Volume 4, Issue 5, May 2019 ISSN (online): 2456-0006
International Journal of Science Technology Management and Research
Available online at: www.ijstmr.com

Authentication Scheme Using Personal Devices

Ms. Prajakta Jachak
Dept. of Information Technology
MET's Institute of Engineering, Nashik

Ms. Priyanka Kumavat
Dept. of Information Technology
MET's Institute of Engineering, Nashik

Ms.Achal Patil
Dept. of Information Technology
MET's Institute of Engineering, Nashik

Prof. Kunal Ahire
Dept. of Information Technology
MET's Institute of Engineering, Nashik

Abstract- ***Now days most of the security system uses traditional methods for the authentication for example by providing user name and password ,smart cards etc but in these techniques the user verified only one time at the initial logging, after that he can access all the resources until he logout. This will lead to session hijacking if authenticated user takes short break the hoaxer can gain the control over system. To overcome these issues we have to use system that should continuously examine the user for assuring the user authority. Current System continuously examine user using multi modal biometrics but still there are some issues such as we all know that face detection(hard biometric) is not 100 % accurate there are some constraints with it, and all these done using image processing and it contains some flaws. Also user can't afford such expensive system. To overcome all these issues we proposed cost effective system, which will continuously monitors user and detect whenever user leaves workstation. For that we are going to used RFID for unique identification, IR/IR sensor to detect presence of user in front of computer System and keystroke dynamics that will checks the behavior of user which are unique for each user so it will provide highest security as compare to exiting logging systems the new thing in our system that we going to used RFID and IR/IR sensor in which there is no need to do image processing, whenever user leaves workstation system will logout immediately. The advanced biometric technique which analyzes the behavior characteristic of the user called behavior biometrics .The behavior biometric technique implements using mouse dynamics that analyze and extract the characteristics movement of the user, when he interacts with the computer. This will provide highest security to the system and resources.***

Keywords— Microcontroller (arduino kit), IR/IR sensor .

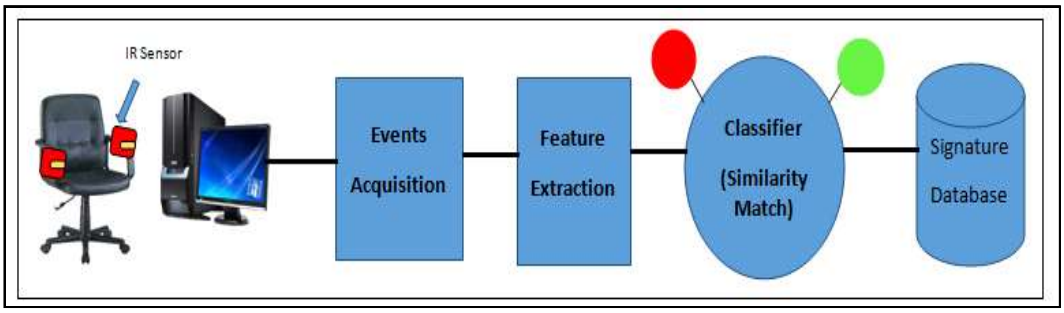
I. INTRODUCTION

Today most of the computer systems, e-banks and websites uses alphanumeric password for user identity verification. However this authentication system does nothing to protect the computer from unauthorized access once the user has started an active session. User authentication at sign on secures the workstation only against unauthorized access while the workstation is powered down. But normally hackers can easily steal the password with the help of so many techniques. Some of the techniques are phishing attacks, key logger and so on. Also sometimes a user computer remains unlocked at that time hackers can install the key logger in user computer or by sending some links to that computer, Ex. Greetings or some images, videos etc. If user clicks on that link key logger installs on that computer, it records every keystroke including passwords, usernames, and screen shots after 5-5 minutes. Also they can send that hacked data to hackers without knowing to user. In high risk environments or where the cost of unauthorized use of a computer is high, Continuous verification/ authentication of the user identity is extremely important. Continuous User Authentication has built

around the biometrics supplied by the user behavioral characteristics and continuously checks the identity of the user throughout a session. This is referred to as continuous authentication. Continuous authentication is very useful for continuous monitoring applications such as intrusion detection. This method identifies the user movements or characteristics when the user interacts with the mouse and keyboard, results in the generation of mouse gestures and checks every time when the user make session and provides authentication to the users.

