocen, G. G. (2025). An In-Depth Analysis of Existing Models for Reconstruction of Events Involved in A Computer Crime. *East African Journal of Information Technology*, *8*(1), 287-296. https://doi.org/10.37284/eajit.8.1.3208.

CHICAGO CITATION

Byaruhanga, Moses & Gilbert Gilibrays Ocen. "An In-Depth Analysis of Existing Models for Reconstruction of Events Involved in A Computer Crime". *East African Journal of Information Technology* 8 (1), 287-296. https://doi.org/10.37284/eajit.8.1.3208.

HARVARD CITATION

Byaruhanga, M. & Ocen, G. G. (2025) "An In-Depth Analysis of Existing Models for Reconstruction of Events Involved in A Computer Crime", *East African Journal of Information Technology*, 8(1), pp. 287-296. doi: 10.37284/eajit.8.1.3208.

 |

Article DOI: https://doi.org/10.37284/eajit.8.1.3208

IEEE CITATION

M. Byaruhanga & G. G. Ocen "An In-Depth Analysis of Existing Models for Reconstruction of Events Involved in A Computer Crime", *EAJIT*, vol. 8, no. 1, pp. 287-296, Jun. 2025.

MLA CITATION

Byaruhanga, Moses & Gilbert Gilibrays Ocen. "An In-Depth Analysis of Existing Models for Reconstruction of Events Involved in A Computer Crime". *East African Journal of Information Technology*, Vol. 8, no. 1, Jun. 2025, pp. 287-296, doi:10.37284/eajit.8.1.3208.

INTRODUCTION

The Crime Scene of any computer-related crime starts with the computer used to commit a crime [3]. A computer can be used as a tool to commit a crime, whereas it can still be used to assist in committing a crime. In both scenarios, a successful and trusted investigation should begin from observing the chronological way in which the events unfolded, leading to the committed crime. Several scholars believe that the reconstruction of these events is one way among many other ways through which the integrity of the crime scene is protected [4].

While taking this direction, several researchers have managed to develop models that can better describe the phases through which an investigator can determine accurately the events that unfolded before, during, and after the crime has been committed [5]. This study took a clear, in-depth analysis of the top 21 models that are widely used to reconstruct events in a computer crime scene.

In this paper, commonly used models, including Defining Event Reconstruction of Digital Crime Scenes, System for Trajectory Reconstruction and Independent Preparation of Evidence in Surveillance (STRIPES), Model for Event-based Scene Analysis and Hypothesis Generation (MESH), among others, were analysed. Literature revealed that a good number of these models have numerous phases. In a comparison made by [6]. All the frequently used models have not least 8 phases and recommend a model as best for crime scene event reconstruction based on the various number of phases in conjunction with the phases being clearly explained. Reviewed literature indicates that the System for Trajectory Reconstruction and Independent Preparation of Evidence in Surveillance (SRDFIM) was recommended as suitable for digital investigation because this was the only model that provided exploratory testing, which means that the researchers developed their methods for testing [6]. What is most challenging is that most of these developed models, including the recommended one (SRDFIM) do not tell why certain characteristics exist on a particular evidence and thereby making it hard to reconstruct the crime scene events. If we are to reconstruct the crime scene, the integrity of the crime scene should be protected at all costs. The main objective of this study was to comprehensively review the available models used for crime scene events reconstruction while discovering the major challenges, limitations and collection of major requirements for paving a way for more efficient and recommended model for crime scene events reconstruction especially digital crimes that amplifies the integrity of the crime scene and answers why certain characteristics exist on evidence collected from the crime scene.

Scope of the Study

This study aimed to explore the strengths and weaknesses of the available and widely used event reconstruction models. The model's analysis took the direction of digital criminals, and therefore, the models analysed were the frequently used models in digital crime scene event reconstruction. A table indicating the phases involved in each of the models reviewed is presented below.

