

**School of Science and technology**

**CSD3999**

**Computer Science Project**



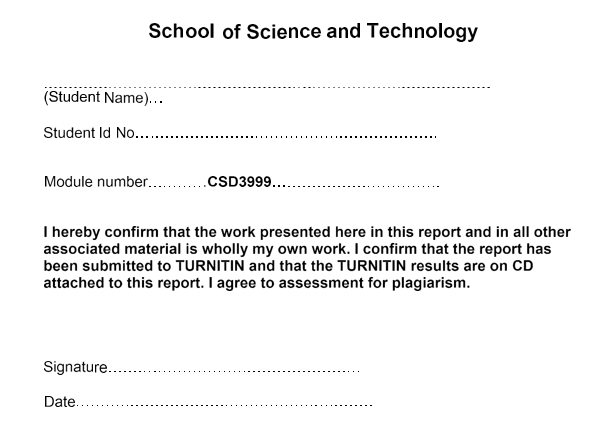
**Date:**

**Supervisor: Dr Florian Kammueller**

**Student Name: Kaiton Michael Kumar**

**Student ID Number: M00576529**

**Title: Security and Privacy – Insider Threats**



**Abstract.** Insider threats, 56% of regular employees pose the largest security risk to their own organization. The research in this paper is based on Middlesex University, the development of security features to deter insider threats on a certain room. These developments if successful can be carried out throughout the university, the recommended developments can be applied to module labs and are designed around cost and educational characteristics. Inheriting Insider threats into Middlesex University helps provide a personal take on the subject. Looking into student and staff threats throughout the report, It is factored how introducing it educationally could increase the risk overall. Furthermore touching on alternative solutions to gather an insight on the subject and whether solutions can solve the security hazards outright.

Table of Contents

[Acknowledgement 4](#_Toc7192578)

[1 Introduction 5](#_Toc7192579)

[2 Literature Review 6](#_Toc7192580)

[3 Methodology 7](#_Toc7192581)

[**3.1** **Room security** 7](#_Toc7192582)

[**3.2** **Security Implementation, method 1** 8](#_Toc7192583)

[**3.3** **Grouping and identifying the threat** 11](#_Toc7192584)

[**3.4** **Method 2** 13](#_Toc7192585)

[**3.5** **Method 3, room for improvement** 14](#_Toc7192586)

[4 Discussing the solution 14](#_Toc7192587)

[5 References 16](#_Toc7192588)

# Acknowledgement

Had I not been encouraged from working alongside Dr Florian Kammueller in my second academic year at Middlesex University, I may not have reached out in my third year for him to be my supervisor. I have learnt that he truly enjoys and understands the importance of research/ investigative writing and shares this strong feat with myself. I do not think I would have gained the confidence in pursuing such thorough research, had I not been fortunate enough to be accepted by Dr Florian who can so closely relate to my own research, and with unlimited knowledge at hand I can state that this should be a very interesting read. Furthermore it is a given that I thank my Family, Peers and facilities my institution has provided. As without these I could not have gotten to this stage, quite literally I may add. I am grateful for the continuous support provided by my family and peers with a strong attitude towards my work as well as their own, giving valuable feedback contributing greatly towards my efforts.

# 1 Introduction

Security and privacy are imperative to everyday life, a simple definition of privacy is to not want to be observed or disturbed by other people, and to an extent security comes hand in hand with privacy. You can’t always have privacy no matter how secure you make yourself when walking around in public, however in social establishments, Academic institutions and work places. Security and Privacy are critical to maintaining safety and invulnerability as far as possibly acquirable to keep students, staff, workers, buildings, corporate infrastructures intact, the list expands globally. A rather delicate example of this is cloud based storage and its vulnerability to breaches, unfortunately I will be using Verizon as an example here. Leading me on to the grand topic of this paper, **Insider Threats**. Verizon the largest wireless telecommunication service in the United States, while not entirely at fault had a data breach in their cloud service. However not by any malicious means, this was done by a third party vendor who worked for Verizon, accidentally. Taking this into account it sounds harsh to label them as an insider threat, but it is not a title to shame or incriminate all who commit it. It simply means the threat and incident was done from an employee, former employee, contractor or work associate from inside the organization. An engineer who worked for the third party vendor in this short largescale example decided to back up user information such as Emails, phone numbers and pins in a cloud based file that was not secured by Verizon, allowing access to all information. In this case it was unintentional, many similar attacks as innocent as they may seem, are more often than not malicious **Insider Threats** and may be attempts to sabotage a business.

