Digital Risk Analysis of Combined Data Attacks

Harihara Sudhan.M.[1],Navin Kumar S.[2], Veeralakshmi P.[3]

[1],[2]Student, Department of IT, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, Tamilnadu, India

[3] Associate Professor, Department of IT, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, Tamilnadu. India.

Abstract - Understanding reasonable framework for Digital attacks is essential for creating material assurance and recuperation measures. Digital-attacks is key for developing appropriate protection and recovery measures.This paper conduct risk analysis of combined information attacks. We compare the combined information attacks - false data injection(FDI) attacks. The combined attacks with limited knowledge of the system model also expose advantages in keeping stealth against the bad data detection. Finally, the risk of combined information attacks to reliable system operation is evaluated using the results from vulnerability assessment and attack impact analysis.

1.INTRODUCTION

The software to be implemented is on digital library management system. Here there are three users. They are the admin, user and author. The first process is the registration of the users who visits to the library. All the details will be entered in the software. Admin has the authority to add, delete modify the details of the book that are available .The user itself has to first register and then login by some required details asked by the system.

1.1 Admin

Get the uploaded book from the author and manually put the book in the database.

A. Login

Admin will login into the system.

B. Upload File

Here Administrator will upload number of books into the system database.This database is a structured database i.e. sorted.

1.2 Author

A. Registration

Author will register into the system with its own details.

B. Login

Author will login into the system.

C. Upload File

Upload Book and manually check whether the book is uploaded or not .Here Author will upload number of books into the system database.

1.3 User

A. Registration

User will register into the system with its own details.

B. Login

Login the user will enter the user name and password, if entered information is correct then the system will

- Redirect to the home page, otherwise it will show an error User want to login into the website.
- To enter the user id and password to login into the webpage.
- It well improves the security and preventing from unauthorized user enters into the network.

C. Search for Book

After login the user will search for book which he/she required.Then user will get ranked data from structured database.Then he/she can download the book and check the result.Otherwise he/she will check the no. of copies of the book and status of a book.

2.PROPOSED SYSTEM

In order to defend against stealth FDI attacks, mitigation schemes have been proposed to improve the bad data detection algorithm. Sequential detection (or quickest etection) of FDI attacks was designed mainly based on well-known Cumulative Sum (CUSUM) algorithm.Combined attacks can succeed with less resources. It reduces the total migration time and service downtime.

3.BLOCK DIAGRAM

3.1 SYSTEM ARCHITECTURE:

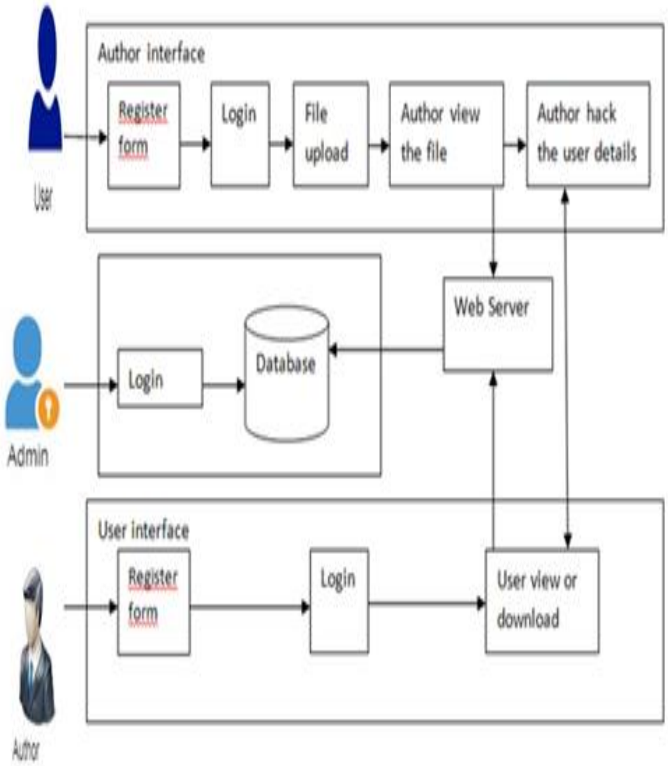

Fig:3.1 System Architecture

3.1.1 USER INTERFACE DESIGN

In this login page we have to enter login user id and password. It will check username and password is match or not (valid user id and valid password). If we enter any invalid username or password we can't enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network.

