A Novel Approach for Detection Insider Attacker Using Body Language

Mohammed Abdallazez Mohammed¹, Suhad Malallah Kadhem¹, Maisa'a Abid Ali K¹

¹Computer Science Department, University of Technology – Iraq.
mabdallazez4@gmail.com
110102@uotechnology.edu.iq

Abstract. One of most important challenges in cyber security is detecting the insider attacker (a person or an employee with an authorized access to resources and data of an organization then uses that access - either wittingly or unwittingly - to harm organization security). This paper propose approach to obtain early indicator to insider attacker before doing the crime. The previous security systems focus on the technical anomaly of an employee to discover the insider attacker and can’t discover it, if there isn’t technical anomaly. This paper attempt to discover insider attacker when there isn’t technical anomaly. Where presented body language-based approach to give earlier alarm of insider attacker. By using three of negative body language gestures (Cross Arms, Clasped Hands, Covering the Mouth) which referred to feeling of insecure, ready for an attack, doubt and a lack of self-confidence, these feelings are the closest to the feelings of the internal attacker. These gestures obtained by use skeleton features from video stream provided by Orbbec Astra Pro camera after passed to rule based classifier to recognize each one of the three body language gestures. Then determined the degree of trust based on the duration of the gesture and the number of occurrences of the same gesture or different gestures and depending on the degree of trust, the organization is alerted to the questionable employees. The test performs on ten of employees, four insider attackers were planted among them, and the results show 70% accuracy of detects the insiders, this approach will detect insider attacker before started his malicious work.

Keywords. insider attacker; body language, cross arms, clasped hands, covering the mouth, rule based classifier.

1. Introduction

The information system integrates not only a digital component (PC, Router, Server, etc.), but also a human component like the user that use the digital component. The question is: How can ensure the security of an information system while taking into account individuals as a component whose behavior may be malicious or careless. The threat is no longer so much outside of organizations, whose firewalls are effective and it no longer targets computers and digital artifacts, which have become more secure; the threat is human which is internal. The human component of the information system constitutes an insider threat to the system’s security. A threat that is found inside the organization itself, masters its processes, its firewall and its security policy, Whether they are intentional or accidental, malicious or
not [1]. The resource of insider threat is insider attacker “Personnel with an authorized access to resources and data of an organization”[2].

Will mention some examples of a real-life Insider attackers to prove the problem. Edward Lin (U.S. NAVY 2017) Found guilty of wrongly transporting classified material, failing to report foreign contact, mishandling classified information, and disclosing secret information to a foreign citizen. also shared technical or political classified information pertaining to the Navy’s Special Projects Squadron Two mission with a foreign government. Ivan Lopez( U.S Army 2014) Risk Indicators Depression, anxiety, sleep disturbances , Recent death of mother and grandfather , $14,000 debt, the crimes are death of three soldiers, who left behind wives and children , Fourteen other soldiers wounded, Lopez was a husband and father and Lessons learned from this case and several others has shaped DoD response to Insider Risk. John Beliveau (Naval Criminal Investigative Service, 2013) Beliveau provided Naval Criminal Investigative Service (NCIS) investigative reports to the subject of an investigation to assist the subject in the avoiding criminal charges, He deliberately leaked the names of cooperating witnesses, reports of witness interviews, and plans for future investigative activities. His actions were part of a larger corruption case involving hundreds of millions of dollars in Navy contracts. The Impacts NCIS investigations were compromised endangering Navy personnel and resources, including a case involving $7 million in fraudulent payments. Bryan Underwood(Former U.S. Marine working as a Cleared American Guard at the U.S. Consulate in China,2011): Underwood took over 30 photographs of sensitive areas and created a schematic that listed all security upgrades to the consulate and locations of surveillance cameras. The Impacts, Later review of the information gathered by Underwood revealed it contained information at the “Secret” level and The loss of Secret information is deemed to cause serious damage to national security. Yuan Li(Chinese National Research Chemist with New Jersey office of Global Pharmaceutical Company, 2012): Li uploaded the information on her personal home computer The stolen information was made available for sale through Abby Pharmatech, Inc. Abby Pharmatech, Inc. is the U.S. subsidiary of a Chinese chemical company Li was a 50% Partner in Abby Pharmatech, Inc. Impacts The company lost valuable research that impacted numerous projects Long held trade secrets were disclosed to competitors and the public Profits from current and future projects were compromised1.

