JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125VOL 7, ISSUE 15, 2020

PERSONALISED OPERATOR SECURITY SCHEME TO PREVENT DATA HACKING OF LEVEL PROCESS CONTROL SYSTEM

R. Karthikeyan[1], V S Hemalakshmi[2], M Yogalakshmi[3], N Yazhini, R Kalaivaani[4]

R. Karthikeyan, Assistant Professor, Dept of Instrumentation & Control, Sri Sairam engineering college, Chennai, Tamilnadu, India. (Email: karthikeyan.ice@sairam.edu.in)
V S Hemalakshmi, Student, Dept of Instrumentation & Control, Sri Sairam engineering college, Chennai, Tamilnadu, India. (Email: @sairamtap.edu.in)
M Yogalakshmi, Student, Dept of Instrumentation & Control, Sri Sairam engineering college, Chennai, Tamilnadu, India (Email: @sairamtap.edu.in)
N Yazhini, Student, Dept of Instrumentation & Control, Sri Sairam engineering college, Chennai, Tamilnadu, India. (Email: @sairamtap.edu.in)
R Kalaivaani, Student, Dept of Instrumentation & Control, Sri Sairam engineering college, Chennai, Tamilnadu, India (Email: @sairamtap.edu.in)

ABSTRACT: In recent years sabotage of process plants by hacking into their control system has been increasing and also alarming. Even though many data encryption and online firewall has been provided: hackers are smart enough to alter the control parameters or start / stop any equipment without the knowledge of the operator in plant. This paper proposes a novel Personalised security system to prevent such hackers from altering or start / stop any process. The proposed system uses the Personalised data such as the face recognition and biometric data of the concerned operator in the plant and creates a physical interlock between the control scheme and security system. The face features and biometric data of all operators are stored in the system and the operator log is maintained for every shift. Only when the finger print and face of the particular shift operator is matched with the shift log the system will allow changing the control parameters or to start and stop the process. This allows better security such that the hackers may find difficult to hack into the control scheme

Keywords: Security system, Face detection, Face Recognition, GUI.

I.INTRODUCTION

In process industries the control scheme are nowadays connected to the outside world for various administrative purposes. This leads to higher security risk of the control scheme where the control parameters or the set point ranges can be changed by any person who has the access on the network. Various hardware implementations has been carried out to make the system safe, but still the problem of safety continues and its being vital in high value process industries like nuclear power plants. Few problems that were identified in recent years are unexpected false alarms going on to mislead the operator and make him panic. Increasing the data in the network and making the response time of the control scheme very slower such that it may lead to a low efficient product or capacity, the pumps were made to misoperate creating a total quality disaster of the products, communication lockups to avoid reporting of incidents. In a noted incident an ex-employee hacked a Dematerialized water plant and made the water flooded with the entire plant wasting gallons of water to the industry which led to a total disaster of the plant which incurred a huge loss.

Another major concern is adopting of wireless technologies is security, as the wireless medium is open for eavesdropping and interference (Mustard, 2006). The security issue is solved by authentication and encryption methods (Karlof et al., 2004). The key features to be monitored and controlled in a high valued industries are regulary checking of the data if it is changed or modified without the authorization of the operator or the background supervisor, Data logging of nature of information being hacked and the code hacked will report hacking easily, creating confidentiality of the operator and supervisor logging dates to create a data base of safer operation.

In this paper we propose a hardware approach to have a personalized security system which regulary identifies the person who has the access to the control parameters and enable a safe passage only for that particular operator to control the process. It uses an Image system and a biometric system to confirm the operator in charge and gives access only to him the control algorithms. This paper gives a cost effective and user

ISSN- 2394-5125VOL 7, ISSUE 15, 2020

friendly performance with higher accuracy. This method has a problem where the images of the recognized faces are considered to be a two dimensional information rather than a three dimensional information. A human face normally has distinct feature in lips, nose and iris. The biometric sensors have a very high speed of operation and accuracy so that it can be reliable if made in connection with other secure parameters thereby increasing the level of security.