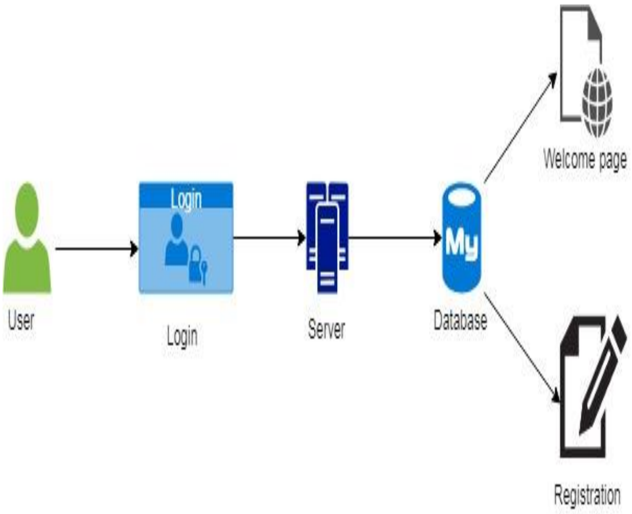

Fig:3.1.1 User Interface Design

3.1.2 AUTHOR INTERFACE DESIGN

Author login page we have to enter login Author id and password.It will check username and password is match or not (valid user id and valid password).

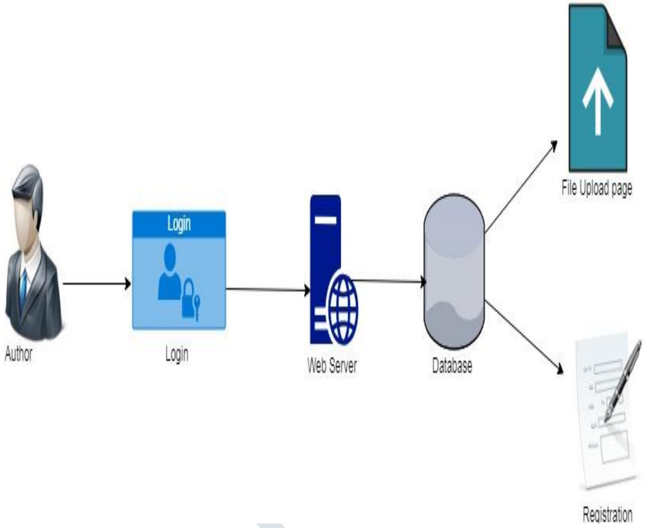

Fig:3.1.2 Author Interface Design

3.1.3 BOOK UPLOAD

Magazine upload into the website and free download book and pdf .User access the Magazine or book used the free website.Magazine or book many author list and book list are present in the website.

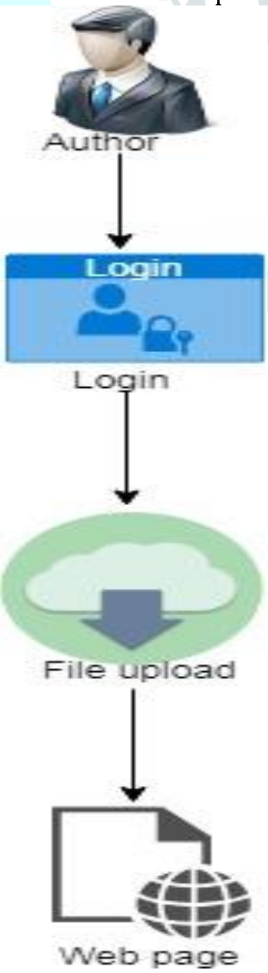

Fig: 3.1.3 Book Upload

3.1.4 AUTHOR VIEW THE BOOK

In this module the author view the book which is being uploaded. Check whether the uploaded book is correct or incorrect the upload the file.Check work the file view the author.

3.1.5 USER VIEW THE BOOK

User view the book list which is being uploaded by the author.Different types of Magazine being uploaded.
User can choose Magazine whatever book view or download etc.

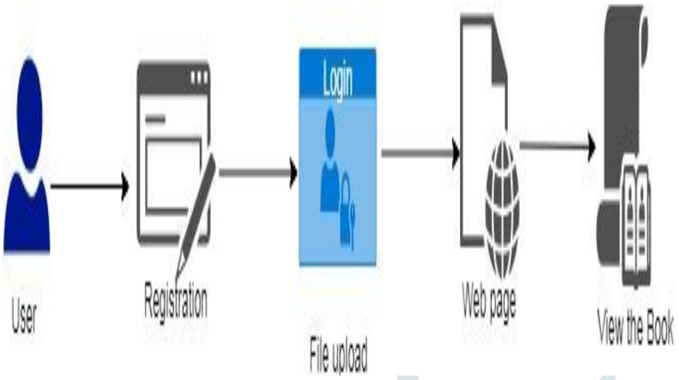

Fig: 3.1.5 User View The Book

3.1.6 AUTHOR VIEW THE USER LIST

Author hack the user personal details.User read the file name and product details.Author hacked the user details.

