Predictive Analysis and Scalable Mechanism in Multilevel Security System by using CPS with Data Mining Techniques

Mrs. Sharada Varalaxmi Mangipudi [1]
Professor& HOD, Dept. of CSE&IT
St. Peters Engineering College.
Hyderabad, AP, India.
sharada.mangipudi07@gmail.com

Dr. M. Srinivasa Rao3
Professor, Dept. of CSE
Director of Academic Audit Cell
JNTU, Hyderabad,
srmeda@jntuh.ac.in

Dr. P. Suresh Verma [2]
Professor, Dept. of CSE
Nannaya University
Rajahmundry, AP, India
vermaps@yahoo.com

***Abstract*— The aim of this paper is to present a new approach in creating a Multi- Level Intelligence security system with the objective of risk-free multilevel security, by supervising the multi-user data access with an efficient auditing mechanism in association with Cyber-Physical System. We assure that it will overcome the existing problems without compromising the current models.**

Keywords-component; Cyber-Physical System, multiuser, data sharing, access control, data auditing, Data mining words.

I. INTRODUCTION

We are aware that defense / military and financial database systems can hold information at different levels of classifications like Public, Confidential, Secret , and Top Secret. The CPS has to confirm that their authentication and privilege can only access the data. The unauthorized data accessing is restricted in all the levels through a CPS, the principal, whose level is as high as the information's grouping. This approach is referred to as multilevel secure or on the other hand as Mandatory access control (MAC) [1].

Multilevel secure systems are necessary for the present cyber world .An enormous amount of research has been done on MLS, the military model of protection worked out in much detailed way than any other way, and it gives us lots of examples of the second order and even third-order effects of implementing a security policy rigorously.

II. RELATED WORK

From the past three decades, there are many intellectuals, research scholars, and many public/Private agencies which focused on this multi-level security system where information is defined in multiple methods.

A. SCOMP

One of the most critical method is the safe correspondences processor(SCOMP), a subsidiary of Multics propelled in 1983 This was an no-cost- saved implementation of what the US Department of Defense trusted it needed for taking care of information at various levels of characterization.

SCOMP was utilized as a part of applications, for example, military mail guards. These are particular firewalls which normally permit mail to go from low to high grouping levels and afterwards shared at the suitable items as orders to lower levels for usage.

B. BLACKER

Blacker was a progression of encryption gadgets intended to consolidate MLS innovation. Already, encryption gadgets were worked with partitioned processors for the ciphertext, or Black, end, and the cleartext, or Red, end. Different conceivable disappointments can be avoided in the event that one can arrange the Red and Black processing. Here we stated, in brief, the historical evaluation of the Multilevel Security with different models in the past.

1) **Biba Model:**
The Biba Model created by Kenneth J. Biba in 1975,is a formal state move arrangement of PC security approach that depicts an arrangement of access control rules intended to guarantee information integrity. Information and subjects are assembled into requested levels of integrity. In all , protection of information integrity has three objectives:

- Prevent information change by unauthorized parties
- Prevent unapproved information adjustment by authorized parties.
- Maintain inward and outward consistency.

2) **Bell-Lapadula Model:** This is a state machine model utilized for implementing access control as a part of government and military applications. It was produced by David Elliott Bell and Leonard J. LaPadula, to formalize the U.S. Department of Defense (DoD) multilevel security (MLS) strategy.
3) **Lattice Model:** This is an access control model in view of the association between any mix of items, for example, assets, PCs, and applications and subjects, for example, people, gatherings or associations.
4) **Water Mark Model:** It is an expansion to Biba Model. In Biba model, no write-up and no read down guidelines are authorized. In this model, the tenets are precisely the inverse of the guidelines in Bell-La Padula model. In the low-water mark design, write down is allowed, yet the subject name, subsequent to composing will be debased to question name.
5) **CMW:** The Chinese Wall Model is a thought that stems from the capacity to compose data. The principle thought is that you can to get to any data you need from any organization, however once you get that data, you are no more permitted to get to data from another organization inside that class of ventures.