The mouse and keyboard gestures are drawn in unit-stroke. User identity verification via mouse and keyboard gesture dynamics is a method that continuously verifies users according to characteristics of their interaction with the mouse. The contribution of this work is threefold: first, user verification is derived based on the classification results of each individual mouse action, in contrast to methods which aggregate mouse actions. Second, we propose a hierarchy of mouse actions from which the features are extracted. Third, we introduce new features to characterize the mouse activity which are used in conjunction with features proposed in previous work. Proposed system uses the IR sensor and keyboard and mouse dynamics when user leaves workstation system will logout automatically. The proposed algorithm Out performs current state-of-the-art methods by achieving higher verification accuracy while reducing the response time of the system.

BLOCK DIAGRAM:



II. LITERATURE SURVEY

Different from existing works, we exploit dynamic authentication credentials along with user-centric access control to solve the static credential problem. Our approach is to introduce one-time usernames utilizing users smart devices and cryptographic primitives such as encryption, digital signature, and hashing. The goal is to create a unique username and password set for each session such that various security vulnerabilities in conventional, static user name and password systems can be tackled. In our comparison study, we focus our attention on 5 different schemes that are closely related to our work.It can be clearly seen that our design outperforms many proposed schemes with respect to the security metrics since we utilize various cryptographic primitives that facilitate meeting the framework security requirements.The estimated idea of this paper is useful for providing high security to the system or resources. The survey up till now, concludes many projects are implemented for initial logging only. Conclusions drawn from the different papers are discussed as follows

Anil K.Jain, An Introduction to Biometric Recognition, In IEEE Transactions on Circuits and system for video technology, 051-8215 , 2004 IEEE said that, Reliable personal recognition is critical to many business processes. Biometrics refers to automatic recognition of an individual based on her behavioral and/or physiological characteristics. The conventional knowledge-based and token-based methods do not really provide positive personal recognition because they rely on surrogate representations of the persons identity (e.g., exclusive knowledge or possession). It is thus obvious that any system assuring reliable personal recognition must necessarily involve a biometric component

III. PROPOSED SYSTEM

Most of the authentication systems use alphanumeric characters in their password, but their system fails from several attacks such as brute force attack, guessing, social engineering etc. Though the biometric technology which is available today produces high

accurate processing, it needs additional or special purpose hardware and large processing time to achieve it. The advanced biometric technique which analyzes the behavior characteristic of the user called behavior biometrics .The behavior biometric technique implements using mouse dynamics that analyze and extract the characteristics movement of the user, when he interacts with the computer. This extracted information is later used for the authentication purpose .The existing systems achieve better work well in continuous authentication.

Verification of each individual mouse action increases the accuracy while reducing the time that is needed to verify the identity of the user since the fewer actions are required to achieve a specific accuracy level, as compared to the histogram- based approach which is explained in. A biometric-based user verification system is essentially a pattern recognition system that acquires biometric data from an individual, extracts a feature set to establish unique user signature and constructs a verification model by training it on the set of signatures. User verification is achieved by application of the model to on-line acquired signatures of the inspected user that are constructed using a process that is identical to the one used during the model construction.