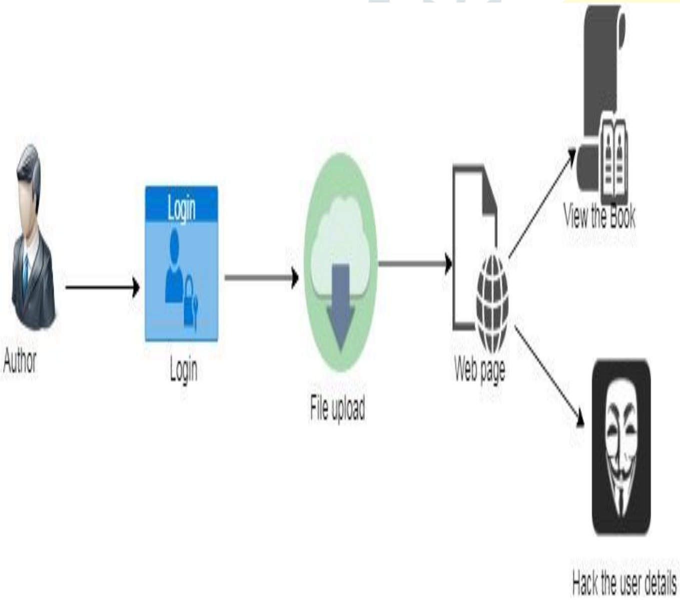

Fig: 3.1.6 Author View The User List

3.1.7 AUTHORIZATION

Admin view and maintain the file details and user details.

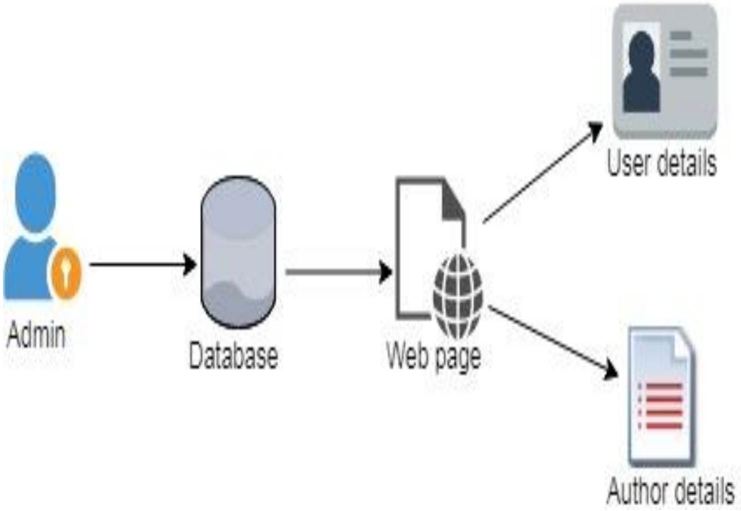

Fig: 3.1.7 Authorization

4.CONCLUSION:

In this paper we see that combined attacks can succeed with less resources (if CA < CI) and lower detection probability when the adversarial knowledge is limited, bringing more risk to reliable system operation. It also should be noted that this paper assumes that the SE treats unavailable measurements due to attacks as a case of missing data, although the amount of missing data under attacks is larger than the one under normal conditions. In the discussion we also showed the potentiality of designing a detector for availability attacks. Besides, availability attacks like DoS attacks could trigger alerts on ICT-specific measures (e.g., Intrusion Detection System). These two features give the opportunities to develop better cross-domain detection schemes for availability portion of the attacks improving the overall combined attacks detection.

5.FUTURE ENHANCEMENT

- Potentiality of designing a detector for availability attacks.
- Besides, availability attacks like DoS attacks could trigger alerts on ICT-specific measures. These two features give the opportunities to develop better cross-domain detection schemes for availability portion of the attacks improving the overall combined attacks detection.
- Future technique are physical impact of combined attacks.

6.REFERENCE

[1] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, “Data attacks on power system state estimation: Limited adversarial knowledge vs. limited attack resources,”http://arxiv.org/pdf/1708.08355v1, 2017.

[2] D. Deka, R. Baldick, and S. Vishwanath, “Optimal data attacks on power grids: Leveraging detection

measurement jamming," in Proc. Of IEEE Int. Conf. Smart Grid Communications (SmartGridComm), Miami Florida , USA, Nov. 2015, pp. 392–397.

[3] Jinping Hao ,Robert J. Piechocki ,Dritan Kaleshi ,Woon Hau Chin and Zhong Fan,"Sparse Malicious False Data Injection Attacks and Defense Mechanisms in Smart Grids,Sept 2015.

[4] K. Pan, A. M. H. Teixeira, M. Cvetkovic, and P. Palensky, "Combined data integrity and availability attacks on state estimation in cyberphysical power grids," in Proc. IEEE Int. Conf. Smart Grid Communications (SmartGridComm), Nov. 2016, pp. 271–277.

[5] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation,"IEEE Transactions on Smart Grid, vol. PP, no. 99, p. 1, 2016.