III. OBJECTIVE OF THE PAPER

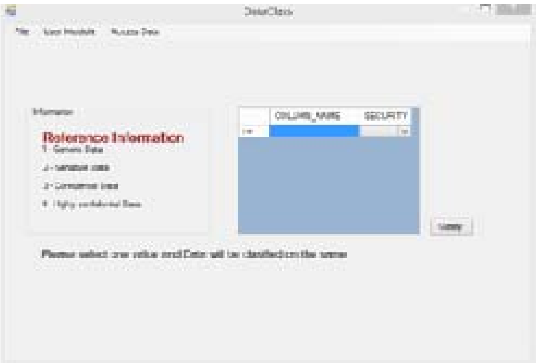
In this article, we proposed the research work with the following objectives

Objective 1: ***Creation of Security Model / Risk-Free Multi-Level Security System***

We built a multi-level security system which is risk-free with the success rates for unauthorized access and control of MLS is computed.

A. *Priority in the data classification*

The Unstructured/Unclassified information is categorized with respect to the quantitative values based on need – urgent, most urgent, future reference and based on the importance – private, public, secret and top secret. Here we have taken the load balancing algorithm for classification of information in the system with appropriate data storage



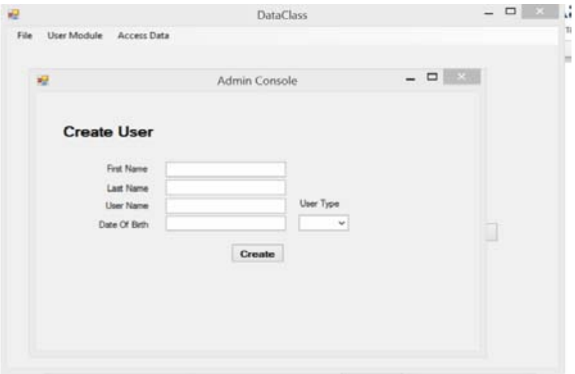
Reference Information
1- Generic Data
2- Sensitive Data
3- Confidential Data
4- Highly confidential Data

Please select one value and Data will be classified on the same

Fig.1 Data Classification

B. *User Classifications*

It is focused on the hierarchical model, in this, the people are classified on their designations. There are many users who may access the data from the information system of the database. For example, in any organization, there will be an administrative hierarchy, right from an attendant to the General Manager. But all are not having the same privileges for data accessing. Here the users are classified based on their designation and their roles and responsibilities. Everybody is authenticated to access their authorized information but they are not permitted to access unauthorized data. By using this user classification, we have reduced the overlapping of data access and the CPS plays a vital role of computing unauthorized data access.



Create User

First Name
Last Name
User Name
Date Of Birth
User Type

fig. 2 User Classification

C. *The storage of information in cluster form in the data warehouse*

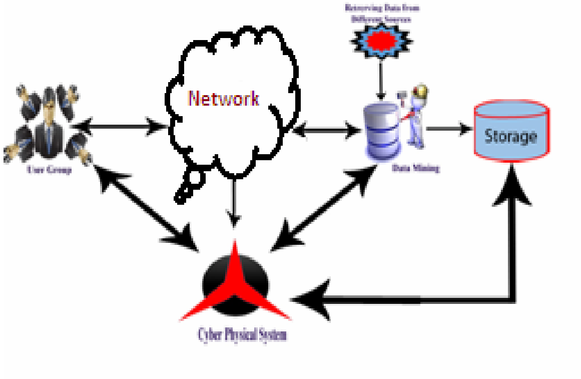


Fig. 3 Data Warehouse

The storage of data is focused on the below- given factors:

i). Access control methods are taken into consideration.

ii). The speed of the processor and Memory size

iii). data storage and its associated functions.

Objective2: ***Supervising the Data Sharing /transmission.***

The Cyber Physical System takes the role of monitoring the data in the data storage system /memory system. Suppose in the network for every second million and billion of users are accessing the data, the existing system may not be calculated - how many users are there on the network, how much data is sharing, the time duration of the individual users.