Article DOI: https://doi.org/10.37284/eajit.8.1.3208

Table 1: Summary of Models Reviewed and

SUMMARY OF MODELS AND PHASES INVOLVED										
PHASES/STAGES	MODELS									
	Defining Event Reconstruction of Digital Crime Scenes	STRIPES (System for Trajectory Reconstruction and Independent Preparation of Evidence in Surveillance)	MESH (Model for Event-based Scene Analysis and Hypothesis Generation)	Data Association for Reconstruction of Trajectories (DART)	Scene Analytics for Events (SAFE)	Consistent Human Description (CHD)	Dynamic Network Analysis (DNA)	A Framework for Video Analysis and Reconstruction of Crime Scenes (FVARCS)	Integrated Multimedia Event Reconstruction System (IMERS)	Crime Scene Investigator (CSI) Model.
Data acquisition		√	√	√	√	√	√	√	√	√
Preliminary analysis						√		√	√	
In-depth interviews						√				
Data preprocessing		√	√	√	√		√			
Social Network Analysis							√			
Object Detection and Tracking				√	√		√			
Network Generation							√			
Network Analysis							√			
Trajectory Generation				√						
Data Association				√	√	√				
Event detection	√		√		√					
Scene analysis		√	√							
Trajectory analysis		√								
Hypothesis generation		√	√							
Hypothesis testing	√	√	√							
Presentation		√	√							√
Reconstruction	√			√	√	√	√	√	√	
Collaboration and synthesis						√			√	
Documentation						√		√	√	√
Review and refinement						√		√		√
Analysis and Interpretation					√	√	√	√	√	√

Phases Involved

Significance

Maintaining the integrity of the crime scene is the ultimate goal for crime scene reconstruction [1]. Unfortunately, most of the available digital forensic tools only help examiners to extract a given piece of evidence and not to help in investigations, nor do they guide examiners on the sequence of events that led to the commission of a crime [7]. This compromises the integrity of the crime scene, which can result in questionable judgments in courts of law. This, therefore, creates an absolute need for a tool for crime scene reconstruction to maintain the integrity of the crime scene. This paper therefore aimed at deeply studying the available models to fully understand their respective phases, process flows, shortcomings, and strengths to propose an appropriate model that can be used for events reconstruction of computer crime scenes.

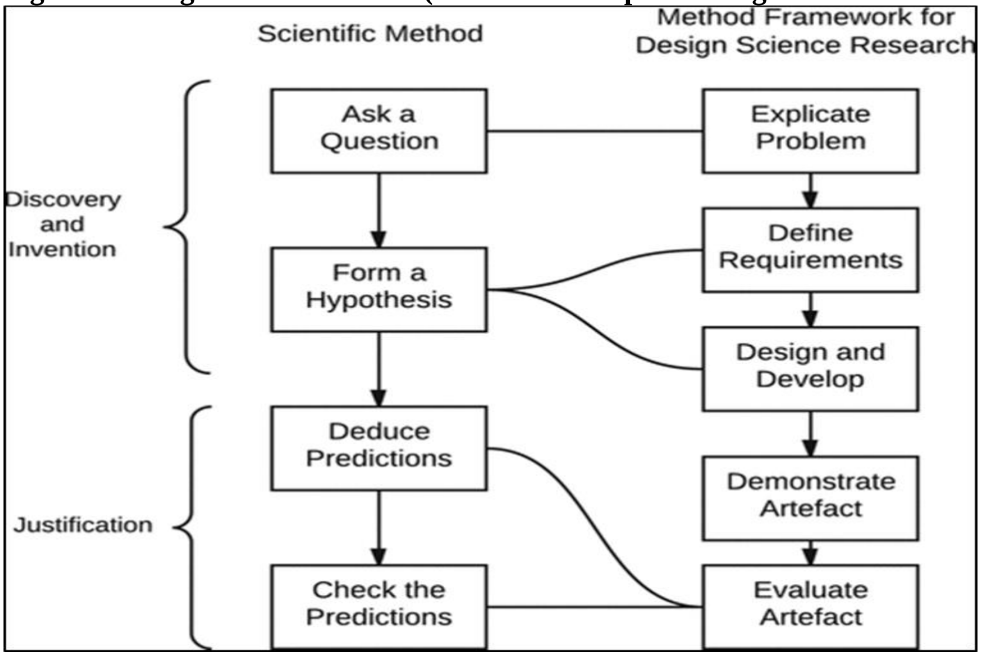
METHODOLOGY

Both the quantitative and qualitative techniques were used to conduct this in-depth analysis of existing models, while the design science methodology was used to collect, analyse, and

Article DOI: https://doi.org/10.37284/eajit.8.1.3208

interpret the results. As many researchers agree, design science is the leading information systems method used [8]. This method employs iterations, which enables the researchers to completely gather all the required information regarding the research topic.