One of most important challenges in cybersecurity is detect the Insider attacker but how detect the insider attacker, this is the more important question because in today’s technological era the boundary between friend and rival is growing fuzzier [2]. protected approaches should not only monitor host network activities by analyzing technical indicators , but also should identify elements of human behavior, motivation, and intent that may characterize malicious insider threats of employees [3].

Most methods of insider attacker detection focus on the technical behaviour (as log to email, using flash memory, etc.), which is a successful method if there is abnormality of this behaviour, either if the attacker did not occur any abnormality is very difficult discover insider attackers, therefore there is a need of another indicator to infer this attacker, this paper suggest the body language for this purpose.

The positive points that promotes the use of body language to detect an insider attacker as mentioned in[11]:

- Trying to adjust your body language without changing something inside is counterproductive. The nonverbal signals you send out are not controllable: Your body will always want to tell the truth about what you are feeling.

- Body language never lies. " What Is Happening on the Inside Is What You See on the Outside. Everybody speaks a body language

The idea of this paper is to detect the insider attacker intent through his body language and thus get an early warning before done the damage, thus even if there is no technical anomaly, it will be possible to identify the attacker before spying or stealing information.

1https://www.cdse.edu/resources/case-studies.html
1.1. Body Language

Body language is visual signals used in people's social intercourse which include movements, postures, and facial expressions that communicate emotions, attitudes and auxiliary information. Body language is postures and movements which can communicate emotions and intentions. Verbal language is mainly used to communicate information while body language is mainly used to communicate interpersonal attitudes [10]. A good knowledge of body language helps you to be more aware of what someone else is really feeling. Your body always wants to tell the truth about what you are feeling. Body language is a kind of stethoscope: It helps you to examine the possible causes of certain types of behavior from the outside. Our body instinctively shows on the outside what is happening on the inside, expressions and gestures tend to tell the truth before we can consciously adjust our behavior. This conscious adjustment is ten thousand times slower than the uncontrollable body language gesture. What people are experiencing internally will therefore be visible externally. Body language always compensates for the things that are said with words. The body language interpretations are accurate in 60 to 80 percent of situations, if they occur singly or in isolation. If you see a certain movement occur repeatedly, the likelihood is greater that the interpretation is correct. If within a short period of time you see a combination of three to five movements that all give a similar signal, you can draw your conclusion with a high degree of certainty [11].

Some negative body language will be used as indicator to insider attacker in this paper because it’s referred to feeling of insecure, ready for an attack, doubt and a lack of self-confidence.

**Crossed Arms.** In certain circumstances, crossed arms can indicate a negative or protective attitude or defensive position. You often see this in situations where someone does not feel comfortable or safe. Crossed arms as a standard position to indicate you are feeling threatened or insecure is something you see all around the world, the crossed arms shown in Fig. 1. [11],[10].

![Crossed arms gesture](image)

**Figure 1.** Crossed arms gesture[11].

**Clasped Hands.** In some situations, it is not possible or appropriate to cross your arms. When this happens, some people resort to secondary gestures and positions that carry the same meaning. One of these gestures is with the hands held low (or placed on a table) in a clasped position. This indicates a degree of nervousness, insecurity, and a need for protection. It is similar to the gestures frequently used by liars, clasped hands shown in Fig. 2.
Covering the Mouth. As shown in Fig. 3. Where some people hold a hand close to or in front of their mouths while they are speaking. Sometimes they add a little false cough, as a kind of justification for this movement. In extreme forms, people even push their lips together tightly. This is a protective gesture, designed to conceal doubt and a lack of self-trust from others. Paradoxically, by doing this they actually create a negative impression. What’s more, they require their conversation partner to work harder to listen, because in this position they speak less clearly and less distinctly. Of course, this makes it much more difficult for them to get their message across. A sudden movement of the hand toward the lips is often a first signal that someone is about to stop speaking. It is possible that the person is momentarily confused or has had a stress-induced blackout, so that she no longer knows what to say. Covering the lips with the hand in this way can also mean that the person has said something she did not intend to say[11].

