

INTRUSION DETECTION SYSTEM

by

WEBSCOPE

‌

SUBMITTED TO

**Dr. Durgansh Sharma**

**Associate Professor, Department of Cybernetics**

SUBMITTED BY

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SNo.** | **Course** | **SAP-ID** | **Roll No.** | **Batch** | **Name** |
| **1** | **Bachelor’s of Computer Applications** | **500069713** | **R174218046** | **2nd Year** | **SAARANSH SHARMA** |
| **2.** | **Bachelor’s of Computer Applications** | **500066119** | **R174218066** | **2nd Year** | **VARUN GUPTA** |

DATE: dd/mm/**2020**

Table of Contents

[ABSTRACT 3](#_Toc37698363)

[INTRODUCTION 4](#_Toc37698364)

[OBJECTIVE 5](#_Toc37698365)

[SUB-OBJECTIVE 5](#_Toc37698366)

[OUTCOMES 6](#_Toc37698367)

[EXPECTED OUTCOME 6](#_Toc37698368)

[SOFTWARE DEVELOPMENT METHODOLOGIES 7](#_Toc37698369)

[METHODOLOGY 8](#_Toc37698370)

[DF DIAGRAM (Level 0, Level 1, Level 2) 10](#_Toc37698371)

[ER DIAGRAM 12](#_Toc37698372)

[PEOPLE, PROCESSES & TECHNOLOGY 13](#_Toc37698373)

[ETVX Specification: (PHASE 1 & 2) 17](#_Toc37698374)

[PERT CHART 18](#_Toc37698375)

[Steps in PERT Planning Process: 18](#_Toc37698376)

[Benefits of PERT- (PERT is useful because it provides the following information) 18](#_Toc37698377)

[PERT CHART (DIAGRAM) 19](#_Toc37698378)

[PROJECT DURATION 20](#_Toc37698379)

[STATE DIAGRAM 21](#_Toc37698380)

[STATE CHART 22](#_Toc37698381)

[CLASS DIAGRAM 23](#_Toc37698382)

[SEQUENCE DIAGRAM 24](#_Toc37698383)

[AI in Intrusion Detection System 25](#_Toc37698384)

[IDS implementation using AI 25](#_Toc37698385)

[Intrusion Detection and Prevention Systems (IDPS) 27](#_Toc37698386)

[REFERENCES 28](#_Toc37698387)

[GITHUB 28](#_Toc37698388)

# ABSTRACT

Intrusion Detection System (IDS) is a security system that acts as a protection layer to the infrastructure. Throughout the years, the IDS technology has grown enormously to keep up with the advancement of computer crime. Since the beginning of the technology in middle 80’s, researches have been conducted to enhance the capability of detecting attacks without jeopardizing the network performance. In this paper we hope to provide a critical review of the IDS technology, issues that transpire during its implementation and the limitation in the IDS research endeavors.

Lastly we will proposed future work while exploring maturity of the topic, the extent of discussion, the value and contribution of each research to the domain discussed. At the end of this paper, readers would be able to clearly distinguish the gap between each sub-area of research and they would appreciate the importance of these research areas to the industry.

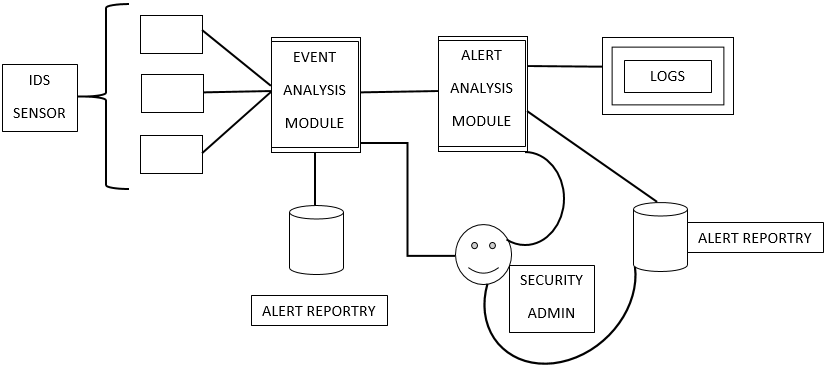
# INTRODUCTION

As the today’s generation we all knew that the criminal/theft has been occurred in user’s life regarding their **data security**. We have four agile-manifesto as well as twelve methodology. Through which we have to take certain steps regarding making a strong security for the user’s. Firstly, individuals and interactions over processes and tools, as we know that intrusion detection system is based on to detect the suspicious activity from the database information. This information will automatically monitor and scan the unauthorized to user information does not allow in our system and there is an administrator to secure our database to add security to secure the database example, Administrator ID, Password, etc. Tools like IDS, sensor, alert repository, login, security admin this are used to secure our database. Secondly, working software over comprehensive documentation, which means the documentation types that the team produces and its scope depend on the software development approach that was chosen. *Here we are going to use* **"Scrum Model** *as it’s the latest methodology of agile system* **– Scrum world, instead of providing complete, detailed descriptions of how everything is to be done on a project, much of it is left up to the Scrum software development team. This is because the team will know best how to solve the problem they are presented."** Thirdly, Customer Collaboration over contract negotiation, when the customer and the project manager — or another project team representative — negotiate contract details. When the customer and the project manager negotiate changes to the contract. When the project team delivers a completed product to the customer. If the product doesn’t meet customer expectations, the project manager and the customer negotiate additional changes to the contract. And lastly we have, responding to change over following a plan, to adaptive planning approach. In this approach, planning is an ongoing activity throughout the execution of the entire project, occurring in small increments as the reality of project execution unfolds.

# OBJECTIVE

Intrusion Detection System (IDS) is a detective device designed to detect malicious (including policy-violating) actions. An Intrusion Prevention System (IPS) is primarily a preventive device designed not only to detect but also block malicious actions.

Depending on their physical location in the infrastructure, and the scope of protection required, the IDS’ and IPS’ fall into two basic types: network-based and host-based. Both have the same function and the specific type deployed depends on strategic considerations.



## SUB-OBJECTIVE

The proper identification of mission-critical systems and points of entry requires the following roles in an organization to be involved in any IDS/IPS deployment:

* Senior Management
* Information Security Officers
* Data owners
* Network Administrators
* Database Administrators
* Operating System Administrators

# OUTCOMES

‌

The outcomes of the project is to make end user’s life easier through making their data security, which could be more secure while working with Intrusion Detection System (IDS).

## EXPECTED OUTCOME

In this project I would like to help end user life more beneficial and securing their profile from the intruders. As IDS work is to make secure of data security from intruders/intrusions.

# SOFTWARE DEVELOPMENT METHODOLOGIES

It play a vital part of developing the software. There are many methodologies which are used by the professional [software development companies](https://www.tatvasoft.com/) nowadays. There are certain advantages and disadvantages associated with each of them. The basic purpose of these methodologies is to provide smooth software development according to the project requirements.

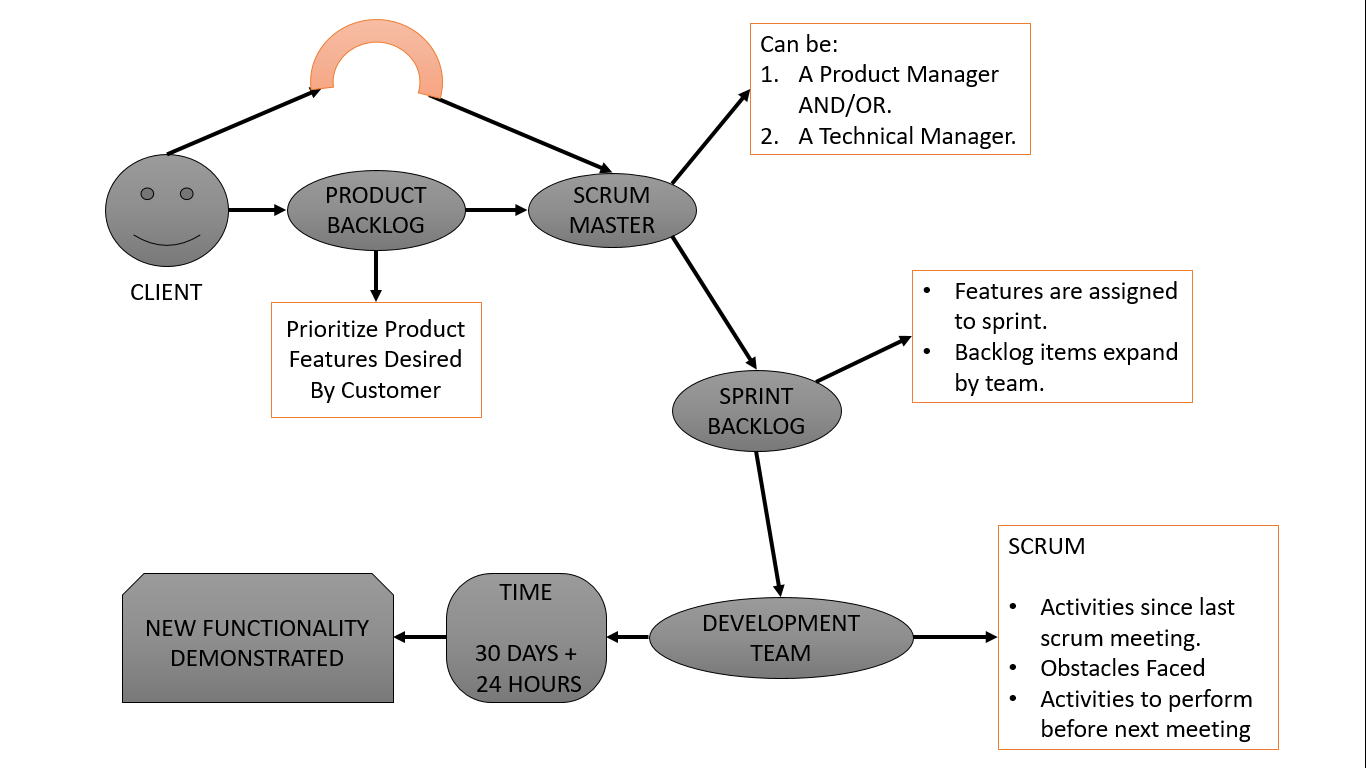
Software development methodology is a framework that is used to structure, plan, and control the process of developing an information system. This kind of development methodologies are only concerned with the software development process, so it does not involve any technical aspect of, but only concern with proper planning for the software development.