In short, I will be investigating potential threats and security risks to Middlesex University from Inside attacks. There are already several measures in place to prevent basic intrusions and possible attack scenarios. Nonetheless by using this research I will produce simple security prototypes that could be expanded upon further to achieve a higher standard of defence against Insider attacks.

I will produce some existing models of areas in which I think may be vulnerable to Insider attacks, analyse the security measure they have already implemented and what can be changed to keep them more secure. I am going to develop a methodology to understand some of the models I create. Furthermore to conclude I will emphasise on why these methods are more plausible for defending against insider threats.

# 2 Literature Review

[Attack tree analysis for insider threats on the iot using isabelle](https://link.springer.com/chapter/10.1007/978-3-319-39381-0_21); see [1] examines company’s staff technology e.g. smart watches etc. -As an example of the ever growing number of IoT devices, this paper explains in detail possible strategies used to attack employers and workspaces. For example it is mentioned that storage spaces on mobile devices transferring valuable data/ information. Using NFC Bluetooth to connect to devices and transfer etc. Another example is paired or existing connections between devices that were associated with the company and company devices. I will be taking in to account that possible devices such as ID cards can also be used, stolen or if possible copied, this would be the easiest way to conceive an insider threat.

Aspects of insider threats is a paper [2] that gives a good incite and introduction on what insider threats actually are, this gives me a broader sense of what to focus on when it comes to cyber security versus physical security on insider threats. I will be introducing a simple approach to Insider threats to expand upon. Further to this I will examine risk assessments and how to approach an “insider threat” [3] When getting to the solution of my project, I will need to look at the wide range of aspects that come with it, for example in this paper we explore the financial burdens brought upon securing and protecting against insider threats. Then on top of that, dealing with the financial impact of a successful insider threat attack and the losses incurred by such.

[4] [Towards an access-control framework for countering insider threats](https://link.springer.com/chapter/10.1007/978-1-4419-7133-3_8). This further discusses creative solutions to protecting and battling insider threats. This discusses access control for example workers forgetting to carry out back up procedures etc. This gives an idea to problems and solutions that could be solved within workplaces that are easily solved. However rather than solving problems, we can stop them before they start by catching the insider threat using HoneyPot sites [5]. Another discussion on the possibility of catching insider threats and how to do so. These kind of solutions will come in handy to implement in my project as the test have proven that they are successful in doing so. Honeypot sites can help gather and develop information on where and how these threats manifest and take place. One of the more appropriate study I will conduct  [is; insider attack detection research](https://link.springer.com/chapter/10.1007/978-0-387-77322-3_5) [6]. I will study a wide range of detection methods in order to stop and recover from insider attacks. This carries out test and gives examples on how to possibly avoid malicious intent by insider threats. More importantly I would like to invest some time understanding detection methods and the use of them when it comes to security. This is essential to a solution I may expand upon further in this paper, using their tests I can determine what would be the best method to be applied to my own produce.