1.2 Related Works
Many attempts to solve insider attacker problem, but all of them focus on abnormality behaviour and don’t consider the normality behaviour to discover the insider attackers. A comprehensive overview of anomaly detection provided by Hassan Takabi [4], present a novel approach for unintentional insider threat (UIT) detection and mitigation based on eye movement patterns. The results show about 82% accuracy on average for users wearing eye glasses and an average accuracy of 84.5% for users without eye glasses. The results demonstrate that users’ eye movement patterns and pupil behaviors can reveal valuable clues about their subjective mental workload and could be used in developing effective tools for unintentional insider threat detection and mitigation in real-world environments. Fanzhi Meng [5],
present a novel attribute classification insider threat detection method based on long short term memory recurrent neural networks (LSTM-RNNs). Experimental results validate that the proposed threat detection method greatly outperforms k-Nearest Neighbor, Isolation Forest, Support Vector Machine and Principal Component Analysis based threat detection methods. Fangfang Yuan [6], present a novel insider threat detection method with Deep Neural Network (DNN) based on user behavior. Specifically, the LSTM-CNN framework to find user’s anomalous behaviour. Xuebin Wang in [7], a new data-centric approach is presented to detect insider threat, which based on characterizing user behavior by extracting the features of user interaction behavior including keystroke dynamics and consecutive queries to model users’ access patterns. Statistical learning algorithms are trained and tested from opening dataset to predict abnormal behavior patterns. Wei Jiang in [8], present a user behavior analysis model, by aggregating user behavior in a period of time, comprehensively characterizing user attributes, and then detecting internal attacks. Firstly, the user behavior characteristics are extracted from the multi-domain features extracted from the audit log, and then the XGBoost algorithm is used to train. The experimental results on a user behavior dataset show that the XGBoost algorithm can be used to identify the insider threats. The value of F-measure is up to 99.96% which is better than SVM and random forest algorithm. Aaron Tuor [9], present an online unsupervised deep learning approach to detect anomalous network activity from system logs in real time. The models decompose anomaly scores into the contributions of individual user behavior features for increased interpretability to aid analysts reviewing potential cases of insider threat. Aaron Tuor depend on system logs in real time to discover the anomaly scores.

According to our deep investigations in the previous work, the literature review could not present a sophisticated system for detect the insider attacker before a technical anomaly. Therefore, finding a way to detect an internal attacker before the crime occurs will greatly reduce the losses of organizations. To achieve that, the proposed model will be able to give earlier indicator of insider attacker before doing the crime. Where, focused on detecting an attacker before a technical anomaly occurs using the attacker’s body language, in an attempt to minimize losses.

The paper format is structured as follows. In section 2, we illustrate the proposed model, we discuss the results in section 3. The conclusion is presented in the last section.

2. The proposed model

The proposed model consists of multi stages to use the body language as early warning of insider tracker as described in Fig. 4. The body language recognized based on the skeleton data provided by Orbbec Astra pro camera. These data contain features used to build rules, which are recognize the body language gestures.
2.1. Video Stream Description
The Astra pro camera used to read the video stream which contain the skeleton data, where it provides 19 joints shown in Fig 5. for each skeleton in each frame. Each joint has position and orientation. The skeleton data is joints coordinates which are x, y and z, where x the dimension on x axis, y the dimension on y axis and z the dimension on z axis which is represent the depth dimension.

2.2. Feature extraction
The feature that used to recognize body language gesture extracted from the joints data, where the feature that are related to the body and barely change with time are extracted as static features. One of the static features is the distance, distance between two points in three dimensions is given by equation (1)[12], When given two joints coordinates like a, b where \( a=(x_1,y_1,z_1), b=(x_0,y_0,z_0) \); the distance between the joint a and joint b is \( d \), where

\[
d = \sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2 + (z_1 - z_0)^2}
\] (1)

the equation (1) will be used to extract the distance feature for each body language gesture then build the rules to recognize the selected body language gestures.

