Biometric Device Assistant Tool: Intelligent Agent for Intrusion Detection at Biometric Device using JESS

Prof. Maithili Arjunwadkar [1], Prof. Dr. R. V. Kulkarni [2]
[1]Assistant Professor, Modern College Of Engineering,
University of Pune ,
Pune 411005
Maharashtra,India.

[2] Professor, Chh. Shahu Institute of Business Education & Research
Shivaji University,Kolhapur
Kolhapur 416004
Maharashtra ,India.

Abstract

While there are various advantages of biometric authentication process, it is vulnerable to attacks, which can decline its security. To enhance the security of biometric process, Intrusion detection techniques are significantly useful. In this paper, we have designed intelligent agent as knowledge based Biometric Device Intrusion Detection tool which is an innovative design. This intelligent agent can be located on the Biometric device. It performs intrusion detection using Operating System's audit trail and device manager information. The system consists of a user interface module, an inference engine, a knowledgebase of illegal transactions and certified biometric devices. Inference engine is implemented using JESS which is a Java Expert System Shell.

Keywords:*Biometric device,liveness detection, intelligent agent, multiagent system,Java Expert System Shell(JESS)*

1. Introduction

Establishing the identity of an individual is of vital importance in several applications like attendance system, health application system, airport security, passports or driver licenses, and financial applications where errors in recognition can challenge the integrity of the system. Instead of using traditional authentication techniques like password, PIN, ID cards etc. the biometrics authentication system is a secure and efficient alternative to traditional authentication systems. The biometric authentication is the automatic identification or verification of an individual using a biological feature they possess such as fingerprints, iris recognition, retina scan, facial features, hand geometry, voice, signature etc. A Biometric Device identifies an individual by examining a unique physical or behavioural characteristic such as the individual's fingerprints, hand geometry, eye patterns, voice, or dynamic signature etc.

The biometric authentication systems are used in either centralized or distributed architecture. They mostly differ by how the processing steps for biometric authentication system are divided between different machines.

While there are various advantages of biometric authentication system, it is vulnerable to attacks, which can decline its security. Attacks on the biometric device can be segregated into different scenarios [1].

The different scenarios are as follows:

1. Forcibly compelling a registered user to enrol and verify or identify.
2. Presenting a registered demised person or dismembered body part
3. Using genetic clone
4. Fake or artificial biometric samples or spoofing.
5. Collecting or submitting biometric sample from unauthorised biometric device

In this paper we focus only on scenarios 4 and 5.

A spoof is a counterfeit biometric that is used in an attempt to circumvent a biometric sensor. It is nothing but a process that defeats a biometric system by providing a forged biometric copy of legitimate user. Although spoofing techniques vary with biometric technologies, one thing they have in common is that they all involve presenting a fake biometric sample to the device. Therefore, it is necessary to capture a biometric sample from a legitimate user. The artificially recreated data is used to attack physiological biometric technologies, for instance, by using a fake finger, substituting a high-resolution iris image, or presenting a facemask. Besides the artifacts, mimicry is often used to spoof behavioral biometric technologies. Spoof detection can occur before biometric data is collected or during data processing. One method for anti-spoofing is called "liveness detection"[2]. The liveness detection is applicable when mimicry is carried out through a biometric device. Liveness detection is a technique which is used to determine the collected or submitted biometric sample taken from live person or fake sample. Liveness detection is based on the principle that additional information can be collected for

biometric sample which is submitted at the time of enrolment and verification process. Liveness detection uses either hardware based system or software based system coupled with the authentication program to provide additional security. Hardware system uses additional sensor to gain measurements outside of the biometric sample itself to detect liveness. Liveness detection in incorporated into a system through the extra hardware components with the capture device that can search through temperature, pulse, blood pressure, skin deformation, pores, , Heartbeat, Skin Resistance, Facial thermograms etc. Software-based systems use image processing algorithms to collect information directly from the collected biometric sample to detect liveness which is integrated into the system [3].