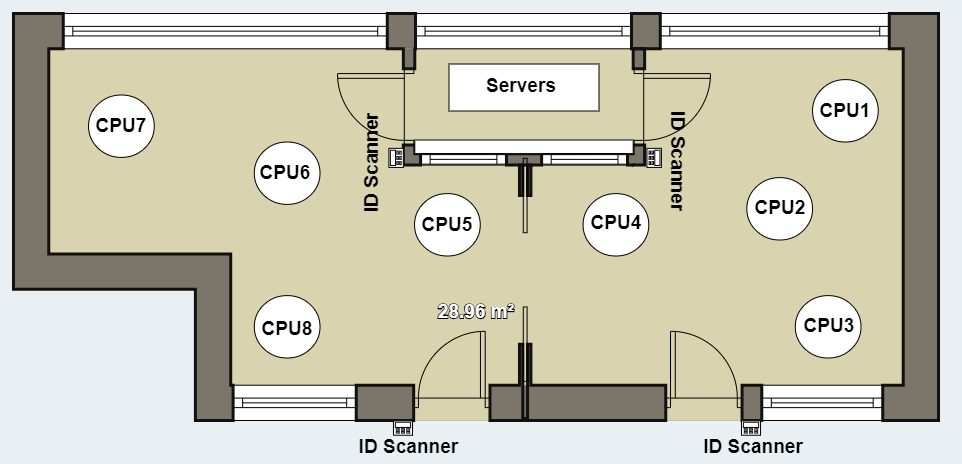
# 3 Methodology

As we approach the solutions I will provide, I would like to give a deep evaluation of what I am actually going to produce. Allowing to ensure that everything corresponds, I will give a background, an architecture/ layout design for the product and implementation plans. Of course subsequently a conclusion to said product and possibilities for expansions to further any prototypes.

In commencement I would like to provide a scenario offering weaknesses that I have examined within Middlesex University, not exactly weaknesses per say, but some simplistic feats that may need a drastic upgrade. In this rundown it will focus on a room that meets criteria for both conditions I will address.

### **3.1 Room security**

The room I am focusing on is a networking room, with several servers, computers, network cabling, varying peripherals and importantly an interior room with a main server setup for staff access only. Further in to the research I will expand on why the room is valuable for the investigation, in essence I will discuss what method I have devised for Initially accessing the room and then using or even tampering with equipment. I will also discuss what possible reasons there are to implement these developments other than security of course. To proceed I am going to analyse the floor plan, or room structure shown in figure 1. I contacted a tutor who helped develop the room, in chance that they may provide me with floor plans and information detailing the room. Most importantly the floor plan is to be used to discuss and narrate the coming methods.



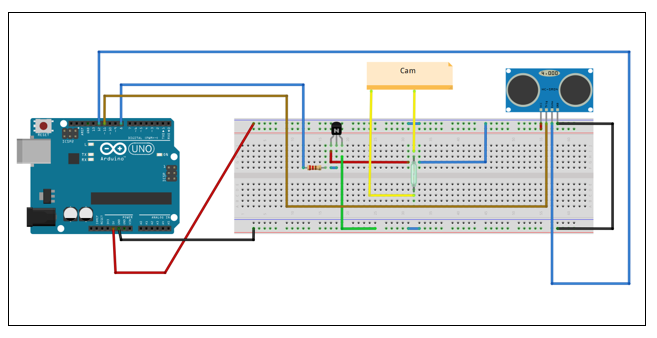
**Figure1.** Floor plan of the analysed room

Shown in figure 1, there are several ID scan locations, the two main doors are accessible for specified students with identification cards. The Inner room is staff only. I created this floor plan attaining high detail regarding the actual room. However it is still deemed rough as it is not the original plan, of which I cannot obtain due to security reasons. I documented several pictures and notes in order to provide a floor plan as accurate to the original room as possible. The main attention to detail are the played around the ID scanners, server and computer islands. The floor plan above will be referred to several times in aid of acknowledging the methods as detailed in the methodology.

Continuing, this room features several computing equipment. Security risks and insider threats immediate once someone has access to the inside and its components. I have devised such security measures to examine whether a user should be allowed inside that room, and specifically on the devices provided for students.

### **3.2 Security Implementation, Method 1**

For my first implementation to this project, featuring the main room only, I have devised a security feature that could be very effective. Keeping in mind this is just a prototype, however it can be created and expanded upon within the university itself given we can utilise on the supplies we have in our Computer Science department. Simply, I will map out the plans before discussing further; I will be taking an Arduino UNO, LDR (Light dependent Resistor), if needed for further development, a Sonar Sensor HC – SR04 and for testing purposes any type of camera seeing that it can be wired onto my relay so it can receive feedback from the sensor or resistor. Shown in figure 2 you can see the layout for a prototype I developed.



**Figure 2.** Using Fritzing I devised a simple prototype of how we could create these security systems in our university.