Whereas, the Cyber-Physical System is an automated device which contains an efficient computing capability on data sharing, scheduling, token passing for improving the system performance among the users by using traffic control techniques. We have developed the MLS by adding a unique feature to CPS. The CPS is in the position to choose the trusted path between the end users, trusted distribution among the network devices and trusted facility management

Objective 3: *Auditing Mechanism*

In this paper, we introduced auditing mechanism through CPS for an efficient MLS such as data transmission, data sharing between the users, the accountability of data and time duration for individual users and total users. A).By using token passing, we can evaluate the number of users for the particular interval of time. B).The total amount of time spent by each user in their respected level and another level of hierarchy.C)The total amount of data accessed by the individual users, group users, and all the users.

The level of information access is calculated with respect to the Users, Time, Data.

The total Number of users is N in the Network, The total allotted time for individual users is t; The total time is required for all the users is T. Therefore, when we calculate the total number of users- if N is increased there will be an interference, collide, deadlock. We have overcome this problem by developing an effective Scheduling algorithm to avoid the above problems. If T is increased, there will be an access control problem to overcome this issue we have set up an elapsed time into the CPS. It automatically activates and alerts the users for the elapsed time.

IV. PROBLEM WITH TRADITIONAL SECUIRTY MODELS

There are some problems in the existing MLS. Suppose the Biba model does not deal with the integrity of data. It is a theoretical model of little use but cannot be implemented in practical. Whereas The Bell–LaPadula model aims at data confidentiality and controlled access to classified data, but not on data integrity and it does not work well for commercial systems. In the watermark model, the integrity level of a subject is non-increasing

V. IMPLEMENTATION OF PROPOSED WORK

We were prepared the plan for implementation of the research work with the following structure of the proposed work.

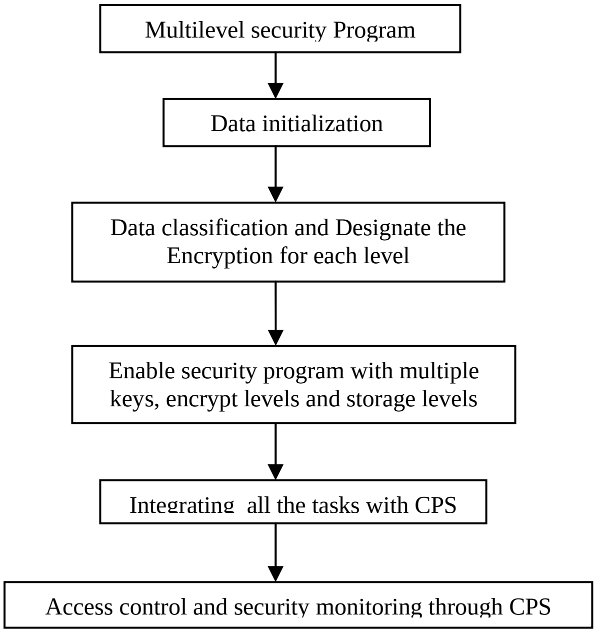
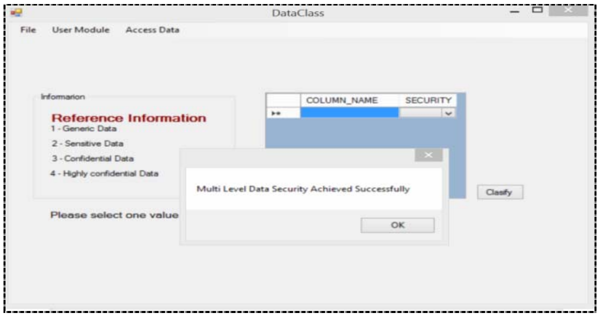

Multilevel security Program
Data initialization
Data classification and Designate the Encryption for each level
Enable security program with multiple keys, encrypt levels and storage levels
Integrating all the tasks with CPS
Access control and security monitoring through CPS

Fig. 4 Sequence work flow

Step 1: The unstructured data has been classified concerning Public, sensitive, confidential and High confidential