The biometric system is flexible regarding device used; the system still needs to make sure that the device is an authorised (certified) device and not fake device which causes fake readings. Consequently, some form of identification mechanism for the device is required. An intelligent agent is a program module which is built for a purpose to continuously sense in a particular environment and acts based on the environmental conditions. Therefore, it is able to carry out activities in a flexible and intelligent manner to be responsive to changes in the environment. Moreover, such an agent is able to learn from its experiences. Since the agent is autonomous, it takes actions based on its built-in knowledge and its past experiences stored in the form of rules. The proposed agent module verifies authenticity of the device before sending the biometric sample to the feature extraction module and it also receives input from biometric device whether liveness detection is active or not without considering hardware based system or software based system liveness detection.

2. Proposed System

In proposed system, we develop an intelligent agent to assist intrusion detection. Biometric process or biometric encryption process is divided into two processes namely enrolment and authentication process. We consider few possible threats that are mentioned below.

1. At the time of legitimate enrolment, the accuracy of the biometric data is essential. If identity is faked, the enrolment data will be an accurate biometric of the individual but identity will be incorrectly matched. Once registered, the system will validate a false identity, and with it illegal access of application
2. At the time of legitimate enrolment and verification, the data should be from the living person.

On the basis of above threats and policies, we have developed intelligent agent which can check collected sample from authenticated biometric device and from a living person. The ability to authenticate a biometric device to the system is a significant step towards a secure biometric process.

A packet containing the biometric sample - UserId, The Capture Time Stamp, The Device Serial Number, Device Model Number, Status of Liveness Detection and Process Name for which sample is captured can be collected from the system to validate device.

The knowledge like make, model and serial number of authentic device is stored as a form of facts and rules in a JESS knowledge base. It is somewhat similar to a relational database, especially in that the facts must have a specific structure. A rule-based system maintains a collection of knowledge nuggets called *facts.* This collection is known as the *knowledge base.* It is somewhat similar to a relational database, especially in that the facts must have a specific structure. Similar to object-oriented languages, *objects* have named *fields* in which data appears; unordered facts offer this capability (although the fields are traditionally called *slots.*) We use unordered facts because they are structured in nature. In our implementation, the biometric device data model has following template definitions.

```
(deftemplate DeviceInfo
(slot make)
(slot model)
(slot serialNo)
……)
```

In addition to the facts, rules are defined. We design different rules for find out fake device which is not certified by authorities. The knowledge is represented as the following rule.

```
If capture purpose is enrolment
AND
Capture sample device is not in the list of certified
device
Then Modify device is fake device ,
        Increase count of fake device ,
        Assert counted value into facts ,
        Assert model info into facts
```

The above rule says that if the capture purpose is enrolment and sample collected from biometric device having make, model and serial number contains in knowledgebase then device is fake device and is not authentic device, then modify device is fake device and increase fake device count and new value asserts into facts. The Defrule can search knowledge base to find relationships between facts, and rules can take actions based on the contents of one or more facts. A Jess rule is something like an IF…THEN statement in a procedural language, but it is not used in a procedural way. While IF…THEN statements are executed at a specific time and in a specific order, according to how the programmer writes those, Jess rules are executed whenever their IF

parts (their left-hand-sides or LHSs) are satisfied, given only that the rule engine is running. This makes Jess rules less deterministic than a typical procedural program. Rules are defined in Jess using the Defrule construct [4].

The following is the JESS language representation of the above rule.

```
(defrule authorisedevice_rule1  ?r1<-
(ActualDeviceInfo(make ?mk )(model ?md)(serialNo
?sn)" + "(capturePurpose
?*apurpose1*)(LivenessDetection ?*ld2*))" +  "?r11<-
(…..))" +                    " => (modify ?r1
(authoriseDevice  \" Authentic Device \" )(…)))");
```

Similarly we defined rules for detection for authentic device, liveness detection status active or not active; to decide whether biometric sample can be accepted or not. In a backwards chaining system, rules are still IF…THEN statements, but the engine seeks steps to activate rules whose preconditions are not met. This behavior is often called "goal seeking". Jess supports both forward and backward chaining. In this paper we use back tracing for post-mortem of the intrusion which is used to find source of intrusion. We use Defquery construct for back tracing which displays detail knowledge about device status, make, model, serial number, userId, capture purpose, liveness detection, time stamp. The Defquery construct lets you create a special kind of rule with no right-hand-side. While rules act spontaneously, queries are used to search the knowledge base under direct program control. A rule is activated once for each matching set of facts, while a query gives you a java.util.Iterator of all the matches. It can be convenient to use queries as triggers for backward chaining. For this to be useful, Rete.run() must be called while the query is being evaluated, to allow the backward chaining to occur. Facts generated by rules fired during this run may appear as part of the query results [5]. We use Defquery as follows:

```
(defquery search-by-mess (declare(variables ?uid ?ct
?rmk)) (ActualDeviceInfo(userid ?uid)" +
"(…)(model ?md)(serialNo ?sno)(…)(captureTime
?ct)"+ "(capturePurpose ?cp)"+
"(…)(Remark ?rmk)))
```