Before I digress, I would like to note, the only security for the room is an ID authentication device, where a student or staff can tap his/hers Identification card on the device and the door will unlock. Further to this the computers have assigned users with specific login credentials, however that is all. I plan to add more security by implementing this easily built system which can be developed upon majorly. This is only the first step, as shown in figure 2, this is a sensor which upon activation will trigger the camera to take snapshots. This compact system will be placed inside or on a monitor, where the camera will have view of the user situated at the machine. Provided that the camera has memory, the HC – SR04 sensor uses non-contact functions up to 400cm. The wire connectivity is as follows; **5V Supply, Trigger pulse input, Echo Pulse Output, and 0V grounding**. Simply the module uses high level signals and given that it receives a pulse signal back it will activate the camera.

Importantly this system is very cheap, furthermore the university can integrate this into modules in lab work, wiring, and working with Arduino UNO and breadboards. This is an easy way to drive user knowledge of this research and teach concurrently as well as save money. All together the system costs £50 – 60 depending on the quality and storage size for camera module and would be less when supplied by the university.

Now it is understood what the system is intended to be used for, I can clarify the outlying piece to complete the product. It’s all well that it can take pictures of users and save it, it is possible to analyse this information and determine by time whether or not a user should be in the room. However that doesn’t clarify if the user is allowed or validated for entry in that room. I have devised a method that goes hand in hand with this system, simply put; **Facial Matching.** As shown in Figure 3. I have produced a facial recognition/ matching system using two files, primarily a folder for faces captured by the motion detecting camera, imported from saved data, and another folder containing the database of users that should be allowed entry to the specified room via picture and ID number. This facial matching system can run a picture of face and match it against all other faces in the database folder. However this being a prototype, I have not yet been given the database of faces and ID numbers to test it on, so of course I will use examples of stock images. So taking a look at Figure 3.



**Figure 3** Using MATLAB and the eigenface algorithm [7] I made an interface that runs an image of a face and runs it against the database.

This simple application on MATLAB was created using the Eigenface algorithm, seeing as faces share similar patterns, this algorithm classifies and separates faces based on general patterns shown in conversion of a *vector X length N (N=imagewidth\*imageheight)*. [7] This is most useful when we have multiple images of a face for one person, however I know the university does not have several images of one users face.

Now given a scenario to justify how these systems work in unison, If someone loses their Identification Card and any unauthorized personnel picks it up, or in some case an authorized user allows access to the room for an outsider. When they attempt to use the computers or loiter around the machines, the system will be able to capture and register their face for reviewing. If we get an Image of the face, we simply place the image into the review folder and match it against the database. If there is not a match then it is clear they should not be in the room. This is a simple solution that is cheap and can be incorporated into lab modules and taught for security purposes.

Some alternative methods that I can apply to this research are; camera recording rather than taking pictures, however I will have to cut and render images of faces from this. This could instead increase the chance of getting an image of the users face. Using the LDR sensor, rather than the sonar sensor. The price difference is not much, however the installation is much more compact and it is easier to programme since it is light based only. The problem is that it may not get accurate feedback and can be harder to rely on if the user is very still. Finally connecting the folder and the saved data from the camera to automatically upload the images to our database. This would save time, but is not relevant to prove the use of this prototype in this case.

This being the more complex method to this research in order to provide security to the room, I will provide findings later in this paper. However facial recognition is globally recognised as one of the greatest security procedures, provided **Apple** predicts facial recognition is so accurate the chance in someone else unlocking their phone is 1 in one million. Airports can tell just by matching faces whether someone has overstayed a visa, colleges in the US now use facial recognition to tell whether or not students cut class. Something we could take note of, however a simple registration form seems to work good enough. Overall this data provided by Norton is extensive and provides enough evidence to back up my case [8].