Figure 1: Design Science Method (Cited from: https://doi.org/10.1007/978-3-030-78132-3_4)



Sample Size

The study population involved computer experts, members from law firms, and individual participants doing investigations on digital crimes. The sampling technique used was snowball sampling, where a computer expert, for instance, refers to another computer expert. In the same way, the members from law firms refer us to another colleague in the same circle of profession, due to the privacy of matters concerning criminal investigations, this sampling technique was ideal [9]. Usage statistics in terms of ease of use, model accuracy, and model level of recommendation were obtained from the respondents. This data was used to compare and contrast several models whose results necessitated the development of a new, simple, and easy-to-use model that is more accurate. A grand total of 73 participants were targeted to be included in this study. Specifically, these included 11 members from law firms, 20 computer experts, 27 educationalists and 15 researchers.

Data Collection

There are several models developed by researchers used for crime scene event reconstruction. These scholarly articles and journals provided vital information to the researchers to find comparisons of the phases/steps involved in them. Furthermore, questionnaires were developed and distributed using the snowballing technique to reach out to the respondents. Considering the nature of this investigation, special knowledge and expertise were required. This method helped the researchers to gather specific information from experienced respondents who have ever used the available models, as one was referencing another.

RESULTS AND FINDINGS

This comprehensive study attracted members from law firms and organisations, computer experts, researchers and educationalists, as it was stated in the sample space section above. The subject of the matter rotated through the 10 (ten) most frequently used models for reconstruction of digital crime

Article DOI: https://doi.org/10.37284/eajit.8.1.3208

scene events. The obtained results are discussed below.

Table 2: Demographic Information of Respondents

Variables	Intermediate Variable	Frequency	Percentage
Age Group	Below 20	2	2.7
	21- 30	31	42.5
	31 – 50	32	43.8
	Above 50	8	11.0
Level of Education	Certificate	2	2.7
	Degree	40	54.8
	Post Graduate (Masters)	21	28.8
	Doctorate (Ph.D)	10	13.7
Participant Category	Computer Expert	20	27.4
	Education Unit	27	37.0
	Member from law enforcement Agencies	9	12.3
	Researcher	15	20.5

Usability/Interaction with the Existing Models

To determine the extent to which the existing models have been used over the years, an interaction/usability analysis was done. As proposed by several scholars, the system usability scale was used [10].

Table 3: Usability Statistics of the 10 Most Frequently Used Models

#	Model	Usability/Interaction results from respondents				
		1	2	3	4	5
1	STRIPES (System for Trajectory Reconstruction and Independent Preparation of Evidence in Surveillance)	5.5	9.6	6.8	24.7	53.4
2	MESH (Model for Event-based Scene Analysis and Hypothesis Generation)	15.1	20.5	19.2	16.4	28.8
3	Data Association for Reconstruction of Trajectories (DART)	23.3	15.1	21.9	17.8	21.9
4	Scene Analytics for Events (SAFE)	17.8	17.8	21.9	12.3	30.1
5	Consistent Human Description (CHD)	20.5	16.4	19.2	16.4	27.4
6	Dynamic Network Analysis (DNA)	15.1	19.2	21.9	16.4	27.4
7	A Framework for Video Analysis and Reconstruction of Crime Scenes (FVARCS)	23.3	16.4	16.4	15.1	28.8
8	Integrated Multimedia Event Reconstruction System (IMERS)	20.5	16.4	19.2	17.8	26.0
9	Crime Scene Investigator (CSI) Model.	19.2	16.4	21.9	8.2	34.2
10	Defining Event Reconstruction of Digital Crime Scenes	16.4	17.8	16.4	23.3	26.0

The usability statistics indicate that a good number of investigators have used/interacted with System for Trajectory Reconstruction and Independent Preparation of Evidence in Surveillance (STRIPES), which obtained the highest percentage of respondents at 53.4%. The results obtained indicate that each of the models listed above is being used regardless of the percentage scores obtained.