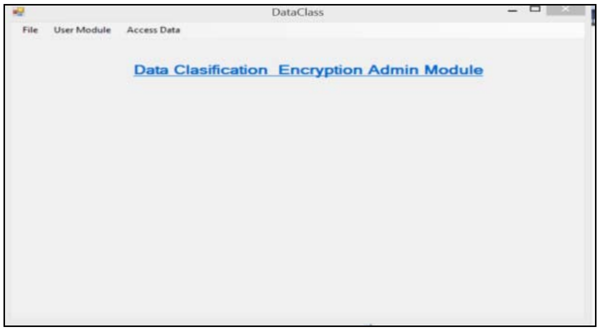


Reference Information
1 - Generic Data
2 - Sensitive Data
3 - Confidential Data
4 - Highly confidential Data

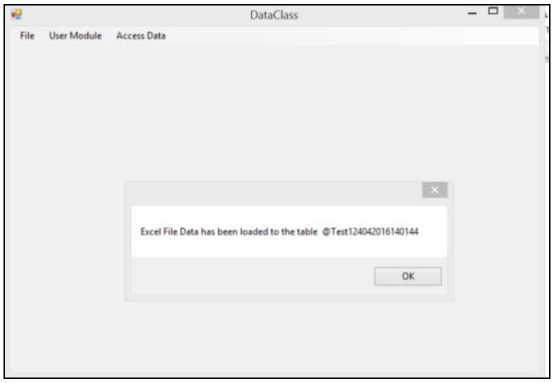
Please select one value

Multi Level Data Security Achieved Successfully

Step 2: After classification the data is encrypted by applying the MD5 algorithm. The original information is entirely modified in the hidden format.

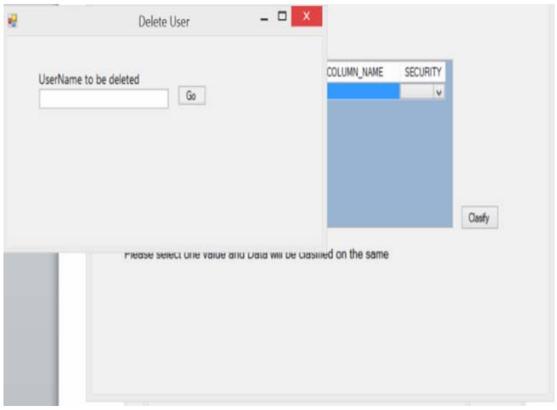


Step 3: The encrypted data loaded into the table form inside of database system.



Excel File Data has been loaded to the table @Test124042016140144

Step 4: After encryption the information is uploaded into the memory system. During the storage of data, a new technique is proposed as top, down and left , right approach through CPS. So that even the authenticated user can not access the unauthorised data. Even if anybody violates, the CPS is going to warn and put that user into the block list.



Please select one value and Data will be clasified on the same

VI. THE FUTURE OF MLS

The MLS becomes a qualitative product in the platform of the firewall; it works well with a server, web server.The existing frameworks are short in light and of the fact that the current models don't give a sufficient insurance advantage in numerous business situations to legitimize their colossal improvement cost and broadly theoretical items. I additionally noted examination on utilizing compulsory access controls to suit both privacy and honesty.

VII. CONCLUSION

The design of security for cyber-physical systems must take into account several characteristics common to such systems. Among these are interactions between the cyber and physical environment, distributed management and control, real-time requirements, and geographic distribution. This paper discusses these characteristics and suggests a design analysis approach that better integrates security into the core design of the system.