### **3.3 Grouping and identifying the threat**

Now that I have distinguished security protocols to defend against an insider threat of moderate level, I will acknowledge why it would occur in the first place. Simply broken down there are several reasons someone would become an insider threat or cater to one. We can user simple or higher logic to explain these developments. To visually represent insider threats in logic we can look at both Psychological and motivational reasoning [9]. This method would involve creating datatypes to be put into data sets and depending on values, definitions and mutations I can devise correspondence models [9]. In essence a simplistic feature of this visual representation is to show;

**Datatype Behavioural = psychological states**

**Datatype Motivations = Motivational states**

The two main traits as shown above to be provided for such representation are Behavioural and Motivational. To create data sets we can define such behaviours or motivations, for example and Insider threat could usually be motivated by making money, carelessness, or do not even realise risks they may bring to the situation. Behaviour traits could stem from particular scenarios, or could already exists within the staff. An easy example to follow in this case before developing on the visual correspondence, is students being given a low mark, failing modules or not passing their dissertation.

So in this case, we give values for students;

**Student Behavioural = happy | stressed | angry | depressed**

**Student Motivations = revenge | fun | recognition**

Now that I have set some constructors, to develop this I will use types to build sets, as there may not be a single motivation or behavioural trait. An insider threat may have several reasons for their actions e.g., **motivations\_Student {revenge, fun}** I can now use these as quantities if I further want to discuss higher logic. However to directly exhibit the traits and reasoning we can just use a simple set, and provide higher logic when necessary to investigate statistics and extract data. This pours into the larger scale, dealing with datatypes such as physical location, logical locations etc. to deal with this in more common terms we can for now create tables of logistics rather than using higher logic [9].

Moving on to the second methodology, staff insider threats. Still applying the knowledge to this room, however as talked about earlier, It will be focusing on the interior room, only accessible by staff. Staff still prove a threat to the main room as in tampering, stealing components in that part of the room, the interior room is only accessible by the staff Identification card, as explained earlier. Thus the reason for focusing on this room in particular.

Staff will be of the greater priority when it comes to monitoring insider threats, using the logistics seen earlier. It would be easy to monitor suspicious behaviour [2], for example,

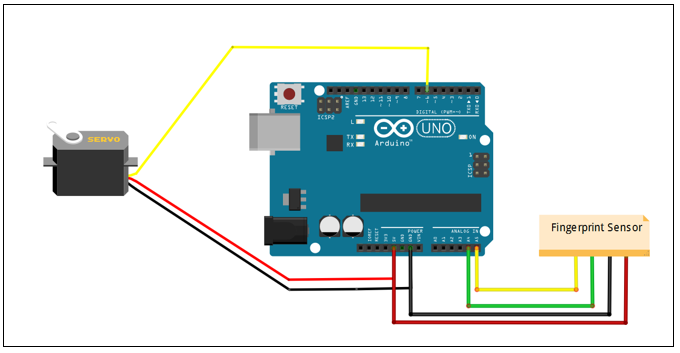
|  |  |  |
| --- | --- | --- |
| **Behaviour** | **Malicious** | **Unintentional** |
| Uncoordinated clock in times | x |  |
| Uncoordinated room access | x |  |
| Unusual login location | x | x |
| Copying Large amounts of data | x |  |
| Accessing new applications | x | x |

**Figure 4** Dataset of common suspicious behaviours linked to insider threats [4]

Given that a system was developed for student behaviour and tracing student identification using facial matching, I comprised a safer suggestion for accessing staff only rooms. Considering anyone can get hold of a staff identification card including other staff, it would only take the misplacement or losing of one to become a security risk.

### **3.4 Method 2**

The interior room discussed that is only accessible by staff is only secure to a certain extent, of course the identification card can be revoked as soon as possible to prevent such occurrences. However a method devised and commonly practiced within corporations can overwrite such problems all together, fingerprint scanning. Shown in figure 5, I devised a basic cheap and resourceful security function. Comprised of university provided equipment, this should already be implemented and taught in lab modules as urged with the previous method. This simple unit was curated by an Arduino UNO, Servo unit and fingerprint sensor module.