Article DOI: https://doi.org/10.37284/eajit.8.1.3208

This is supported by literature about these models, which align with these results, making them the most frequently used.

In computer crime investigation, any crime scene event reconstruction model that results in accurate results should be given a higher priority and recommended over the most frequently used model. To determine the accuracy of the most frequently used modes, the research used the Likert scale of 1-5 to gather views extent to which users agree with the accuracy of the model to collect data about the most accurate model as presented in Table 3.

Table 4: Model-level Accuracy Statistics

#	Model	Respondents' Level of Accuracy Recommendation				
		1	2	3	4	5
1	STRIPES (System for Trajectory Reconstruction and Independent Preparation of Evidence in Surveillance)	6.8	12.3	21.3	27.4	31.5
2	MESH (Model for Event-based Scene Analysis and Hypothesis Generation)	11.0	16.4	31.5	15.1	26.0
3	Data Association for Reconstruction of Trajectories (DART)	5.5	9.6	17.8	20.5	46.6
4	Scene Analytics for Events (SAFE)	8.2	17.8	24.7	23.3	26.0
5	Consistent Human Description (CHD)	6.8	11.0	31.5	21.9	28.8
6	Dynamic Network Analysis (DNA)	8.2	16.4	27.4	23.3	24.7
7	A Framework for Video Analysis and Reconstruction of Crime Scenes (FVARCS)	2.7	15.1	26.0	23.3	32.9
8	Integrated Multimedia Event Reconstruction System (IMERS)	5.5	12.3	30.1	31.5	20.5
9	Crime Scene Investigator (CSI) Model.	9.6	13.7	27.4	15.1	34.2
10	Defining Event Reconstruction of Digital Crime Scenes	6.8	16.4	28.8	23.3	24.7

Results obtained from this analysis indicate that the Association for Reconstruction of Trajectories (DART) attained the highest percentage of 46.6%. Regardless of the interaction levels of this model being low, as seen from Table 3, it was recommended as the model that produces reasonably accurate results. This could be attributed to its capability to handle noisy and incomplete data. By associating data points, this model can generate trajectories that are physically plausible and follow a smooth path. The divergent results of usability/interaction versus model-level accuracy add more interesting area to analyse.

To determine the most recommended models, results obtained from the study presented in Table 5 indicate that Systems for Trajectory Reconstruction and Independent Preparation in Evidence Surveillance (STRIPES) is the most recommended model for crime scene Reconstruction.

Article DOI: https://doi.org/10.37284/eajit.8.1.3208

Table 5: Model-level Recommendation Statistics

#	Model	Respondents' Recommendation of Existing Models				
		1	2	3	4	5
1	STRIPES (System for Trajectory Reconstruction and Independent Preparation of Evidence in Surveillance)	0.0	5.5	12.3	24.7	57.5
2	MESH (Model for Event-based Scene Analysis and Hypothesis Generation)	6.8	16.4	27.4	20.5	28.8
3	Data Association for Reconstruction of Trajectories (DART)	5.5	16.4	30.1	21.9	26.0
4	Scene Analytics for Events (SAFE)	8.2	9.6	30.1	23.3	28.8
5	Consistent Human Description (CHD)	11.0	15.1	23.3	23.3	27.4
6	Dynamic Network Analysis (DNA)	6.8	15.1	31.5	15.1	31.5
7	A Framework for Video Analysis and Reconstruction of Crime Scenes (FVARCS)	6.8	19.2	20.5	27.4	26.0
8	Integrated Multimedia Event Reconstruction System (IMERS)	9.6	16.4	30.1	16.4	27.4
9	Crime Scene Investigator (CSI) Model.	12.3	17.8	28.8	19.2	21.9

Table 5 shows that the high level of interaction greatly affects the model level of recommendation. System for Trajectory Reconstruction and Independent Preparation of Evidence in Surveillance (STRIPES), being the highest model interacted with by most of the investigators, as seen from Table 1, also attained the highest percentage of recommendations, regardless of its low level of accuracy, as seen in Table 2.