Similarly we backtrack for fake device, authentic but inactive liveness detection for enrolment and verification process.

3. Result Screen

It exhibits five different tables which display information about device status at Enrolment, device status at Verification, list of device which failed in liveness detection at Enrolment, list of fake device and list of device which failed in liveness detection at Verification. It also displays different graphs which depict how many transactions are attempted through fake devices, devices where liveness detection fail and authentic device where liveness detection active. Figure 1 shows output of intelligent agent which displays on the screen two different list, containing message, UserId and Capture time and for enrolment and verification process. User can select any row from table and see the details which contain Capture purpose is Enrolment or verification, User ID, device make, device model device serial no, liveness detection status and capture time of capture sample. List of Liveness detection fails at authentic devices at enrolment process. Graph 1 which shows 22 attempts through fake devices, 33 attempts through authentic devices with Liveness Detection failed 38 attempts through authentic devices with active liveness detection at enrolment process. List which is at center shows list of fake devices at enrolment and verification process. Graph 2 which shows 15 attempts through fake devices, 39 attempts through authentic devices with Liveness Detection failed, 51 attempt through authentic devices with active liveness detection at verification process. List of authentic devices with Liveness detection fails at verification process.

4. Prevention Technique

We suggested few Prevention techniques that can be implemented using following policies with this intelligent agent to avoid biometric device intrusion at enrolment and verification process as follows:

- off_line and on_line system enrolment or verification should be in the presence of legitimate person. In both cases enrolment data entry screen should contain signature or any other identity of that legitimate person.
- Either hardware or software based Liveness detection is used for on-line and off-line systems. In both cases enrolment or verification data entry screen should contain check status that sample comes from device having any liveness detection technique, signature and any other identity of that legitimate person.

5. Conclusion

In this paper, a simple implementation of knowledge based Biometric Device Intrusion Detection assistant is portrayed. This intelligent agent is located on the Biometric Device. The intrusion detection is executed in background. When it detects suspicious or illegal activities, it notifies the security administrator. For detecting intrusive activities, IDS can use audit file data. In this paper we consider Distributed HOST-based IDS which are in charge of monitoring several biometric devices. It performs intrusion detection using Operating

System's audit trail, Device manger data or information from multiple monitored hosts. The system consists of a user interface module, an inference engine, a knowledgebase of certified biometric device, illegal transactions and audit trail of biometric device. Inference engine is implemented using JESS which is a Java Expert System Shell.

6. Future Work

In this paper we design and implement intelligent agent for biometric device intrusion detection. In future the research will expand to design other agents and preventive actions for detected intrusion using different AI techniques.

7. References

[1] T. Matsumoto, H. Matsumoto, K.Yamada, S. Hoshino, "Imact of Artificial 'Gummy' fingers on fingerprint systems", proceedings of SPIE , vol 4677, Jan 2002.

[2] Bori Toth "Biometrics Liveness Detection" Information security Bulletin, Oct 2005.