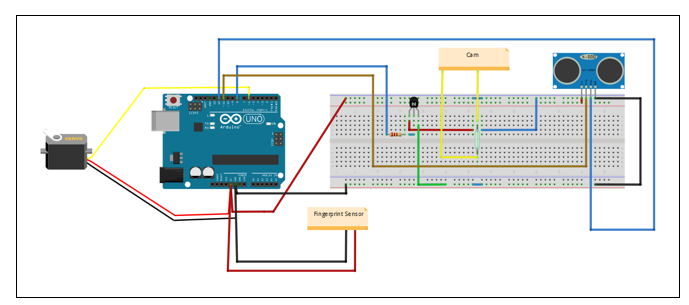


**Figure 5** Basic fingerprint Arduino UNO system using servo unit to operate locks

This basic system as discussed previously stores user fingerprints using the Arduino IDE file preference such as trusted or enrol, each fingerprint is simply attained and correlate the fingerprint with a number. Using serial outputs you can follow steps to set it up easily, this may seem very elementary, however this is a lot more secure even as a main security function, with identification card authentication as a backup feature. Even with the in-complexity towards this level of research the aim is to implement availability to introduction for lab modules, the fact that it could be studied and created by students does not affect the level of security it provides and proves as an educational influence in the field. Let alone further proving it is a cheaper alternative to changing every identification card reader to this system. It provides security solely for rooms that should be accessed by staff, the overall cost of the system is £30 - £40 depending on quality and capacity of sensor used, plus servo module size and functionality.

### **3.5 Method 3, room for improvement**

Room for improvements consist of; small led monitor display to show errors and warnings for incorrect inputs, small alarm for warning or to serve as notice that the fingerprint is recognised, finally it can be merged with the preceding system to create a more advanced system as shown in Figure 6.

**Figure 6** This is the merged systems, providing this is still a prototype, there may be room for errors.

This is a merged system, as explained in the two previous methods. The functionality remains the same however this would be classified as an advanced security system, able to match the faces of staff entering the room against the database file for staff granted access. Whilst also taking and scanning fingerprints to acknowledge and allow initial access to the room.

# 4 Discussing the solution

All systems shown previously would need a power supply, but for testing purposes can be hooked up to computer systems for faster results. A power supply would work fine for testing away from systems. Official integration would stray away from the subject. Briefly, to test prototypes we only need parts to work, or a functioning prototype that is not yet inbuilt. As mentioned before systems are tested on the computers, applications tested separately and systems built on applications such as Fritzing and tested for feedback. To get these results for prototypes we look for application functionality, preciseness of facial matching as detailed on figure 3 and compatibility with systems built in security methods.

To further discuss, an important sub investigation to take into consideration and mentioned several times in the previous methods. Is the possibility of teaching computational security as a module in university, labs are already in use for developing wiring, and simple module functionality. However this is a basic fundamental module for first year students to learn how to interact with hardware. In turn it could serve as a great learning experience in countering Insider threats and developing knowledge of security at the same time. The possibility of a computational security module would tie together with my methodology, considering the use of MATLAB programming, preferably machine learning combined with hardware interaction to develop security tools and the practicality of having access to the equipment first hand provided by the university. It is an untouched area of expertise that can easily take the place of hardware labs with no extensive educational value but helping students learn how CPUs connect through wiring. A further point to be clarified is that by no means does implementing a computational security module act as a solution to insider threats, as it could produce new ones in itself. Allowing students to learn about insider threats and develop knowledge of security can allow them to develop the fundamentals to become greater insider threats. Not to deter the option of creating the module. It is always a factor to consider, as the same for teaching robotics when we look for those to blame for robots taking over the world. But to digress, without the teaching of insider threats and security there would not be protection against it, so it is still necessary and very worthy of consideration.

The development of this report was to discuss insider threats, the possibilities of insider threats to Middlesex University, solutions and reasoning for the solutions factoring in price, improvements and of course possibility of educational implementation. The insight to what can be developed and the extent to which development could be carried out is endless. I previewed a brief merging of two methods, a very simple integration that shows a very simple security method and a more complex method unify so basically. Foremost it is not so much how the unification can take place, it is the compatibility of security and its surroundings. Such that you cannot have point security to protect people from falling into railway station tracks, even though it clearly states “Mind the Gap” it does not prevent the event from occurring. More so, a do not enter sign does not stop one from entering. This is a simple deviation yet can be applied in several aspects of insider threats and security, when staff choose to target their employed corporation with malicious intent or accidental security breach. The simplest scenario being a room they are not supposed to enter or equipment they are not supposed to tamper with, a common behavioural habit is curiosity.