For each body language gesture extract distance features, these features will be used by rule-based classifier to recognize the negative body language gestures, the distance features of each gesture with shorter abbreviated describes in table 1.

| Table 1. Distance features with shorter abbreviated. |
|----------------------------------------------------|
| The gesture                   | The feature | The shorter abbreviated |
|-------------------------------|-------------|------------------------|
| Cross Hand                    | distance between joint left elbow and joint left shoulder. | dle_ls                  |
|                               | distance between joint right elbow and joint right shoulder | dre_rs                  |
|                               | distance between joint right hand and joint left shoulder. | drh_ls                  |
|                               | distance between joint left hand and joint right shoulder. | dlh_rs                  |
| Clasped Hands                 | distance between joint right hand and joint left hand | drh_lh                  |
|                               | distance between joint left hand and joint left shoulder. | dlh_ls                  |
|                               | distance between joint right hand and joint right shoulder. | drh_rs                  |
| Covering Mouth                | distance between joint right hand and joint head for right hand | drh_h                   |
|                               | distance between joint left hand and joint head for left hand | dlh_h                   |

2.3. Algorithms
The first algorithm in Fig.6. is used to compute employee's trust degree, the second algorithm in Fig.7. is rule based classifier algorithm, it’s called by the first algorithm to check each frame if contain any of three body language gestures(Cross Arms, Clasped Hands, Covering the Mouth) or not. In algorithm1 When read video stream the parameters as shown in table 2.

After initialize the parameters, the algorithm implement while loop with condition employee is active and the threshold not reached, the next stage capture the frame from video stream then increment the total number of frames \( T_f \) by one, after that pass the frame to algorithm2 to check if the frame contain
If the frame contains one of the three body language gestures the \(B_f\) parameter will be incremented by one and compute the new trust degree by equation (2):

\[
TD = TD - \frac{(B_f/T_f) \times 100}{(2)}
\]

Table 2. Algorithm 1 Parameters.

| Algorithm           | Parameter | Description                      | Initial Value |
|---------------------|-----------|----------------------------------|---------------|
| Compute employee's  | \(T_f\)  | total number of frames           | 0             |
| degree              | \(B_f\)  | total number of frames which     | 0             |
|                     |           | contain body language gesture    |               |
| TD                  |           | trust degree                     | 100           |

Where decrement the amount \(\frac{(B_f/T_f) \times 100)}\) from trust degree, when employee consume more time in gesture or directly do another gesture the trust degree continue with decrement until TD=threshold will be launch the alarm. If the frame don’t contain any body language gesture the trust degree will incremented by equation (3) until reach the initial value.

\[
TD = TD + \frac{(B_f/T_f) \times 100}{(3)}
\]

Algorithm 1: Compute employee's trust degree

**Input:** video stream

**Output:** Trust degree (TD)

**Process:**

- initialization variables
  
  \(TD=100, \ T_f=0, \ B_f=0\)

- While (TD> threshold and employee is on) do // employee is on means he/she is sitting in his particular place
  
  - Capture the frame (F)
  
  - \(T_f=T_f+1\)

  - Call algorithm2 // that take (F) and return (Check of Body Language Gesture)

  - if Check is true then // this mean it is a body language gesture
    
    - \(B_f=B_f+1\)

    - \(TD= TD - \frac{(B_f/T_f) \times 100)}\) //decrease the TD when employee body language gesture give a negative signal

  - Else if (\(B_f>0\) and TD<100) then
    
    - \(B_f=B_f-1\)

    - \(TD= TD + \frac{(B_f/T_f) \times 100)}\) // increase TD when employee body language gesture don’t give a negative signal

- End While //end the while loop

- If (TD<= threshold) then
  
  - Launch the alarm // launch alarm when TD less or equal the threshold

- Step 3: return (TD)

End Algorithm 1.

Figure 6. Compute employee's trust degree algorithm.