**The 12 mainly used software development methodologies with their advantages and disadvantages:**

|  |  |  |
| --- | --- | --- |
| [Waterfall Model](https://www.tatvasoft.com/blog/top-12-software-development-methodologies-and-its-advantages-disadvantages/#anchor1) | [Prototype Model](https://www.tatvasoft.com/blog/top-12-software-development-methodologies-and-its-advantages-disadvantages/#anchor2) | [Agile software development](https://www.tatvasoft.com/blog/top-12-software-development-methodologies-and-its-advantages-disadvantages/#anchor3) |
| [Rapid Application Development](https://www.tatvasoft.com/blog/top-12-software-development-methodologies-and-its-advantages-disadvantages/#anchor4) | [Dynamic Systems Development Model](https://www.tatvasoft.com/blog/top-12-software-development-methodologies-and-its-advantages-disadvantages/#anchor5) | [Spiral Model](https://www.tatvasoft.com/blog/top-12-software-development-methodologies-and-its-advantages-disadvantages/#anchor6) |
| [Extreme Programming](https://www.tatvasoft.com/blog/top-12-software-development-methodologies-and-its-advantages-disadvantages/#anchor7) | [Feature Driven Development](https://www.tatvasoft.com/blog/top-12-software-development-methodologies-and-its-advantages-disadvantages/#anchor8) | [Joint Application Development](https://www.tatvasoft.com/blog/top-12-software-development-methodologies-and-its-advantages-disadvantages/#anchor9) |
| [Lean Development](https://www.tatvasoft.com/blog/top-12-software-development-methodologies-and-its-advantages-disadvantages/#anchor10) | [Rational Unified Process](https://www.tatvasoft.com/blog/top-12-software-development-methodologies-and-its-advantages-disadvantages/#anchor11) | [Scrum Development](https://www.tatvasoft.com/blog/top-12-software-development-methodologies-and-its-advantages-disadvantages/#anchor12) |

# METHODOLOGY

**Scrum Development Methodology**



The **Scrum Development Methodology** can be applied to nearly any project. This process is suited for development projects that are rapidly changing or highly emergent requirements. The Scrum software development model begins with a brief planning, meeting and concludes with a final review. This development methodology is used for speedy development of software which includes a series of iterations to create required software. It is an ideal methodology because it easily brings on track even the slowest progressing projects.

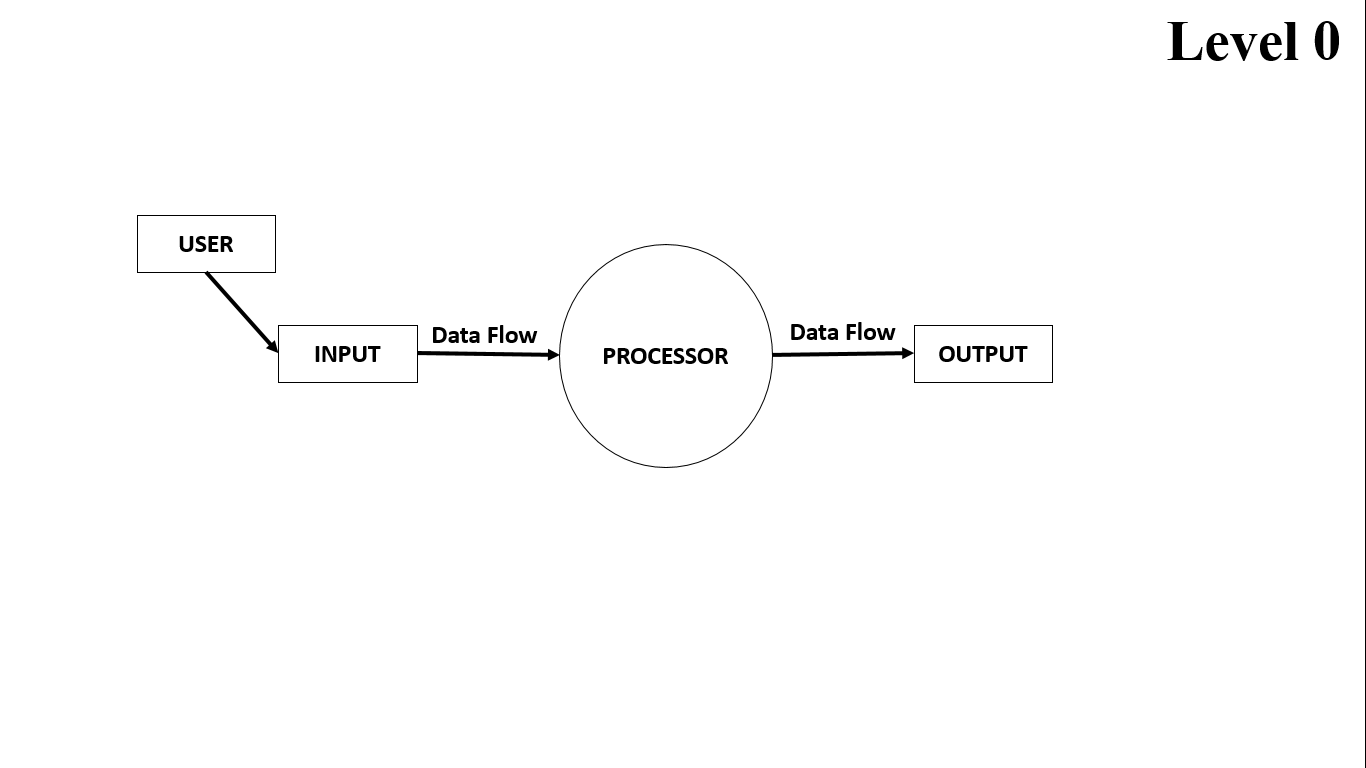
#### **Advantages of Scrum Development:**

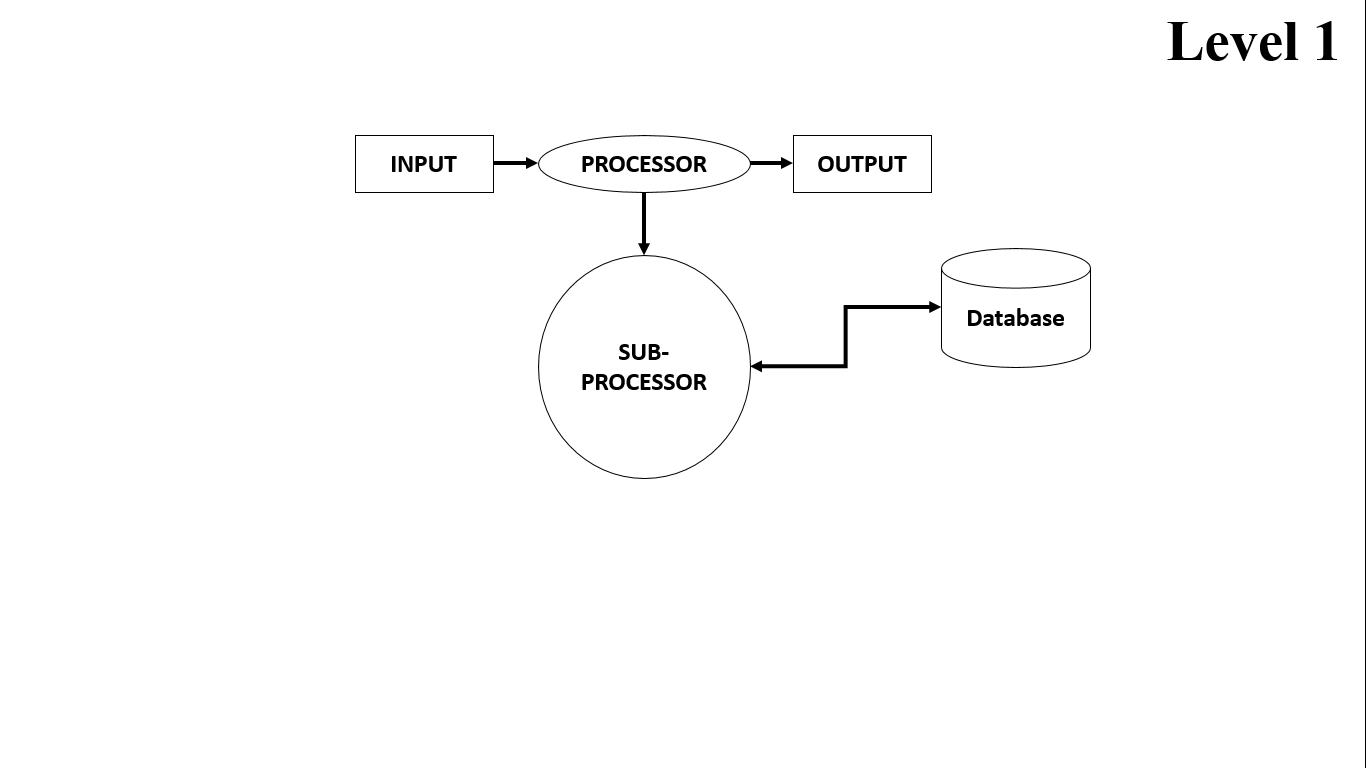
* + In this methodology, decision-making is entirely in the hands of the teams
  + This methodology enables project’s where the business requirements documentation is not considered very significant for the successful development
  + It is a lightly controlled method which totally empathizes on frequent updating of the progress, therefore, project development steps is visible in this method
  + A daily meeting easily helps the developer to make it possible to measure individual productivity. This leads to the improvement in the productivity of each of the team members