II. PROPOSED SYSTEM

Fig 1. Shows the conventional process control system in which a PID controller is used to control the level in a process tank by actuating the control valve. The tuning parameters such as proportional gain, derivative gain and integral gain can be changed by the supervisor or the control engineer in the field

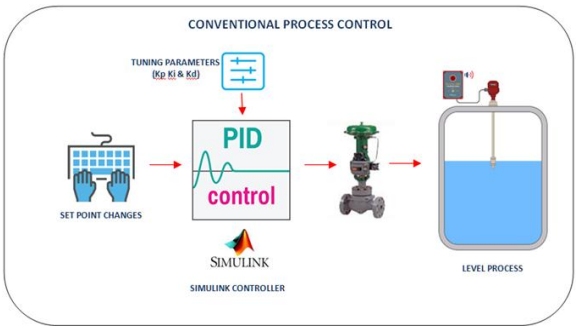

Fig. 1. Conventional level process control scheme implemented in process industries.

As well the operator has the access of altering the ser point that is the desired level into this process or changing the alarm set points such as high level alarm or low level alarm so as to alert the operator or to shut the process of any abnormality. The data are fed through a key board input to a touch screen monitor. Few hardware keys are providing so as to protect from unauthorized person changing the dates.

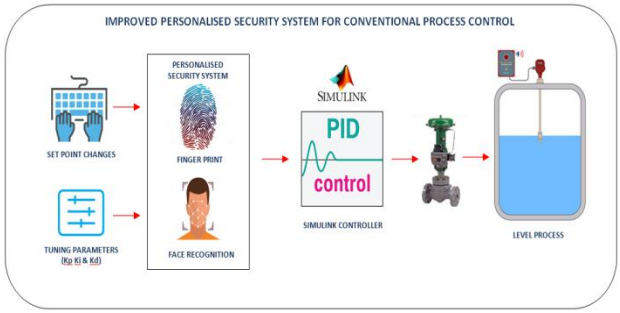

Fig. 2. Proposed improved personalized security scheme for level process.

Fig 2. shows the proposed personalized security system in which the change of control parameters like Controller gains and operator parameter such as set points and alarm limits are protected and the change is authorized only if the hardware check such as image and biometric system passes with the concerned shift operator, supervisor and engineer which will be a dynamic data and will be confidentially maintained so as to improve the security performance.

Every time for an operator to change the set point or alarm ranges him as to authenticate his information through face recognition and biometric system which are a hardware system attached to the specially designed keyboard which has a digital signature. The particular operator of the shift can change the desired level only from the particular keyboard and console and only for the particular shift from details mentioned in the operator log file which is a dynamic data controlled by the administration of the industry. This increases the complexity

ISSN- 2394-5125VOL 7, ISSUE 15, 2020

of identifying a data to be hacked and make the existing system safe without need of much costlier devises our system

As the input data to change any high value parameter can be configured to use this interlock and non essential parameter can have an option of excluding from this security to speed the operation. Fig. 3 shows the flow diagram of how the personalized security scheme is proposed. A camera and a biometric sensor form the acquisitions system. This data is given to the software for face recognition and biometric pattern matching. Initially the possible operator's facial and biometric dates are stored and the system is trainee to indentify that particular operators.

The output of the recognitions systems overrides the data input changed from the keyboard if the face and biometric recognition fails and further data input is locked to the last value and a alarm goes on to indicate a security breach.

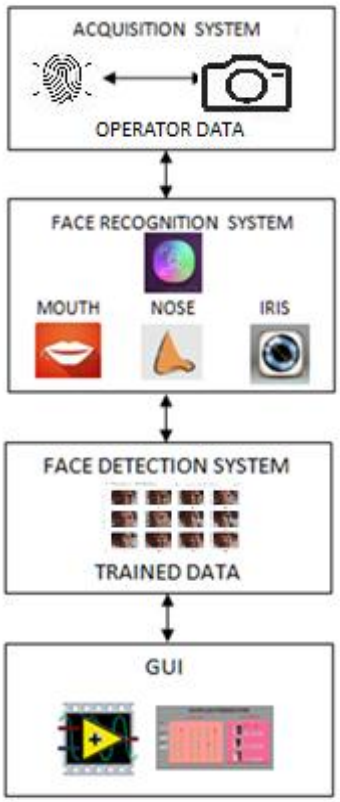

Fig. 3. Control flow of Improved personalized security scheme.