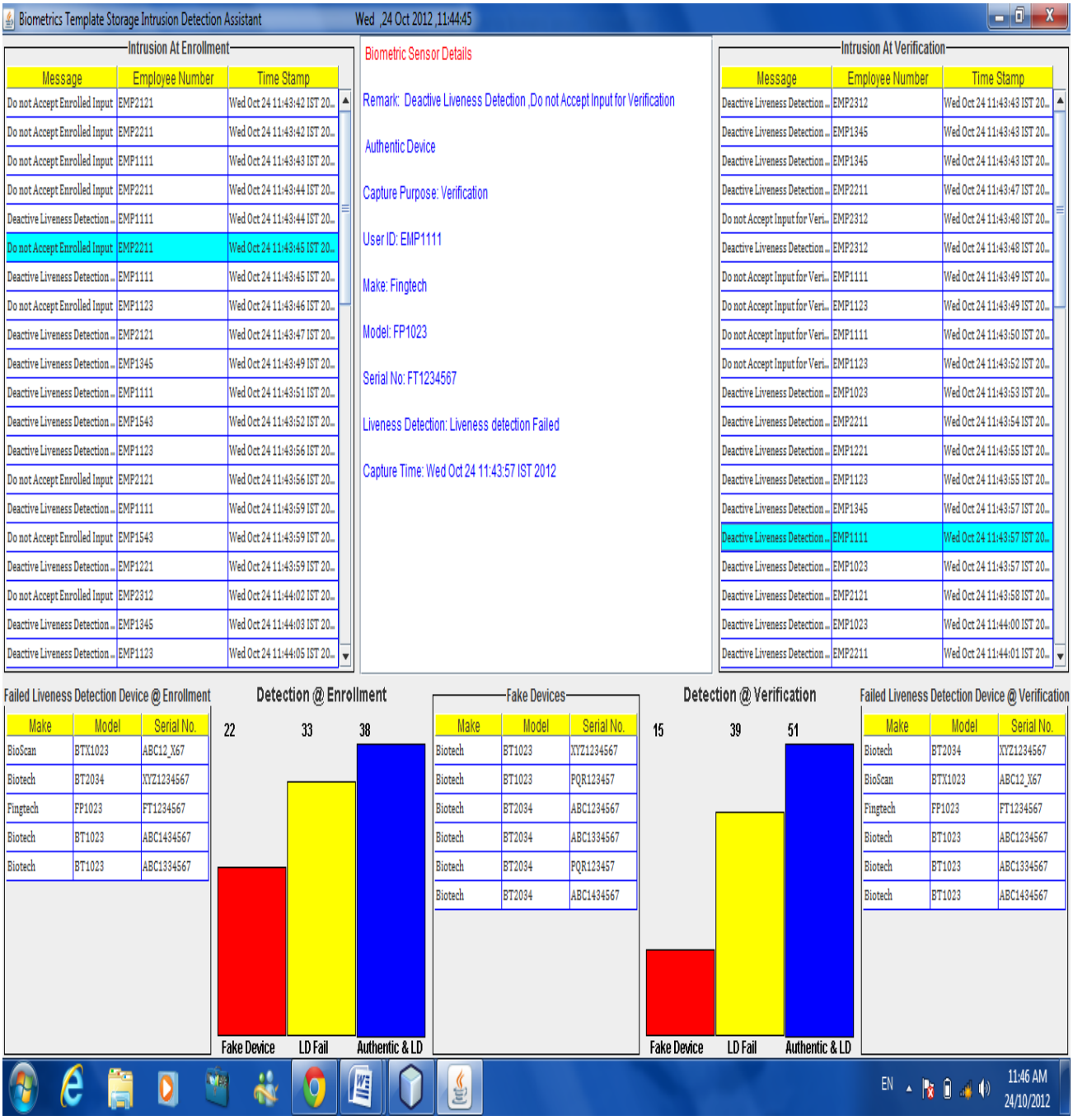
[3] Qinghan Xiao "Security Issues in Biometric Authentication" Proceedings of the 2005 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY

[4] Maithili Arjunwadkar and Dr. R.V. Kulkarni "The Intelligent Intrusion Detection Tool For Biometric Template Storage" published in Journal of Artificial Intelligence ISSN: 2229–3965 & E-ISSN: 2229–3973, Volume 3, Issue 1, 2012, pp.-42-48

[5] Ernest Friedman –Hill, "Jess, The Expert System Shell for the Java Platform" http://herzberg.ca.sandia.gov/jess

Maithili Arjunwadkar, MCA and pursuing Ph.D. from Symbiosis International University, India under Computer studies**.** She is working as assistant professor in PES's Modern College of Engineering, Pune-05 affiliated to University of Pune, Maharashtra, India.

Dr. R.V.Kulkarni, Ph.D. working as professor in Professor Chh. Shahu Institute of Business Education & Research, Kolhapur–416 004, ,Registered guide in Symbiosis International University, India. He is working as Computer Consultant. He has published many research papers.



(Fig 1: Output of intelligent agent)