Correlation Analysis of Existing Models

The degree of association between two variables is known as correlation [11]. To determine the relationship between model level of interaction, level of accuracy, and finally the level of recommendation, a correlation analysis was done between these variables. The correlation considered the models that had the best results from the above variables. These models are STRIPES, CSI, SAFE, DART, FVARCS, DNA, and MESH.

Table 6: Existing Model Correlation Analysis Values

Models	Interactivity VS Level of Accuracy		Interactivity VS Model Recommendation		Level of Accuracy VS Recommendation	
	Sig.	Interpretation	Sig.	Interpretation	Sig.	Interpretation
STRIPES	0.166	Low	0.506	low	0.074	Moderate
CSI	0.158	Low	0.301	low	<.001	high
SAFE	0.014	High	0.672	low	0.079	Moderate
DART	0.305	Low	0.290	low	-.118	low
FVARCS	0.837	Low	0.193	low	0.020	high
DNA	0.022	Moderate	0.791	low	0.624	low
MESH	<.001	High	0.840	low	0.205	low

The results in Table 6 proved that the model level of interactivity has a very low correlation with the model level of accuracy. This clearly explains why STRIPES is the most frequently used model, as seen in Table 3, but it is not the leading model regarding accuracy, as seen in Table 3. The number of phases and how descriptive they are are greatly influenced by the level of accuracy of the results from the model. From these results, the model level of accuracy greatly determines the model level of

Article DOI: https://doi.org/10.37284/eajit.8.1.3208

recommendation. This simply implies that investigators recommend models that produce accurate results.

Regression Analysis of the Existing Models

To extensively determine the nature of the relationship between the model level of interaction, model level of accuracy, and the model level of recommendation, we performed a deeper regression analysis among these variables. Two hypothesis statements were used and represented by H1 and H2 as follows.

- The model level of accuracy has a positive effect on its recommendation (H1)
- Model level of interaction is less significant and has a very low effect on model recommendation (H2)

The dependent variable (Model level of recommendation) was regressed with the two predicting variables being investigated (Model level of accuracy and Model level of interaction).

Table 7: Hypothesis Results

MODEL	FREEDOM	VARIABLES	H1	H2
STRIPES	F (2,70) = 1.696, p < 0.5	B	.147	.034
		t	1.712	.388
		p-Value	.091	.699
		Result	**Supported**	**Supported**
CSI	F (2,70) = 20.872 p<0.001	B	.596	-.192
		t	6.330	-2.336
		p-Value	<.001	.022
		Result	**Supported**	**Supported**
SAFE	F (2,70) = 2.075, p = .133	B	.233	-099
		t	1.991	-.986
		p-Value	.050	.327
		Result	**Supported**	**Supported**

From the regression analysis results, the model level of accuracy has a great impact on its recommendation. F (2,70) = 1.696, p < 0.5, F (2,70) = 20.872 p<0.001 and F (2,70) = 2.075, p = .133. Considering the p-value obtained in the H1 and H2 under every model that was used in regression, it was found that the model level of accuracy more significantly determines or affects its recommendation than model interaction. Therefore, the level of accuracy of a model positively predicts its level of recommendation.

Limitations of the Study

- This study explored a total of nine (9) available digital forensic models which include; System for Trajectory Reconstruction and Independent Preparation of Evidence in Surveillance (STRIPES), Model for Event-based Scene Analysis and Hypothesis Generation (MESH), Data Association for Reconstruction of Trajectories (DART), Scene Analytics for Events (SAFE), Consistent Human Description (CHD), Dynamic Network Analysis (DNA), A Framework for Video Analysis and Reconstruction of Crime Scenes (FVARCS), Crime Scene Investigator Model (CSI) and Integrated Multimedia Event Reconstruction System (IMERS).
- Limited data availability: The research faced difficulties in obtaining relevant and comprehensive data for the testing and evaluation of the digital forensic models. The availability of data is dependent on the

Article DOI: https://doi.org/10.37284/eajit.8.1.3208

cooperation of law enforcement agencies and the willingness of victims to report incidents.