A. Hardware System

The acquisition system consists of two devises in this prototype a web cam is used and it also uses a bio metric sensor used has a working voltage of 5V and a working current of 80mA which is a 40mmx25mm module has an accuracy of 0.1%. These are low cost devises used for prototype purpose. The actual hardware is a level process station which has a level sensor and a control valve for controlling the process to the tank. Lab view hardwires are

Used for data acquisition and the control algorithm are implemented in Lab view software. The face recognition and biometric algorithm are also implemented through Lab view software

B. Face Recognition System

ISSN- 2394-5125VOL 7, ISSUE 15, 2020

The vision toolbox in Lab view is used to read the image captured. The data values of the pixel are stored as matrix information and are given an algorithm which based on a Viola Jones alga. The images are cropped for the area of face into an image file in jpeg format of a lesser known resolution. Further many such face is cropped into various features and in this paper three features such as lips of the operator, nose of the operator and the iris of the operator is cropped and taken separately and stored in a particular ID format to get it trained.

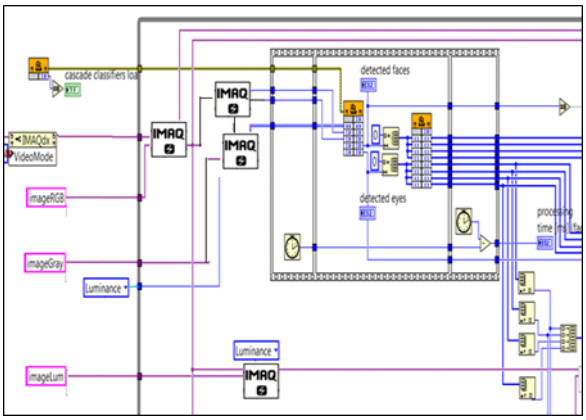

Fig. 4. Lab view block diagram of face detection

Figure 4 shows the lab view block diagram using vision toolbox. It captures the image from the camera to convert the image to binary values stored in a two dimensional array. A eigenface algorithm is used to convert the two dimensional image data of feature cropped image with a known resolution into a one dimensional vector and several such vectors creates a matrix of images. The pixel mean value of the vector is determined and compared with vector of each image one dimensional vector to the average into a new training matrix.

C.Face Detection System

A Matlab software is used for face detection system in which trained data of each features extracted by the different persons is stored after normalizing. The data. The database is stored in a system to otherwise recognize the measured feature of the particular operator where an illuminant map extraction is used. Whenever an operator is effectively predictable the system marks the output to the Lab view to process the interlock for authentication of the particular operator. Fig. 5 shows the images of the various people posting as an operator and the images are trained to effectively identify the particular operator of the shift which is listed in the operator log file separately which access I only give to the administrator. If any other operator face is detected is gives a separate output signal to the lab view interlock logic to stop the access to the high dates

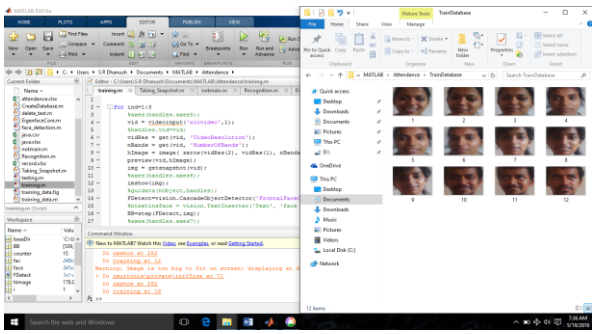

Fig. 5. Matlab test face detection system

ISSN- 2394-5125VOL 7, ISSUE 15, 2020

D. GUI

For the purpose of the prototype a lab view frontend is created to analyze the performance and the effectiveness of the system. The front end has a Set point control scroll bar a process variable bar graph and also has a bar graph for the output. The tank level is displayed and the chart plots the trend of the past level for future data analysis. The Face recognition and the biometric interlocks are provided and the name of the operator and his image is also displayed and store in the logging.

III.RESULTS

Using the database of 10 enrolled operators that are stored in the image folder the sample image of the operator is captured and for prototype purpose stored as a jpeg file. The image has a resolution of 720 X 1800 pixels. The execution speed varies with resolution and as the resolution increases the training time also increases. The accuracy of the algorithm also increases with increase in the pixel resolution. However, as there is a decrease in computational speed this may not be a suitable in critical system.

Application like a level process with large time constant system is a non sensitive application where computational time is not vital parameter. The image processing and biometric interlocks comes into effect only when there is a need for change in vital parameter like proportional gain, integral gain, derivative gain, set point changes, alarm range changes and change in certain important control configuration and fail safe systems.

Several limitations maps are to be taken into account and also the position of the operator while authenticating is also plays a vital role in effective identification. Many noise cancelling algorithm are used to improve the performance.