REFERENCES

[1] https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c08.pdf

[2] http://domino.research.ibm.com/library/cyberdig.nsf/papers/D2C93A2DF2AFD3968525728F00528D26/$File/RC24190.pdf

[3] http://wenku.baidu.com/view/e80e4866783e0912a2162a2f.html

[4] http://www.utdallas.edu/~bxt043000/Publications/JournalPapers/DAS/J13_Multilevel_Secure_Object_oriented_Data_Model_Issues_on_Noncomposite_Objects_and_Versioning.pdf

[5] Adams, C. M., "VOIP Quality Measurements in a Multilevel Secure (MLS) Environment," Masters Thesis, Naval Postgraduate School, Monterey, California, March 2008

[6] *[6].Bell, David Elliott (December 2005).* "Looking Back at the Bell-LaPadula Model" *Proceedings of the 21st Annual Computer Security Applications Conference. Tucson, Arizona, USA. pp. 337351*.10.1109/CSAC.2005.37.Slides - Looking Back at the Bell-LaPadula Model

[7] [7].http://nathanbalon.com/projects/cis576/Biba_Security.pdf

[8] [8].National Institute of Standards and Technology, Cyber-Physical Systems: Situation Analysis of Current Trends,Technologies, and Challenges, 2012.

[9] [8].Feng Xie and Tianbo Lu, Security Analysis on Cyber-Physical System Using Attack Tree, The Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2013.

[10] [10].Yong Peng and Tianbo Lu, Cyber-Physical System Risk Assessment, The Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2013.

[11] [11] Kyoung-Dae Kim and P.R. Kumar, “Cyber-physical systems: A perspective at the centennial,”Proceedings of the IEEE, vol.100, no. Special Centennial Issue, pp. 1287–1308, 2012.

[12] [12] Ragunathan (Raj) Rajkumar, Insup Lee, Lui Sha, and JohnStankovic, “Cyber-physical systems: The next computing revolution,” in Proceedings of the 47th Design Automation Conference, 2010, DAC ’10, pp. 731–736.

[13] [13] U.S. Energy Information Administration, U.S. Department of Energy,“International Energy Statistics,” [Online]:http://www.eia.gov/.

[14] [14] Boldizsr Bench, Gbor Pk, Levente Buttyn, and Mrk Flegyhzi,“The cousins of stuxnet: Duqu, flame, and gauss.,”FutureInternet, vol. 4, no. 4, pp. 971–1003, 2012.

[15] [15] T.M. Chen and S. Abu-Nimeh, “Lessons from stuxnet,” Computer, vol. 44, no. 4, pp. 91–93, 2011.

[16] [16] Industrial Control Systems Cyber Emergency Response Team,Department of Homeland Security, “ICS-CERT Alerts,” [Online]: https://ics-cert.us-cert.gov/alerts.

[17] [17] Igor Nai Fovino, Andrea Carcano, Marcelo Masera, and AlbertoTrombetta, “An experimental investigation of malware attacks on scada systems,”International Journal of Critical InfrastructureProtection, vol. 2, no. 4, pp. 139–145, 2009.

[18] [18] Aldar C.-F. Chan and Jianying Zhou, “Cyber-Physical DeviceAuthentication for the Smart Grid Electric Vehicle Ecosystem,”IEEE Journal on Selected Areas in Communications, vol. 32,no. 7, pp. 1509–1517, 2014.

[19] [19] Mike Rogers and C.A. Dutch Ruppersberger, “InvestigativeReport on the U.S. National Security Issues Posed by ChineseTelecommunications Companies Huawei and ZTE,” inU.S. House of Representatives, 112th Congress, 2012.

[20] [20] Sanaz Rahimi and Mehdi Zargham, “Analysis of the securityof{VPN}configurations in industrial control environments,”International Journal of Critical Infrastructure Protection, vol.5, no. 1, pp. 3 – 13, 2012.

[21] [21] Troy Nash,“Backdoors and holes in network perimeter,”[Online]: http://ics-cert.us-cert.gov/controls ystems/,2005

[22] JulianL. Rrushi, “Scada protocol vulnerabilities,” in Critical Infrastructure Protection, vol. 7130 ofLecture Notes in ComputerScience, pp. 150–176. Springer Berlin Heidelberg, 2012.

[23] U.K. Premaratne, J. Samarabandu, T.S. Sidhu, R. Beresh, andJian-Cheng Tan, “An intrusion detection system for iec61850automated

substations,"Power Delivery, IEEE Transactions on,vol. 25, no. 4, pp. 2376–2383, 2010.

[24] K. Elissa, "Title of paper if known," unpublished.

[25] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[26] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[27] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.