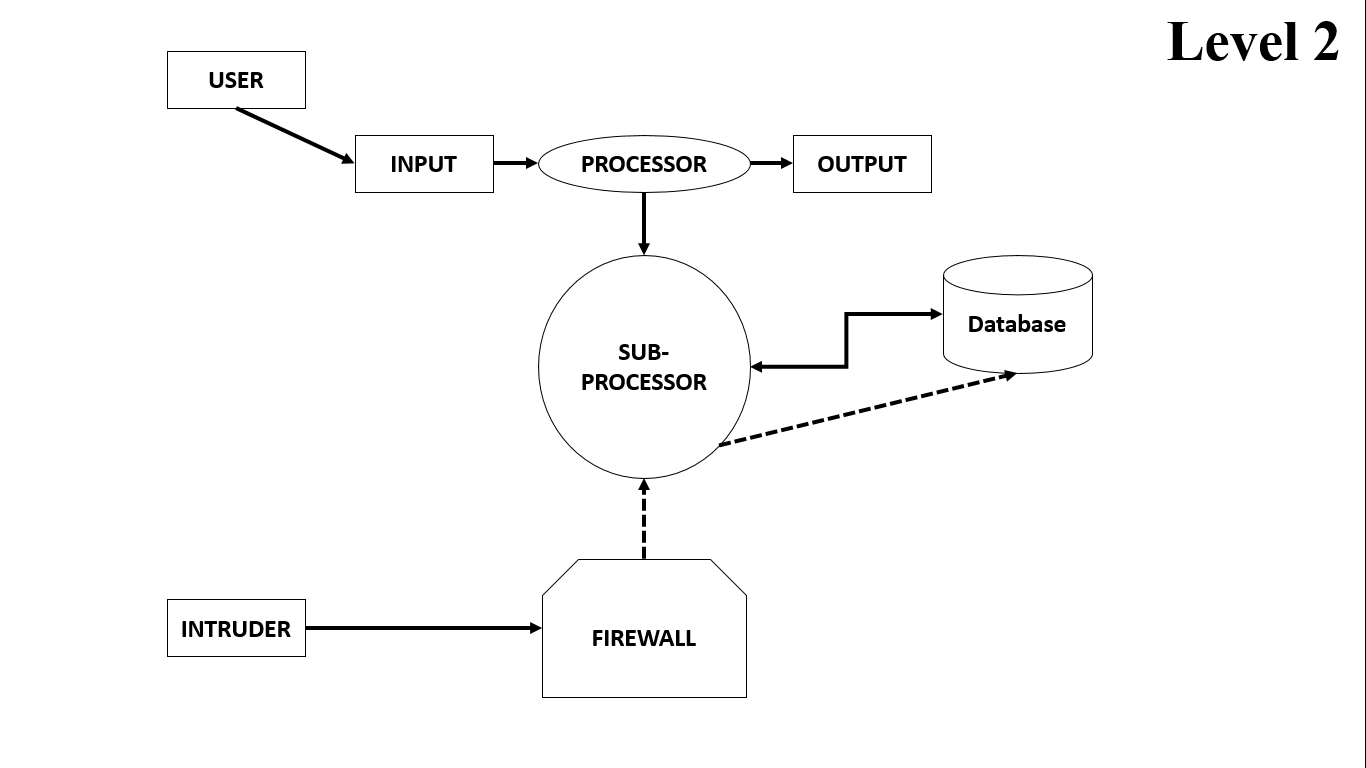
#### **Disadvantages of Scrum Development:**

* + This kind of development model is suffered if the estimating project costs and time will not be accurate
  + It is good for small, fast moving projects but not suitable for large size projects
  + This methodology needs experienced team members only. If the team consists of people who are novices, the project cannot be completed within exact time frame

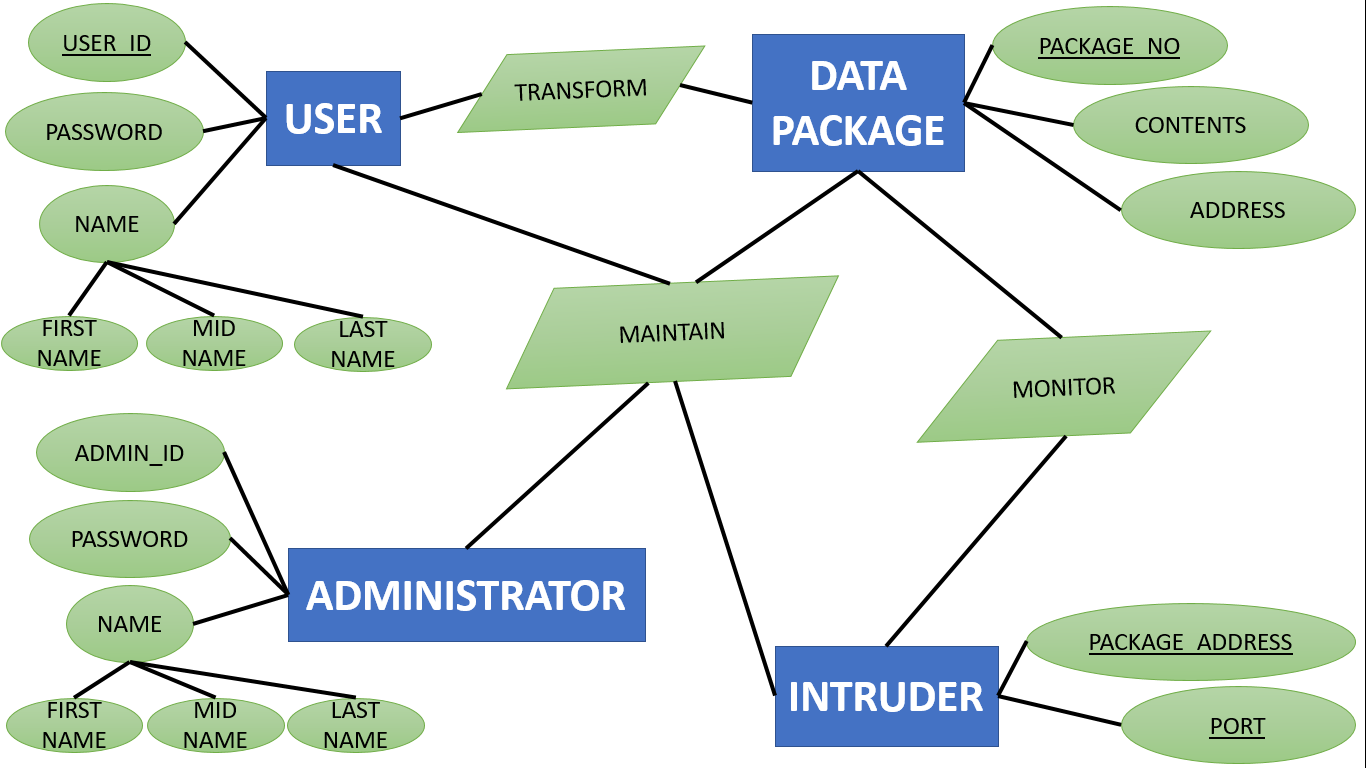
# DF DIAGRAM (Level 0, Level 1, Level 2)