The rule based classifier algorithm is called by the compute employee's trust degree algorithm where it takes a set of values of the distance feature then it check if there is a gesture or not.
Algorithm2: Rule Based Classifier

Input: set of distances features.
Output: body language gesture.

begin
if ( |dle_ls - drh_ls |<= thrashold1) && (|dre_rs - dlh_rs |<= thrashold1) then return “the gesture is cross hand”; 
else if (drh_lh<= thrashold2)&&( dlh_ls> dle_ls) &&( drh_rs> dre_rs)then return “the gesture is clasp hand”; 
else if (drh_h<thrashold3)||( dlh_h<thrashold3) then return “the gesture is covering mouth”; 
end if;
End Algorithm2.

Figure 7. Rule based classifier algorithm.

The distance features will be passed to the rule-based classifier to discover each frame if it contains one of the body language gesture.

Rules Description. After extracted features the rules built for each body language gesture in algorithm2, describe as shown in table 3.

Table 3. Rules description.

| Gesture  | Rule                                                                 | description                                                                 |
|----------|----------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Cross    | if ( |dle_ls - drh_ls |<= thrashold) && (|dre_rs - dlh_rs |<= thrashold) then return cross hand; | The difference between dle_ls and drh_ls and the difference between dre_rs and dlh_rs must be smaller than the predefined threshold selected depend on trial on ten of employees, where measured these two distances of ten employees with different sizes and clothes then taken the range. |
| Hand     |                                                                      |                                                                             |
| Clasped  | if (drh_lh<= thrashold2) &&( dlh_ls> dle_ls) &&( drh_rs> dre_rs) then return clasp hand; | The rule of clasped hand is the drh_lh must be less than specific threshold and dlh_ls and drh_rs larger than another threshold, the thresholds selected depend on trial on ten of employees. |
| Hands    |                                                                      |                                                                             |
| Covering | if (drh_h<thrashold3)||( dlh_h<thrashold3) then return covering mouth; | drh_h must less than threshold for covering mouth with right hand and dlh_h must less than same threshold for covering mouth with left hand, the threshold selected in the same way of above thresholds. |
3. Results
Experiments were conducted on ten employees, where four of them (insider attackers), the results demonstrated competence in distinguishing the body language gestures that shown in Fig. 7.

![Figure 7. The body language gestures.](image)

Where (a) cross arms gesture, (b) clasped hands gesture, (c) covering mouth by right hand and (d) covering mouth by left hand. Also the degree of trust had calculated to the employees according to the time consumed with gesture and the number of gestures, as shown in Table 4.

| Employees | Cross Hand | Clasped Hands | Covering Mouth | Total gestures time | Trust degree | Actual class | Launch alarm |
|-----------|------------|---------------|----------------|---------------------|--------------|--------------|--------------|
| 1         | x          | x             | x              | 0s                  | 100%         | Not insider  | no           |
| 2         | x          | x             | ✓              | 10s                 | 94%          | Not insider  | no           |
| 3         | x          | ✓             | x              | 23s                 | 90%          | Not insider  | no           |
| 4         | x          | x             | x              | 0s                  | 100%         | Insider      | no           |
| 5         | ✓          | ✓             | x              | 130s                | 66%          | Insider      | no           |
| 6         | ✓          | ✓             | x              | 67s                 | 85%          | Not insider  | no           |
| 7         | ✓          | ✓             | ✓              | 192s                | 46%          | Insider      | yes          |
| 8         | ✓          | ✓             | ✓              | 90s                 | 78%          | Not insider  | no           |
| 9         | ✓          | ✓             | ✓              | 200s                | 43%          | Not insider  | yes          |
In this paper, the interpretation of the body language was adopted based on two important factors: the duration of gesture, the frequency of the gesture itself, or other gesture having the same meaning. The degree of trust affected by these two factors, where same gesture sometimes has a great impact on the degree of trust and sometimes slight. As example when one employee do the gesture for half minute the trust degree of this employee will greater than other do it for ten second, also the same when do more than one gesture with same meaning. The results in table1 affected by the duration the employee consume in gesture and how many gestures the employee do, this two factor demonstrate why employee five and employee six with deferent trust degree although the two employee do the same gestures Clasped Hand and Cross Hand. The confused matrix of the results is shown in table 5.

| Total instances=10 | Actual insider | Actual not insider |
|-------------------|----------------|--------------------|
| Predicate insider | 2              | 1                  |
| Predicate not     | 2              | 5                  |

True Positives (TP)=2, True Negatives (TN)=5, False Positives (FP)=1, False Negatives (FN)=2.
The Accuracy = ((TP+TN)/total)*100 = ((2+5)/10)*100= (7/10)*100= 70%.
Misclassification Rate= ((FP+FN)/total)*100 = ((1+2)/10)*100= (3/10)*100= 30%.