Moving on to a basic discussion on alternative solutions, there are methods already set in place that may not be developed upon or that are not as secure as they may seem. However they are still methods used by corporations on a daily basis in order to deter such events from happening. [4]

Detection and Mitigation address insider threats in the most logical way, using methods such as forensics to sniff out discrepancies, as stated when detailing higher logic. The ability to detect motive and malicious intent is very basic and cannot really be applied. Reason being a company would not attempt to press false accusations/ suspicions upon an employee. This is why the first factoring solution would be **monitoring**, while judging legalities and ethical reasoning for monitoring employees. Monitoring would incur the use of cameras, clock in and clock out times, as well as login and log out times.

Another moderate solution is corporate **policies** including policy hierarchy, these policies are based on legal regulation, ability to meet business requirements, and security requirements [4]. Policies generally depict behaviour, depending on dynamicity, staff will tend to look at possibility of obscuring or figuring out flexibility in the policies.

To clarify, solutions never really solve the problem, of course to an extent, or to amount to what is intended. Knowing this creating solutions even to the extent of merging my own two methods still could face difficulties and unpredicted scenarios. The solutions could be dismantled quicker than when they were developed. Chiefly we cannot rely on our solutions to protect us from harmful scenarios, no matter the quantity of solutions implemented, there will always be loopholes or unpredictable circumstances to be met. We dictate what the best solutions are, by self-assessment.

# 5 References

[1] [Attack tree analysis for insider threats on the iot using Isabelle](https://link.springer.com/chapter/10.1007/978-3-319-39381-0_21)

Kammüller, F., Nurse, J.R. and Probst, C.W., 2016, July. Attack tree analysis for insider threats on the iot using isabelle. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 234-246). Springer, Cham.

[2] Aspects of insider threats

Probst, C.W., Hunker, J., Gollmann, D. and Bishop, M., 2010. Aspects of insider threats. In *Insider Threats in Cyber Security* (pp. 1-15). Springer, Boston, MA.

[3] A risk management approach to the “insider threat”

Bishop, M., Engle, S., Frincke, D.A., Gates, C., Greitzer, F.L., Peisert, S. and Whalen, S., 2010. A risk management approach to the “insider threat”. In *Insider threats in cyber security* (pp. 115-137). Springer, Boston, MA.

[4][Towards an access-control framework for countering insider threats](https://link.springer.com/chapter/10.1007/978-1-4419-7133-3_8)

Crampton, J. and Huth, M., 2010. Towards an access-control framework for countering insider threats. In *Insider Threats in Cyber Security* (pp. 173-195). Springer, Boston, MA.

[5] Honeypots: catching the insider threat

Spitzner, L., 2003, December. Honeypots: Catching the insider threat. In *Computer Security Applications Conference, 2003. Proceedings. 19th Annual* (pp. 170-179). IEEE.

[6] [A survey of insider attack detection research](https://link.springer.com/chapter/10.1007/978-0-387-77322-3_5)

Salem, M.B., Hershkop, S. and Stolfo, S.J., 2008. A survey of insider attack detection research. In *Insider Attack and Cyber Security* (pp. 69-90). Springer, Boston, MA.

[7] Obtaining the Eigenface basis

Krueger, J., Robinson, M., Kochelek, D. and Escarra, M. (2019). *OpenStax CNX*. [online] Cnx.org. Available at: https://cnx.org/contents/m0ECB7MO@3/Obtaining-the-Eigenface-Basis [Accessed 4 Apr. 2019].

[8] How does facial recognition work?

Steve, S. (2019). Symantec Corporation [US] [online] Available at: https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html how does facial recognition work? [Accessed 4apr. 2019].

[9] Modeling Human Behaviour with Higher Order Logic: Insider Threats

Boender, J., Ivanova, M.G., Kammüller, F. and Primiero, G., 2014, July. Modeling human behaviour with higher order logic: Insider threats. In *2014 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 31-39). IEEE.