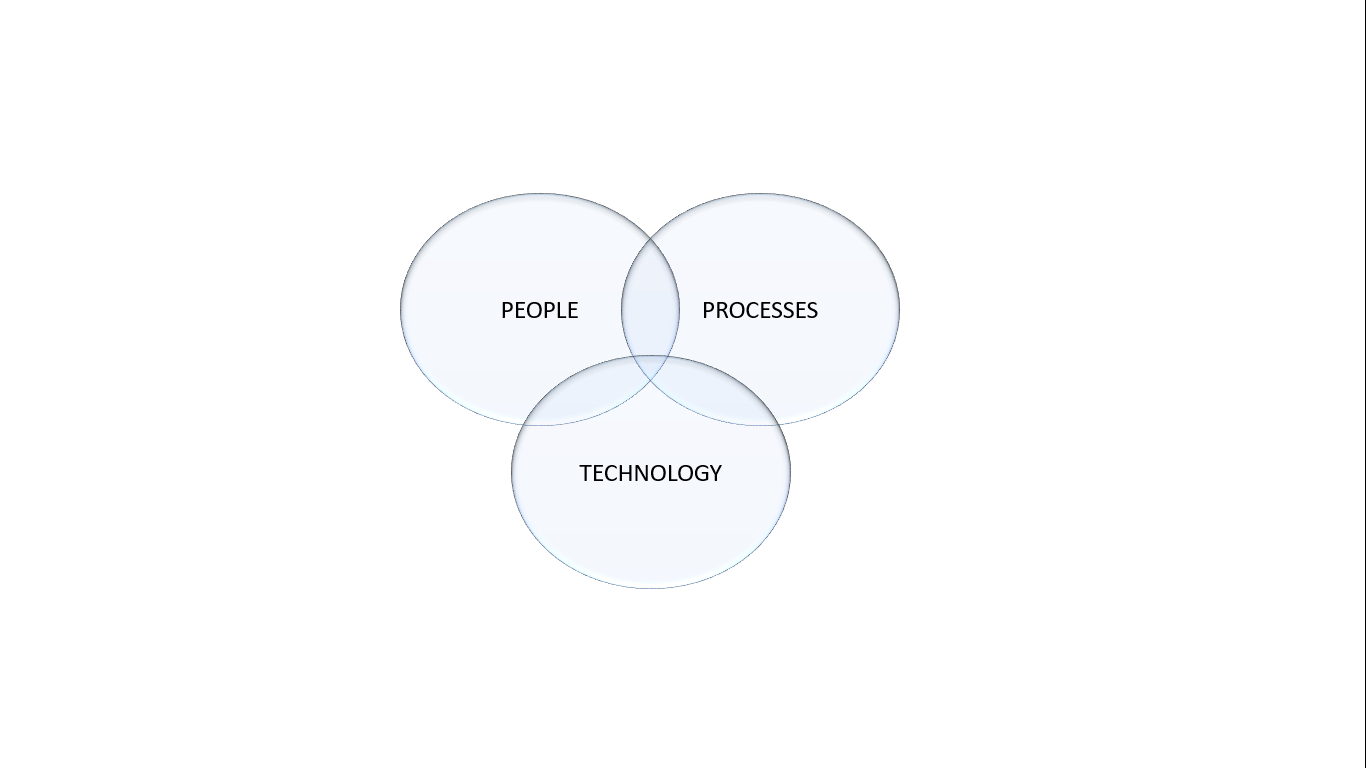




# ER DIAGRAM

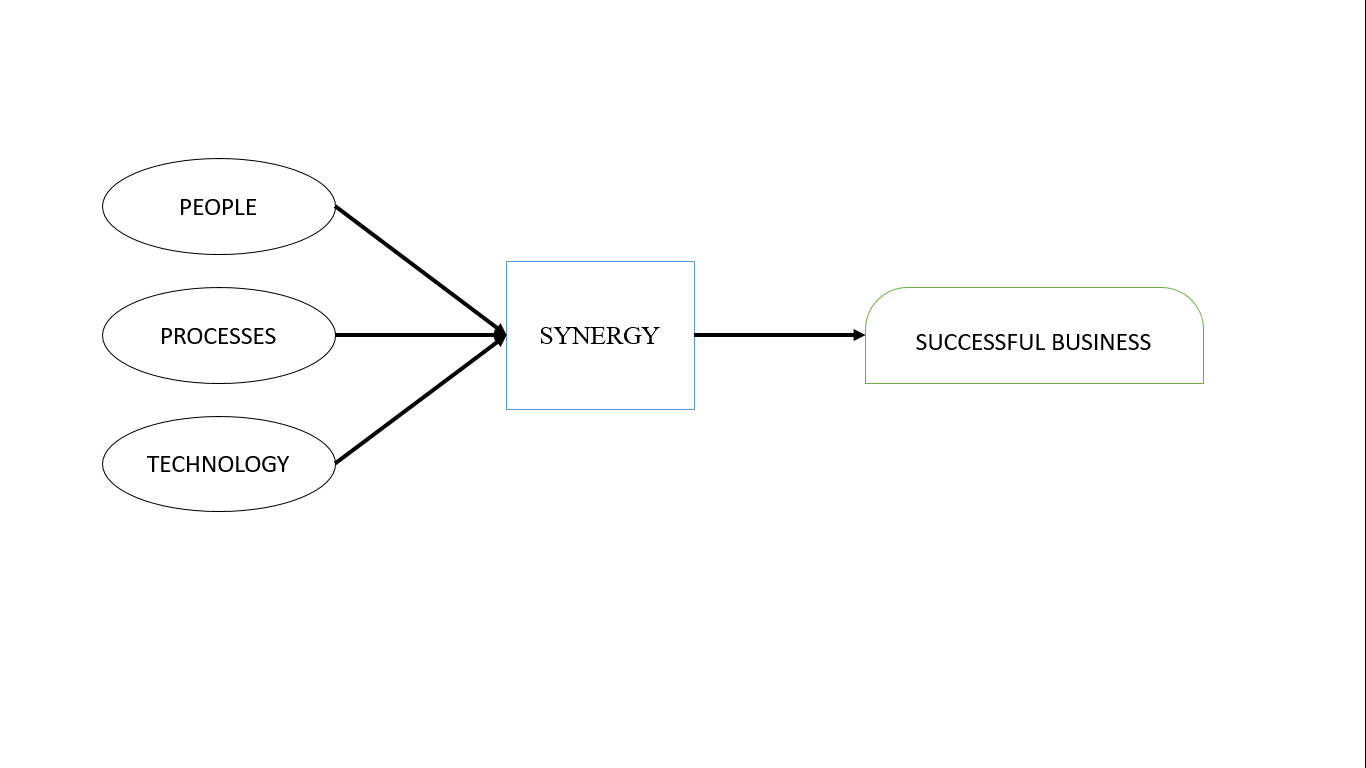


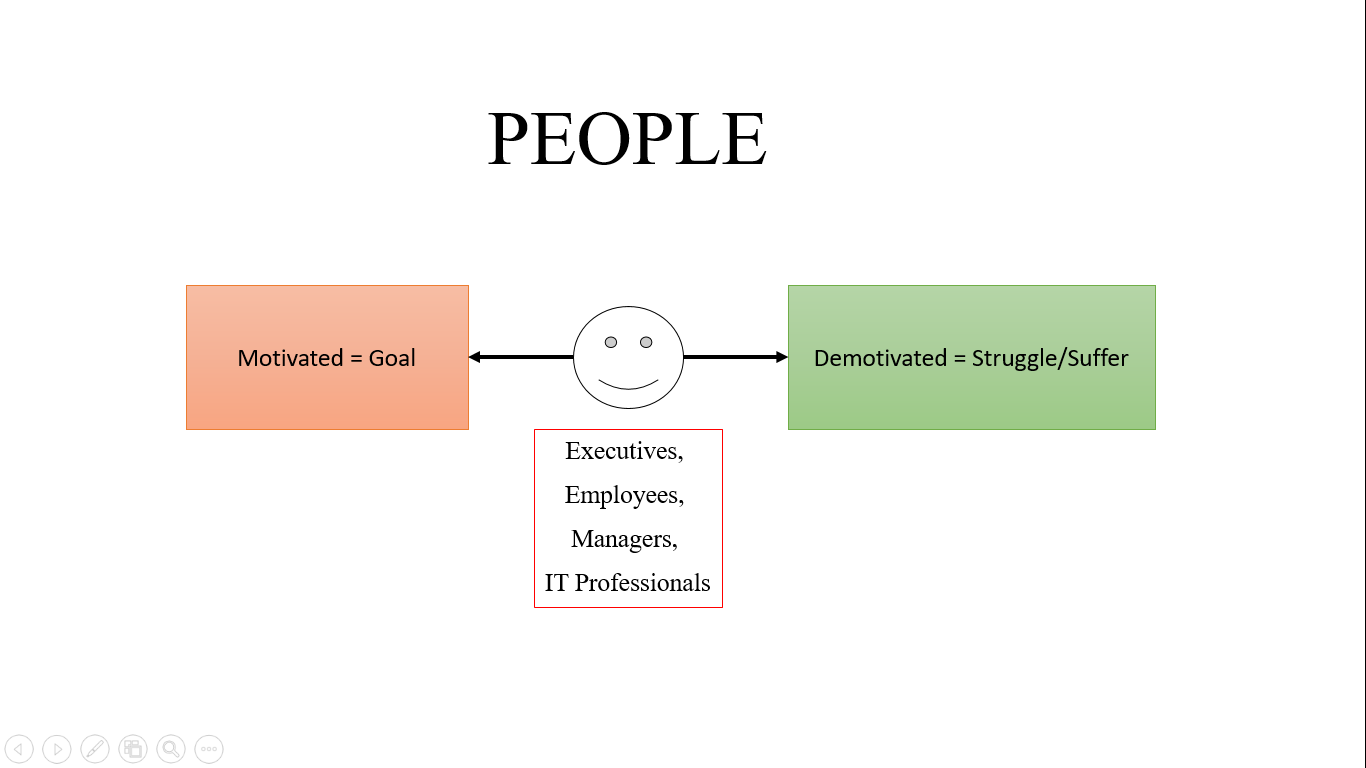
# PEOPLE, PROCESSES & TECHNOLOGY



**Points to Remember**

1. Without technology we are nothing.
2. Without processes technology is nothing.
3. Above all if there are not people who use technology, there nothing can be done.