Figure 6, shows the lab view frontend panel diagram of a normal shift operator who is trying to change the control parameter the system recognizes the operators facial and biometric data and allows him to access the set point and the gain values. The authentication of face system is shown in the front panel diagram as well the biometric authentication is also indicated in addition the operator face image is also displayed in the front panel as well as stored in the data logger for future analysis.

Fig. 6. Lab view front panel diagram an authenticated operator changing the control parameters.

From the figure 7 it is clear when the algorithms detects a different facial or biometric recognitions the interlock gets activated and the algorithm stops the operator from changing the key control parameters. It locks the clue of the output to the last previous output such then it does not enter into an abnormal condition and the process is safe. It also generates an alarm in the system showing the access of unauthorized person and indicated and logs his face and finger print image.

ISSN- 2394-5125VOL 7, ISSUE 15, 2020

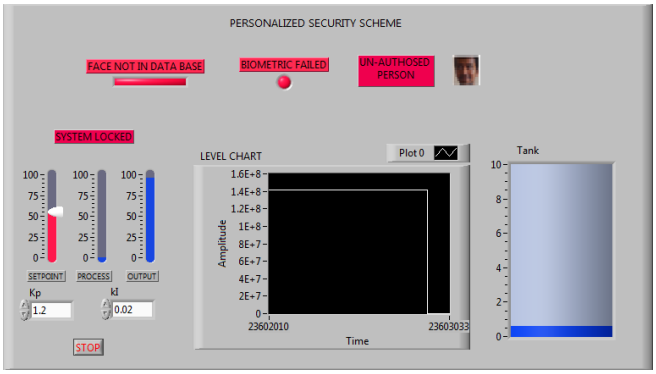

Fig. 7. Lab view front panel diagram of an unauthorized person tiring to access the control parameters.

This particular security system developed was checked in a real time level process systems with 3 people trained as operators. It gave access to all the operators to change the vital parameters and while an unknown person tried to access the data it locked the system and the level process went it a safe system where the last output just before unauthorized person was detected.

IV.CONCLUSION

Using Lab view for a personalized security scheme for a level process favored a better result in terms of external hacking of the high value parameters so as to sabotage the process. This proved to be a low cost solution but the speed of operation of the system reduced when there was a intention of set point changes as the two basic algorithms as to execute to authenticate the operator or supervisor or the plant engineer.

Lighting during blackout is a vital drawback but it can be easily avoided. The system studied with 3 operators and it can be extended to many such operators. Future plans are to study, analyze the speed of operation of certain critical process like reactor temperature based on the yearlong data and can improve security of the system..

V. ACKNOWLEDGMENT

We thank for the support of our Management of Sri Sairam Engineering College, teachers of Dept. of instrumentation and control engineering. We thank for their enormous support, motivation, and resources

REFERENCES

[1] Paul Viola and MichaelJ. Jones, "RobustReal-TimeFace Detection,"International Journal of Computer Vision, vol. 57, no. 2, pp. 137-154, May 2004.
[2] Chetan.R, Rajesh Nayak, "Automated Attendance System Based on Facial Recognition International Journal for Research Trends and Innovation " Volume 2, Issue 6 | ISSN: 2456-3315
[3] Hitesh Walia, Neelu Jain "Fingerprint Based Attendance System Using LabVIEW and GSM" International Journal of Innovative Research in Science, Engineering and Technology Vol. 5, Issue 7, July 2016
[4] T.Thaj Mary Delsy, N.M.Nandhitha, Feasibility of spectral analysis techniques for disruption analysis in Aditya tokamak. International Journal of Engineering & Technology, [S.l.], v. 7, n. 4, p. 3843-3846, dec. 2018
[5] T.Thaj Mary Delsy, N.M.Nandhitha, "Spectral statistical analysis of low frequency coefficients from diagnostic signals depicting MHD disruptions", 978-1- 5090-4967- 7/17/$31.00 2017 IEEE,
[6] Sandhya, P & Thaj Mary Delsy T. (2016). Adaptive detection of pulmonary nodules in ct images by segmentation and classification using matlab. 8. 11980-11985.
[7] H. A. Mayank Agarwal, "Face Recognition Using Eigenfac e aproach," IRCSE, vol. 2, no. 4, pp. 1793-8201, August 2010.
[8] Vinay Hermath, Ashwini Mayakar, "Face Recognition Using Eigen Faces and," IACSIT, vol. 2, no. 4, pp. 1793-8201, August 2010.