- Limited generalizability: The digital forensic models that were discovered in the field were not applicable to all types of computer crimes. The effectiveness of the model is limited to specific types of crimes and is not applicable to more complex scenarios.
- Rapidly evolving technology: The field of digital forensics is rapidly evolving, and new tools and techniques are constantly being developed. A number of models became outdated quickly before being fully used by the investigators.
- Human error: The success of digital forensics investigations is dependent on the skills and expertise of the investigator. Human error can lead to inaccurate results and potentially undermine the effectiveness of the digital forensic models.
- Legal and ethical issues: The use of digital forensic tools and techniques raises legal and ethical concerns, such as privacy and data protection.

CONCLUSION AND RECOMMENDATION

Digital crime has taken a new shape today, and hence, maintaining the integrity and accuracy of the crime scene requires a proper and effective model to reconstruct the events that unfold leading to a computer crime. Several researchers have contributed to finding a suitable model to use while reconstructing the crime scene events as seen from the background of this paper. Through these researchers, numerous models have been developed in this direction, among which this paper constructed a deeper analysis. The results indicate that the accuracy of the model greatly impacts the level of recommendation. Furthermore, the description of each phase and the larger the number of phases involved in a model enhances its capabilities of producing accurate results.

In order to collect the evidence accurately, an iterative-based model is recommended to exhaustively gather all necessary information regarding the crime scene to produce an accurate chronological order and timelines of events that happened before, during, and after a crime has been committed. Further research should be geared towards mapping the various phases in these models to produce a standard model that can be used to reconstruct computer crime scenes.

REFERENCES

[1] C. S. R.-S. R. co. › 2014/03 › Crim..., “Chapter 10 Crime Scene Reconstruction BASIC PRINCIPLES FOR PHYSICAL EVIDENCE,” pp. 1–27, (2014).

[2] “SPSS.” https://en.wikipedia.org/wiki/SPSS (accessed Nov. 22, 2023).

[3] Carrier, Brian D., and Eugene H. Spafford. "Defining event reconstruction of digital crime scenes." *Journal of Forensic and Sciences* 49, no. 6 (2004): JFS2004127-8.

[4] L. I. Institute, “Criminal Law.” https://www.law.cornell.edu/wex/criminal_law (accessed Jan. 22, 2023).

[5] Edition, Third. "An Introduction to Scientific and Investigative Techniques."

[6] Rani, Sudesh. "Digital forensic models: A comparative analysis." *International Journal of Management, IT and Engineering* 8, no. 6 (2018): 432-443.

[7] Ocen, Gilbert Gilibrays, Stephen Mutua, Gilbert Barasa Mugeni, Simon Karume, and Davis Matovu. "Evaluating factors responsible for inconsistencies in mobile devices digital forensic evidence extraction process model." *International Journal of Advance Research, Ideas and Innovations in Technology* 5, no. 6 (2019).

Article DOI: https://doi.org/10.37284/eajit.8.1.3208

[8] Peffers, Ken, Tuure Tuunanen, Marcus A. Rothenberger, and Samir Chatterjee. "A design science research methodology for information systems research." *Journal of Management Information Systems* 24, no. 3 (2007): 45-77.

[9] Biernacki, Patrick, and Dan Waldorf. "Snowball sampling: Problems and techniques of chain referral sampling." *Sociological methods & research* 10, no. 2 (1981): 141-163.

[10] G. W. Sasmito, L. O. M. Zulfiqar, and M. Nishom, "Usability Testing based on System Usability Scale and Net Promoter Score," *2019 2nd Int. Semin. Res. Inf. Technol. Intell. Syst. ISRITI 2019*, no. February, pp. 540–545, 2019, doi: 10.1109/ISRITI48646.2019.9034666.

[11] Asuero, Agustin Garcia, Ana Sayago, and A. G. González. "The correlation coefficient: An overview." *Critical reviews in analytical chemistry* 36, no. 1 (2006): 41-59.