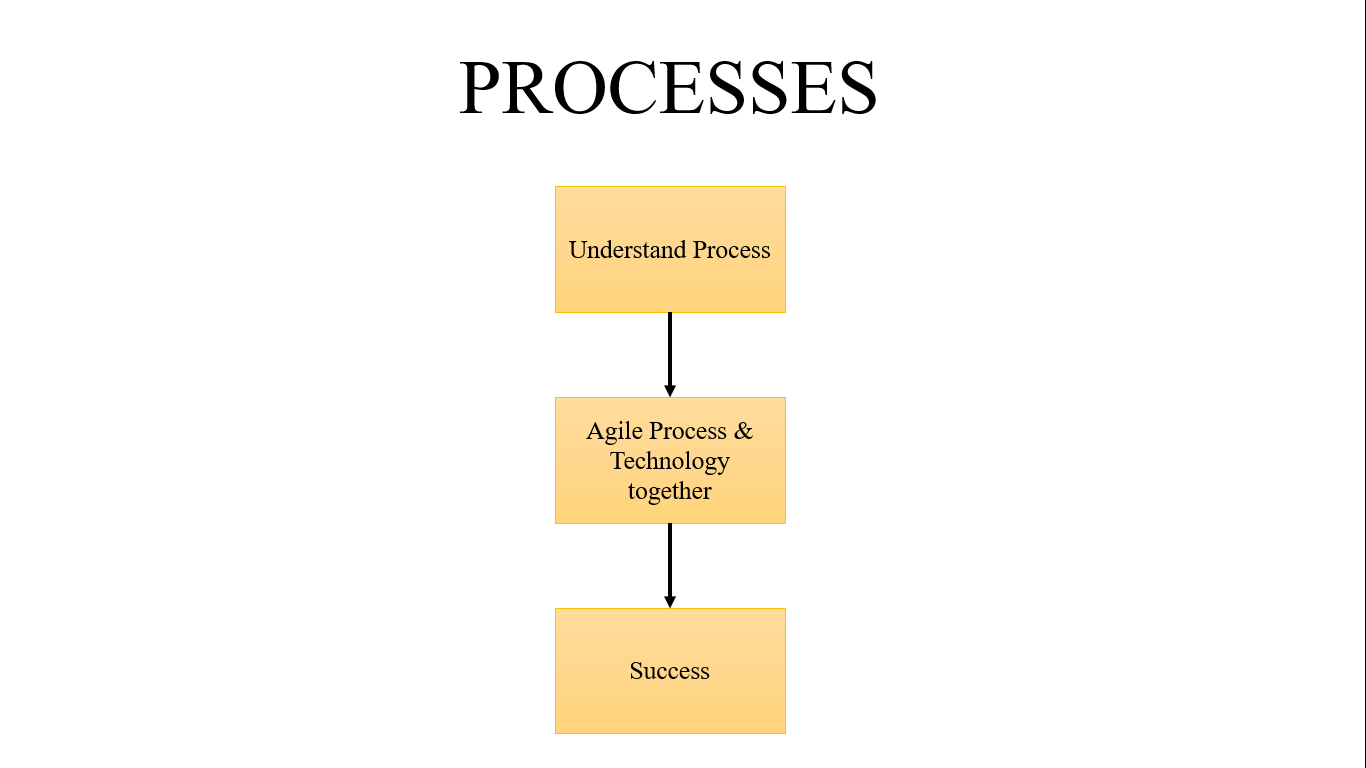




With this innovative idea for this intrusion detection system, so we satisfy the want of people and that are the end user as they are going to ultimately try our product and these end user are going to give feedback for our product. Intrusion detection system is going to offer to secure our database will satisfy the people this is help to secure our database and tools will help the people changes in our database and main important part, Any off access our database or breach the database is disallow this is to safe the database of unauthorized user is not access them, in project divided in the groups for good interaction in group for doing his work .All this work a lot of interaction in the group members. The more person in there team, the more interaction is required in there team and there is such difficulties to manages there team, the project manager must define the relationships between the roles to enable the effective coordination and control of the project. And individuals with different personalities are often expected to work together as a cohesive team. Team efficiency is often dependent on the interaction between team members and the coordination of the team leader. In team member there the better coordination is to study equally because is to give idea to more attractive or more easily to display the project to coding member is to recall the all project is more to code there no error or difficulties to face to represent to people is to easy, There is main important part to equal contribution all the team members, the more persons there is on a team the more difficult it is to communicate and share information among team members. Thus team size affects both efficiency and productivity of teams directly. In the team member motivated the other members to doing the work, there is more important to communicate manager to employees.

And off the executive the project, firstly check the mistake and after finally check to show the project to the manager check the all things and check the coding and manager help to IT professional read the all project and check the code there is any mistake in code, coder is satisfy the code is to tell the project manager is satisfy.

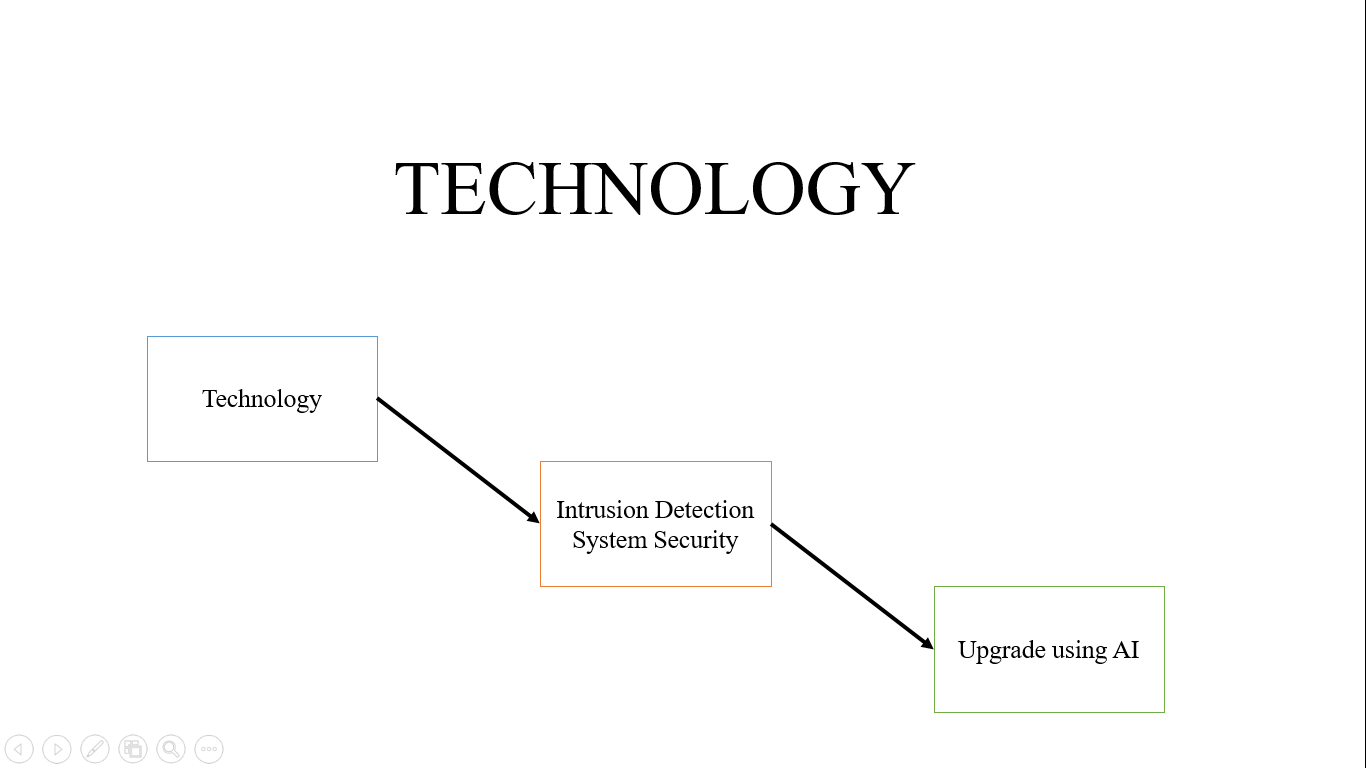
* **People will always put their own interests ahead of the interests of the group.**
* **People are self-interested.**
* **Commercial production decisions are based on rational expectations.**



What process is to flow to development our project, In phase 1 of our project we discussed the software development and methodologies as these provide the platform for developing our project and we took one methodology that is scrum development and another main discussed about the Manifesto of agile development there is 4 point is to incorporate in our project and we discussed the flow diagram of our project and Entity relationship model and DFD explain three level [0 1 2] also. In phase 2 include the certain aspects of our project it’s the sequences of steps that is undertaken of our developer. Those process is to incorporate with the product. Those processes has certain tasks is to execute in the product. In software engineering flows the certain steps of process. Is to flow the steps and you the better Result and success achieve in the project objectives.

Software process produce the high quality software and better costing. There are two major processes are include:

* **Development**: main focusing on the development software and also coordinate the team work.
* **Project management**: and focusing on the planning and also plan, in project management is flow the stages, the efficient time to complete stages in the project.



The technology that we will be used in the project will be **Artificial intelligences** for the requirement of the project. We have to use the Artificial intelligences from Intrusion detection system security is to secure the database using host id and password, is to upgrade the security using the AI, is access the more security in the database to secure that is add the security (fingerprint sensor, face recognition) administer using this security to add in the database is to another people not to access them, and use the storage memory to store the database for not to delete or realize any information in database.