These results show that body language reveals an insider attacker, when he intends to do a job that harms the organization, In the status that the insider attacker does not appear on it the specific gestures, it cannot be detected as in the employee 4. While the fifth employee had two posts and his degree of trust was 66, which did not exceed the limit, So the system did not launch an alarm.

Employees 1, 2, 3, 6, 8 and 9 were trustworthy so they did not launch the alarm. The Employees 10, 7 were not so trustworthy for them so the alarm was triggered.

The threshold used in the results above is 50%, where if the degree of confidence is less than 50, the alarm will be triggered Otherwise not. It is possible to control the acceptable threshold of confidence according to the vision of the top management of the organization and according to the sensitivity of the information that the employees deal with, their health and psychological conditions and the environmental factors in the workplace. Therefore, these results can change according to the threshold.

4. Conclusion
The insider attacker is a great risk, So it's better to use the method to detect insider before started his malicious work, the most of the ways to detect the insider depends on the technical anomalies that occur during the commission of the offense and therefore will have achieved its goal or part of it, this paper gives method to obtain an early indication of the attacker before the initiation of malicious work through the language of his body and because the language of the body never lie and has no ability to control, it was used to detect the insider attacker, where the body language of insider attacker tells us about what hiding in his mind, this facts used in this paper to provide earlier alarm before the insider do the crime.

The tests were carried out on ten employees, including four insider attackers. In the beginning, the degree of trust is complete for all. The degree of trust changes according to the reading of the body language of the employee.
Interpretation of body language depends on the duration of the gesture and repetition it or repetition of other gestures with the same meaning. Where the Orbbec Astra camera was used to read the video then calculate the coordinates of the skeleton joints and extract the distance feature between some joints to distinguish the gesture of body language using a rule-based classifier. The results showed that the accuracy of reading body language and calculating the degree of trust was 70%, so this paper gave method to early warning of the insider attackers.

References
[1] Pierre-Emmanuel Arduin, “Insider Threats”, Volume 10, © ISTE Ltd 2018.
[2] Mehul S. Raval, Ratnik Gandhi and Sanjay Chaudhary, “Insider Threat Detection: Machine Learning Way”, © Springer Nature Switzerland AG 2018.
[3] Frank L. Greitzer, “SOFIT: Sociotechnical and Organizational Factors for Insider Threat”, IEEE Symposium on Security and Privacy Workshops 2018.
[4] Hassan Takabi, “Prediction of Human Error Using Eye Movements Patterns for Unintentional Insider Threat Detection”, IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA) 2018.
[5] Fanzhi Meng, Fang Lou and Yunsheng Fu, “Deep Learning based Attribute Classification Insider Threat Detection for Data Security”, IEEE Third International Conference on Data Science in Cyberspace 2018.
[6] Yanan Cao, “Insider Threat Detection with Deep Neural Network ” International Conference on Computational Science 2018.
[7] Xuebin Wang, “Insider Threat Detection Using Characterizing User Behavior”, IEEE Third International Conference on Data Science in Cyberspace 2018.
[8] Wei Jiang, “An Insider Threat Detection Method Based on User Behavior Analysis”, © IFIP International Federation for Information Processing 2018.
[9] Aaron Tuor, “Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams”, Association for the Advancement of Artificial Intelligence 2017.
[10] Jianxue Yin, “Body Language Classification and Communicative Context”, International Conference on Education, Language, Art and Intercultural Communication (ICELAIC) 2014.
[11] Kasia Wezowski and Patryk Wezowski, “Without Saying a Word”, Kasia Wezowski and Patryk Wezowski 2018.
[12] Jiande Sun, “View-invariant gait recognition based on kinect skeleton feature”, Springer Science+Business Media, LLC, part of Springer Nature 2018.