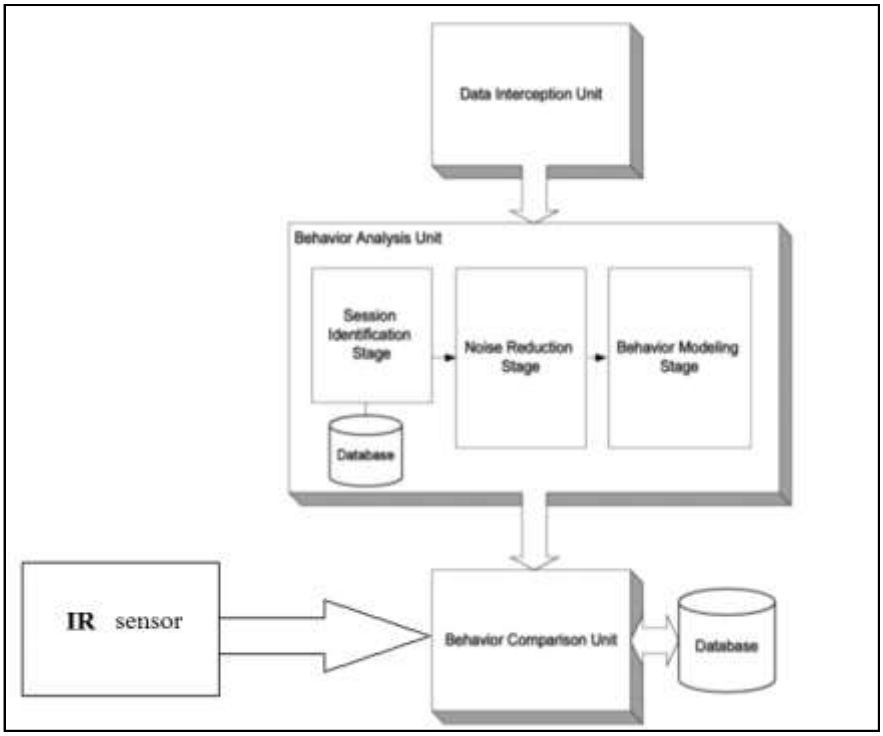


Fig 1: Architecture of proposed system

Mathematical Model:

Class of Problem:

The Class P

P is the class of decisions that are polynomials bounded. P is defined only for decision problems. It may seem rather extravagant to use the existence of a polynomial Time bound as the criterion for defining the class of more or less reasonable problems polynomials can be quite large. There are, however a number of good reasons for this choice. First, while it is not true that every problem in P has an acceptably efficient algorithm, we can certainly say that if a problem is not in P, it will be extremely expensive and probably impossible to solve in practice.

A second reason for using a polynomial bound to define p is that polynomials have nice "closure" properties. An algorithm for a complex problem may be obtained by combining several algorithms for simpler problems. Some of the simpler algorithms may work on the output or intermediate result of others.

A third reason for a using polynomial bound is that it makes P independent of the particular formal model of computation used. A number of formal models are used to prove rigorous theorems about the complexity of algorithms and problems.

The Class NP
NP is the class of decision problems for which a given proposed solution for a give input can be checked quickly (in polynomial time) to see if it really is a solution. More formally, inputs for a system and proposed solution must be described by strings of symbols from some finite set.

NP-Hard Problems
NP-hard (Non-Deterministic polynomial time hard), in computational complexity theory, is a class of problems that are, informally at least as hard as the hardest problem in NP.A problem H is NP-hard if and only if there is an NP-complete L that is polynomial time turning reducible to H.

NP-Complete Problems
NP-Complete is the term used to describe decision problems that are the hardest ones in NP in the sense that, if there were polynomials bounded algorithm for an NP-complete problem, then there would be a polynomials bounded algorithm for each problem in NP.

This is a P class problem. The algorithms used in this system are fixed algorithms.
So it will not go into NP Hard class.

formulae:

1. Trajectory Center of Mass (TCM) - A single feature that measures the average time for performing the movement where the weights are defined by the traveled distance:

$$TCM = \frac{1}{S_n} \sum_{i=1}^{n-1} t_{i+1} \sqrt{\delta x_i^2 + \delta y_i^2}$$

2. Scattering Coefficient (SC) - measures the extent to which the movement deviates from the movement center of mass:

$$SC = \frac{1}{S_n} \sum_{i=1}^{n-1} t_{i+1}^2 \sqrt{\delta x_i^2 + \delta y_i^2} - TCM^2$$

3. Third and Fourth Moment (M3, M4) – Evaluation Measures:

The implemented system evaluation can be done according to the FAR, FRR, EER. In order to create the ROC curve we have examined the FAR and FRR for various values of _ 2 [0; 1]. It gives that decreasing the value of k produced a lower FRR and a higher FAR. Accordingly, it first calculated Ppost for all test instances. Then, sorted the test instances in descending order according to Ppost and processed the instances one at a time from beginning to end setting k=Ppost. After obtaining the ROC graph, the actual value of k should be set according to the desired FAR/FRR.

$$FRR = \sum_{j=1}^{n} count(FR_j)/n * 100$$
$$FAR = \sum_{j=1}^{N} count(FR_j)/N * 100$$

EER is the values at which both ERR and EAR are equal. Low EER value indicates accurate authentication system.

IV. RESULTS

Table : Comparing Verification Accuracy between Internal and External Users

Method	FRR	FAR	No of Mouse Actions	Movement Type
Existing method	9.53%	17.66%	30 mouse actions	Free movement
Implemented method	5.20%	12.44%	30 mouse actions	Free movement

The table shows comparisons between implemented system and existing system. In this global FRR and FAR is calculated. We observed an improvement in performance with internal FRR 5.20% and FAR 12.44%. So that external EER is 8.82% which is much lower than existing method so that system gives accurate results.