# ETVX Specification: (PHASE 1 & 2)

1. **ETVX approach to specify a step1:**
   1. **Entry criteria**: what conditions must be satisfied for initiating this phase1

[Given this (ER diagram, DFD level 2)]

* 1. **Task**: what is to be done in this phase1

[Fulfill this conduction according to our constructor (ER diagram, DFD level)]

* 1. **Verification**: the checks done on the outputs of this phase1
  2. **exit criteria**: when can this phase1 be considered done successfully

1. **ETVX approach to specify a step2:**
   1. **Entry criteria**: what conditions must be satisfied for initiating this phase2

[Given this (pert chart and software processes)]

* 1. **Task**: what is to be done in this phase2

[Fulfill this conduction according to our constructor (pert chart and software processes)]

* 1. **Verification**: the checks done on the outputs of this phase2.
  2. **Exit criteria**: when can this phase2 be considered done successfully.

# PERT CHART

PERT stands for PROGRAM EVALUATION & REVIEW TECHNIQUE.

A chart is a tool that shows project as network diagram. It was develop in 1950 for US Navy to reduce both the time and cost required for complete a project.

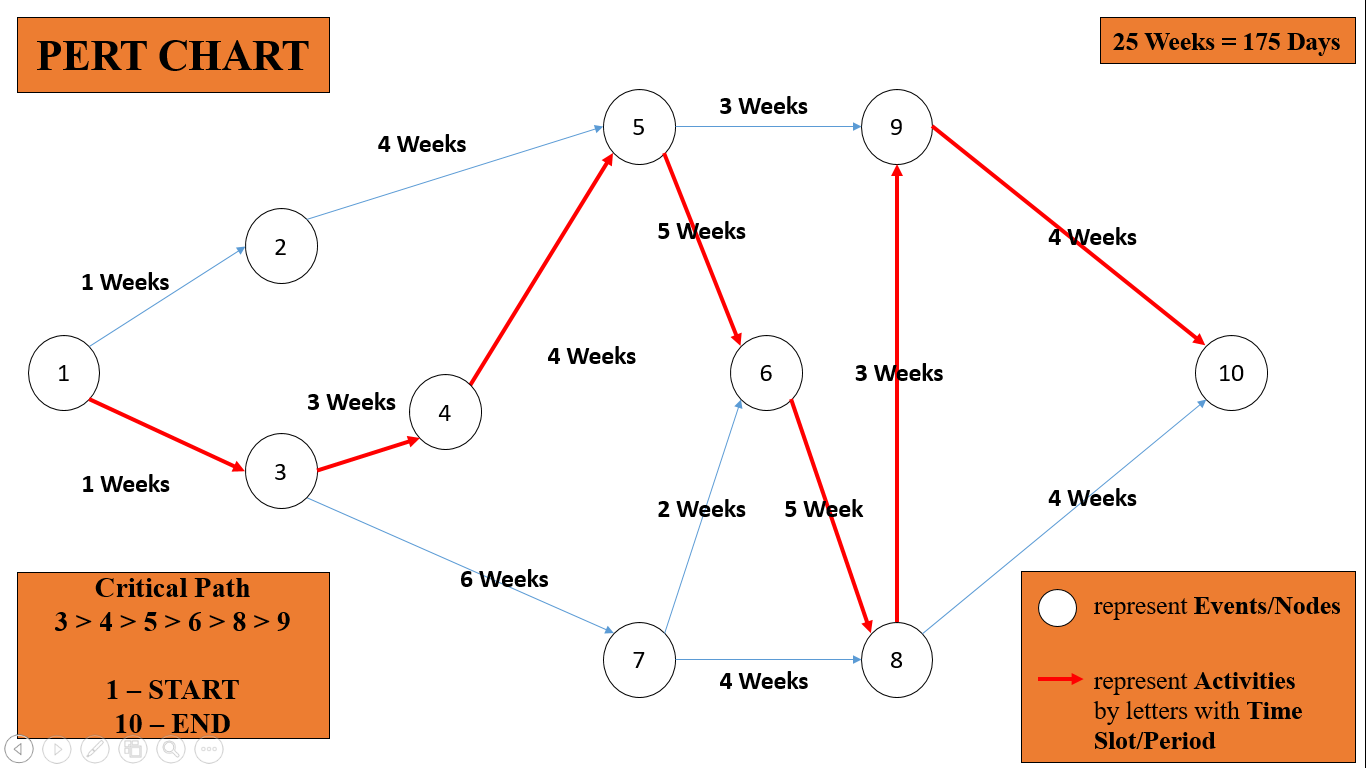
## Steps in PERT Planning Process:

1. Identify the specific activities and milestones.
2. Determine the proper sequence of activities.
3. Estimate the time required for each activity.
4. Determine the critical path.
5. Update the PERT CHART as the project progress.

## Benefits of PERT- (PERT is useful because it provides the following information)

1. Expected product completion time.
2. Probability of completion before a specific date.
3. The critical path activities that directly impact the completion time.
4. Activity start & end dates.

# PERT CHART (DIAGRAM)



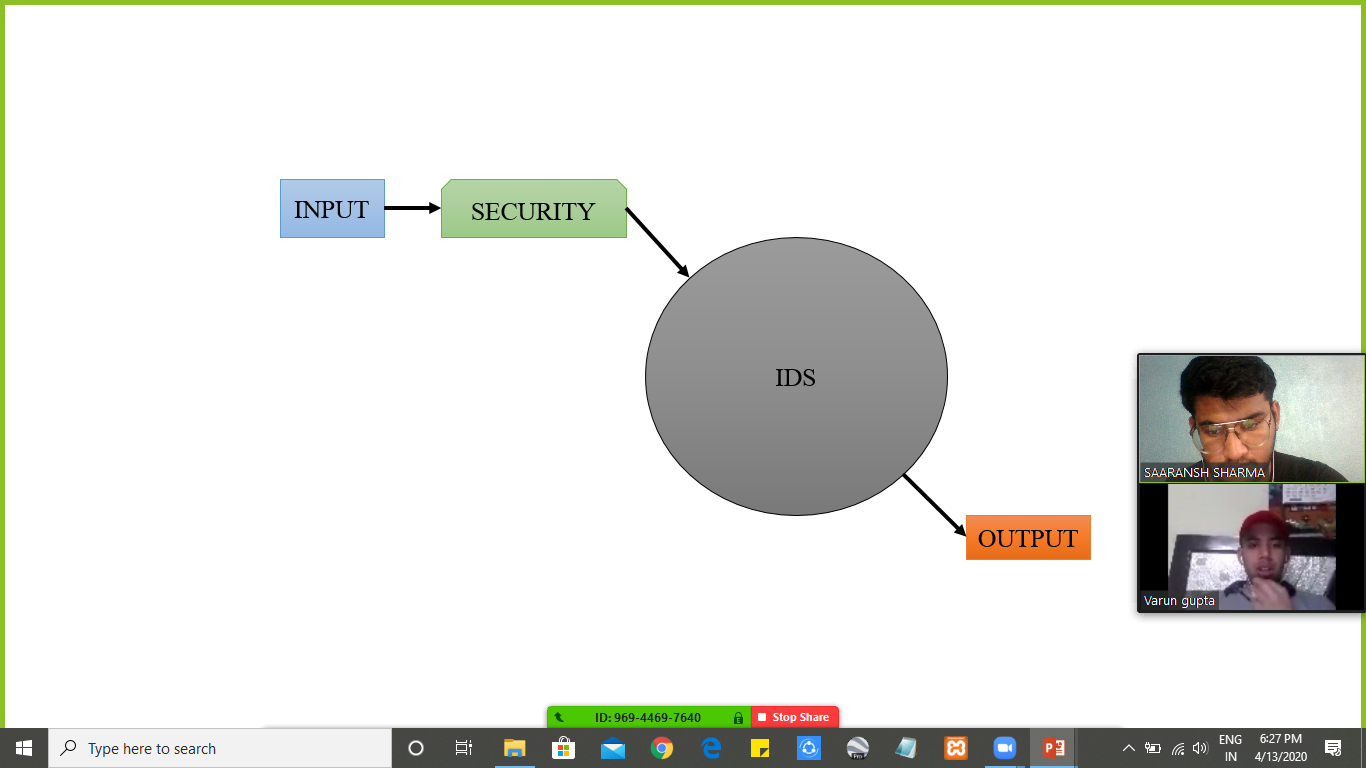
|  |  |  |  |
| --- | --- | --- | --- |
| **EVENTS/NODES** | **ACTIVITES** | | **Critical Path** |
| **EVENT occurred in TIME SLOT** | **25 WEEKS** |
| 1. Start | 1 – START – 3 | WEEK 1 | **1** |
| 2. Feasibility Study | 3 – Feasibility Study – 4 | WEEK 3 | **3** |
| 3. Requirement Analysis | 4 – Requirement Analysis – 5 | WEEK 4 | **4** |
| 4. Design | 5 – Design – 6 | WEEK 5 | **5** |
| 5. Coding/Algorithm | 6 – Coding/Algorithm – 8 | WEEK 5 | **6** |
| 6. Testing | 8 – Testing – 9 | WEEK 3 | **8** |
| 7. Maintenance | 9 – End – 10 | WEEK 4 | **9, 10** |

# PROJECT DURATION

|  |  |  |  |
| --- | --- | --- | --- |
| **TASK NAME** | **DURATION** | **START DATE** | **END DATE** |
| 1. Feasibility study | 3 WEEKS | 8/1/2020 | 28/01/2020 |
| Technical Feasibility | 1 WEEK | 8/1/2020 | 14/01/2020 |
| Economic Feasibility | 1 WEEK | 15/01/2020 | 21/01/2021 |
| Behavior Feasibility | 1 WEEK | 22/01/2021 | 28/01/2020 |
| 2. Requirement Analysis | 4 WEEKS | 29/01/2020 | 25/02/2020 |
| Requirement Gathering | 1 WEEK | 29/01/2020 | 4/2/2020 |
| Group Interaction | 2 WEEK | 5/2/2020 | 18/02/2020 |
| Analysis | 1 WEEK | 19/02/2020 | 25/02/2020 |
| 3. UI-Design | 5 WEEKS | 26/02/2020 | 31/03/2020 |
| Firewall | 2.5 WEEK | 26/02/2020 | 14/03/2020 |
| Log Management | 2.5 WEEKS | 15/03/2020 | 31/03/2020 |
| 4. Coding / Algorithm | 5 WEEKS | 1/4/2020 | 5/5/2020 |
| Firewall | 2.5 WEEK | 1/4/2020 | 18/04/2020 |
| Log Management | 2.5 WEEKS | 19/04/2020 | 5/5/2020 |
| 5. Testing | 3 WEEKS | 6/5/2020 | 26/05/2020 |
| Unit Testing | 1 WEEK | 6/5/2020 | 12/5/2020 |
| Integration Testing | 1 WEEK | 13/05/2020 | 19/05/2020 |
| System Testing | 1 WEEK | 20/05/2020 | 26/05/2020 |

# STATE DIAGRAM

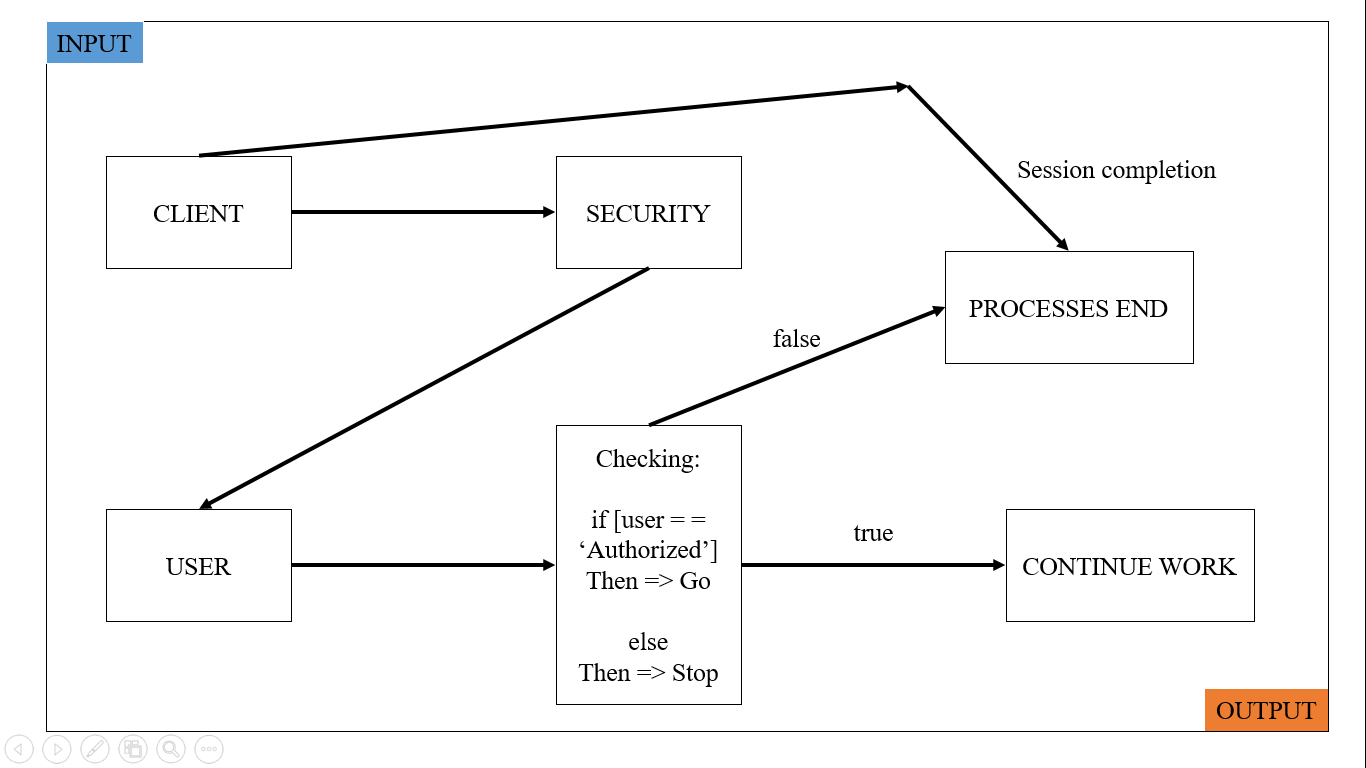
In this diagram, we can see the input and output is occurred and in the processes part (Security and IDS) will help the user to get in the database and process output as information.



# STATE CHART

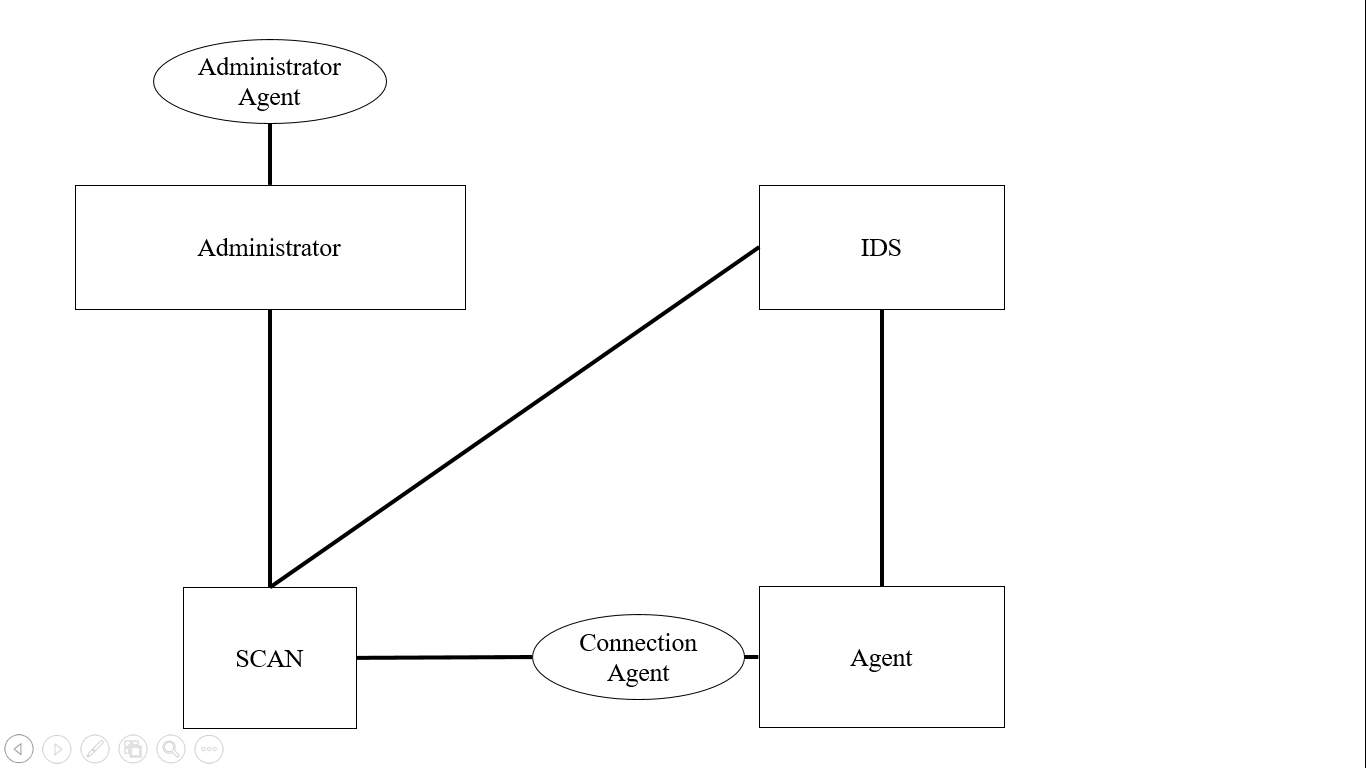
In the following diagram we can see the state chart that talks about a Client, Server/Network, a Sensor, Logs (Data), Administrator, an IDS and an Intruder.

Here, we are going to secure a data from Intruder.