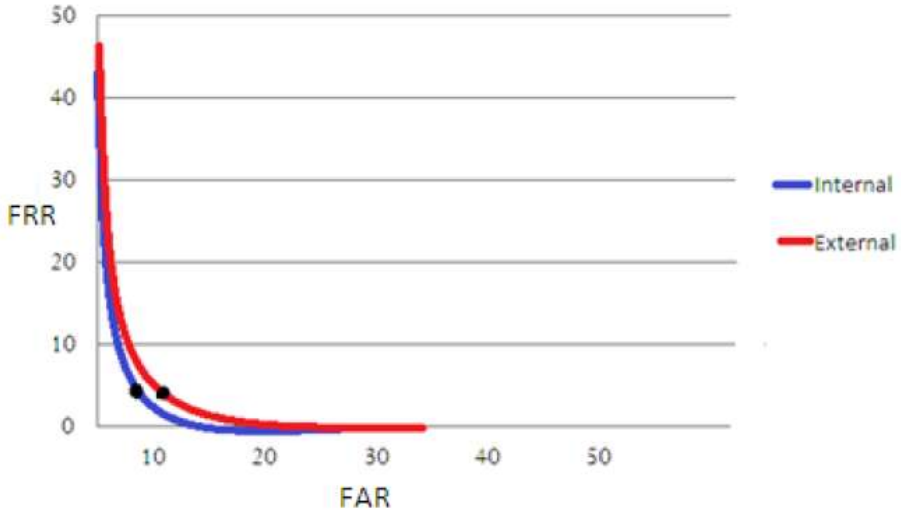


Fig 2 : ROC Curve Comparing Verification Accuracy between Internal and External Users

CONCLUSION

This work presents a trust-aware system for generating personalized user recommendations in social networks. Its foundations lie on a reputation mechanism that is mathematically formulated, comprising both local and collaborative rating formation. Trust is calculated using local rating, collaborative rating. Transitivity of trust is also calculated using different formulas. And finally Trust-Aware Personalized Recommendations is formed.

Hence conclude from this paper using by fault diagnosis tool for circuit breaker wiring harness get less consumption of time and then tool operate purpose not required skilled person and easily operate this tool. in future this is most important tool because save more time according to fast or digital word.

FUTURE WORK

Future plans include the study of different social networking systems and by applying trust-aware system to that Social networking systems and evaluating its performance in different ways which helps us to make trust aware system more helpful for social networking users. This Future work can be done with the help of following some factors, 1) For different social pages and groups 2) direct rating to friend profile Some future plans for this factors are, 1. Social Networking websites contains some groups or pages, these system made helpful for calculating trust for that groups or pages. This trust factor can be calculated by trust factor of that

group/ page users and posts added into it. This trust factor helps users who wants to join that group or pages. 2. Direct rating of one user to his friend can be made. One user gives rating to her friend this rating is made useful for calculating trust or handling mutual friend requests.

REFERENCES

1. A.A.E. Ahmed, I. Traore, "A new biometric technology based on mouse dynamics", IEEE Transactions on Dependable and Secure Computing (2007)165-179.
2. L. Breiman, "Random forests", Machine Learning (2001) 5-32.
3. E. Erzin, Y. Yemez, A.M. Tekalp, A. Eril, H. Erdogan, H. Abut, "Multimodal person recogniti for human vehicle interaction", IEEE MultiMedia (2006) 18-31.
4. P. Grother, E. Tabassi, "Performance of biometric quality measures", IEEE Transactions on Pattern Analysis and Machine Intelligence (2007) 531-543.
5. Kale, A. Sundaresan, A.N. Rajagopalan, N. Cuntoor, A. Roychowdhury, V. Kruger, R. Chellappa, "Identification of humans using gait", IEEE Transactions on Image Processing (2004) 1163-1173.
6. A.Kumar, S. Shekhar, "Personal identi_cation using multibiometrics rank-level fusion", IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews (2011) 743-752.
7. M. De Marsico, M. Nappi, D. Riccio, G. Tortora, "NABS: novel approaches for biometric systems", IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews (2011) 481-493.
8. B J Gorad, D.V Kodavade, "User Identity Verification Using Mouse Signature", IOSR Journal of Computer Engineering (2013) 33-36.
9. Peter Ordal, David Ganzhorn, David Lu, Warren Fong, "`Continuous Identity Verification through Keyboard Biometrics'", Department Of Computer Science (2005) 20-24.
10. D. Shanmugapriya, G. Padmavathi, "`A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges'", IJCSIS (2009) 115-119.