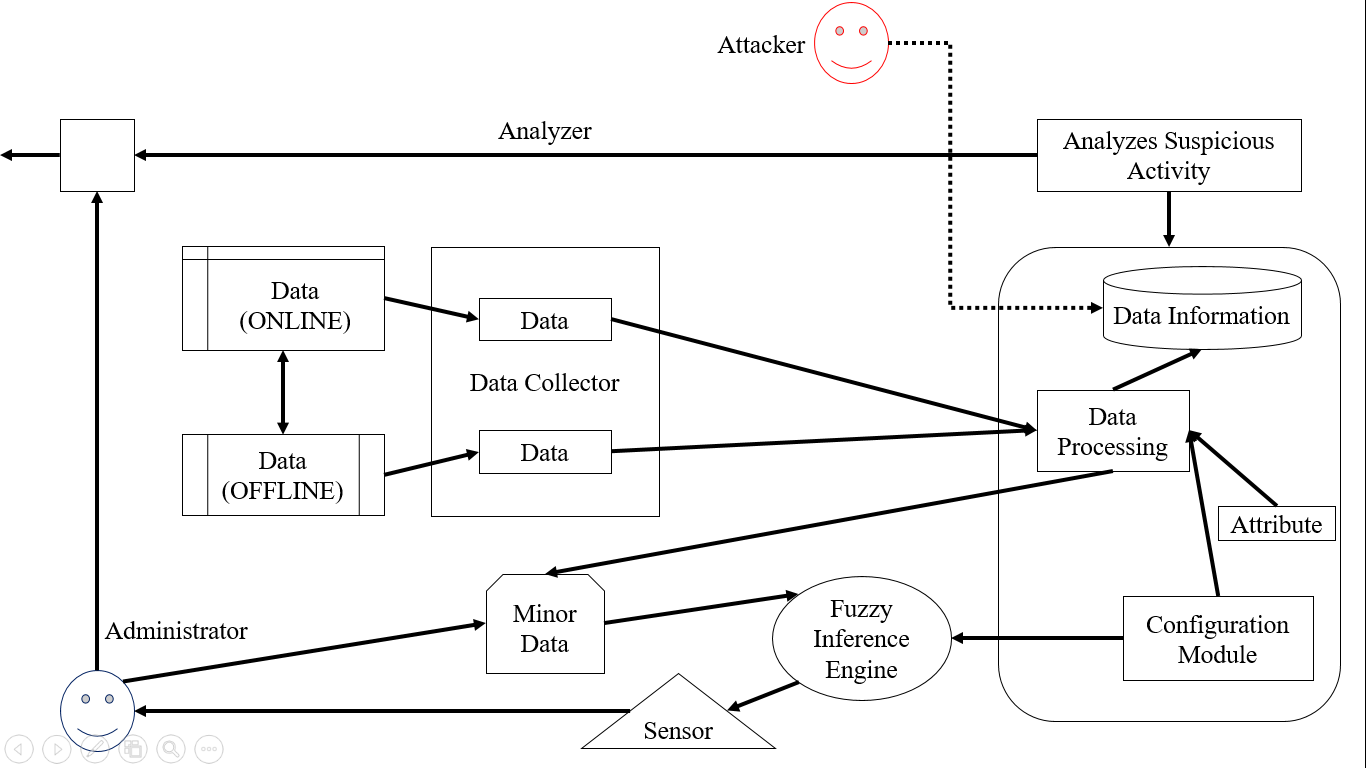
# CLASS DIAGRAM

In this diagram we can see every data is connected to agent and administrator.



# SEQUENCE DIAGRAM

In this diagram, we can see the data is online and offline, and an attacker will try to access to the information and the sensor inform to the administrator to update and change the information and send further.



# AI in Intrusion Detection System

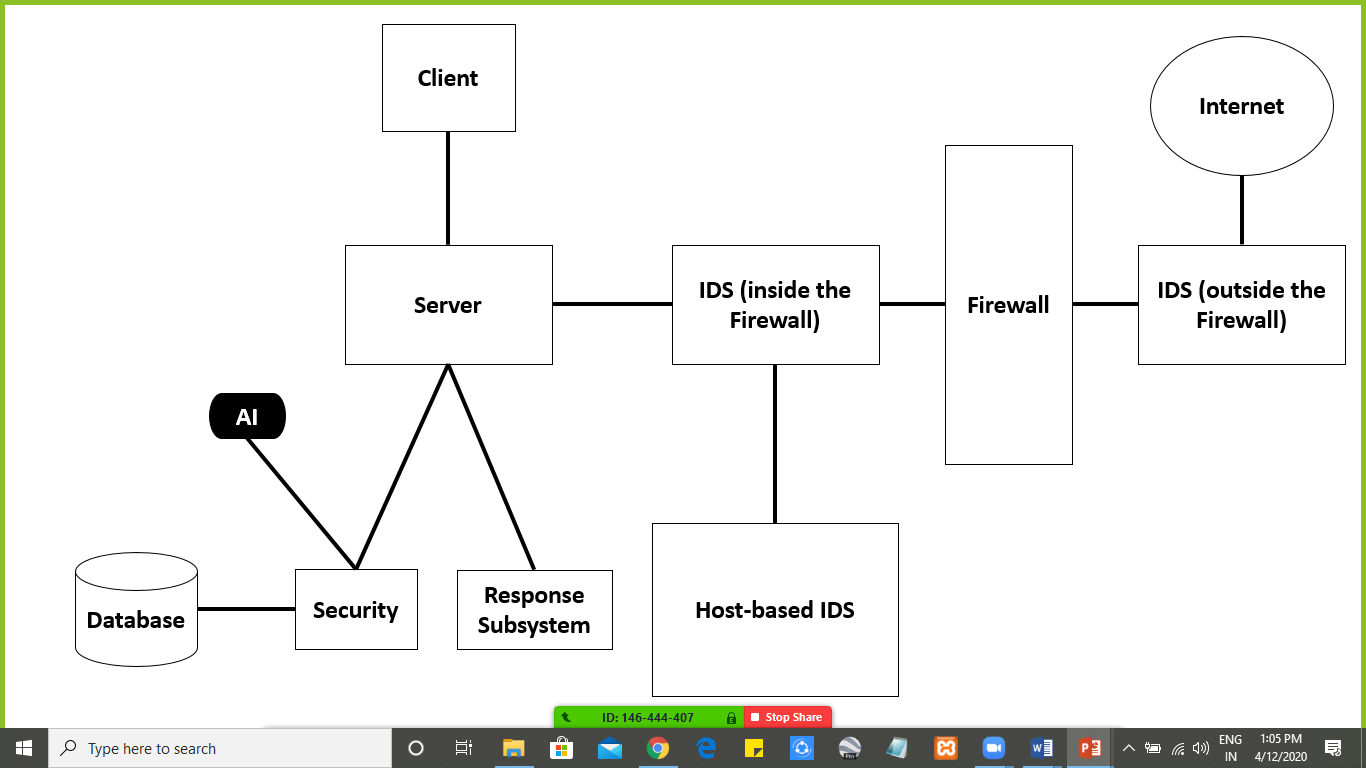
“In IDS, using AI for security would help us to recognize the **user** so that an intruder couldn’t access to the security breach and our database information is secured.”

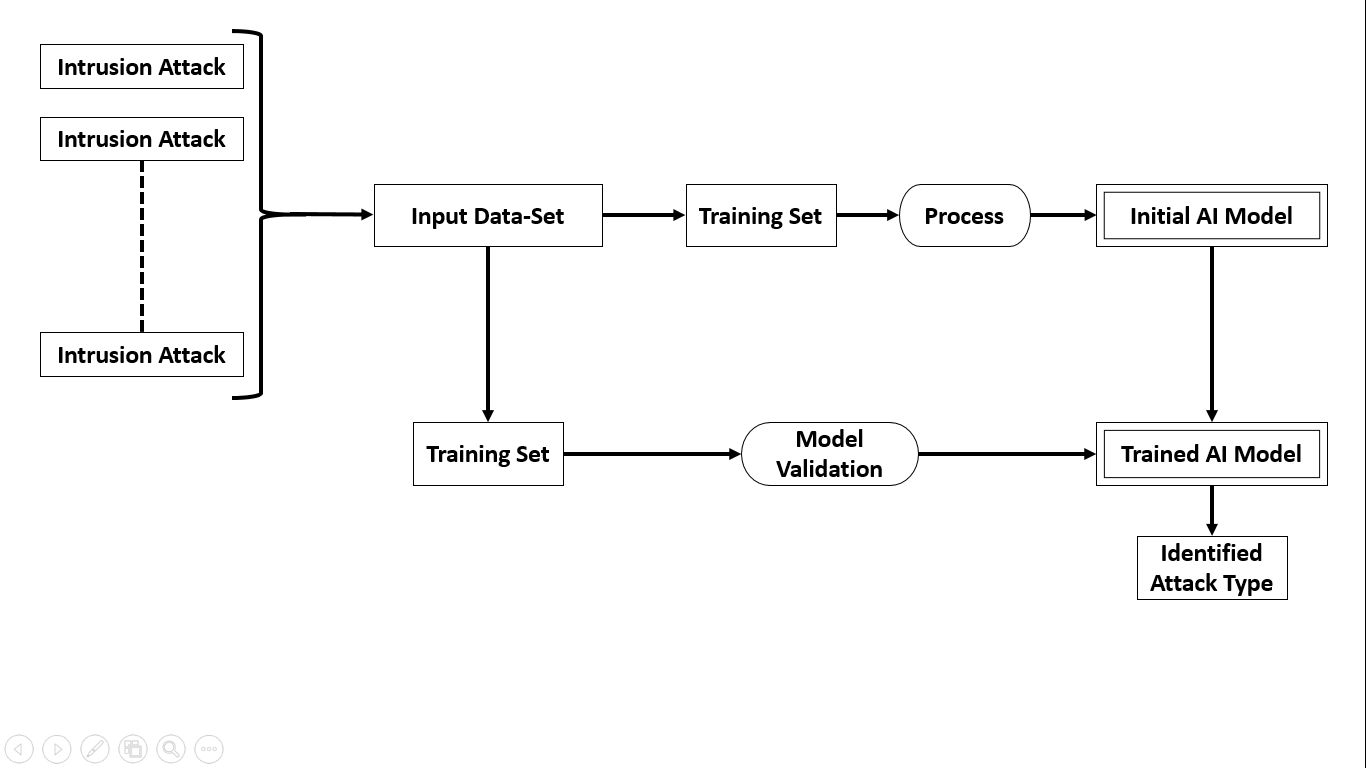
## IDS implementation using AI

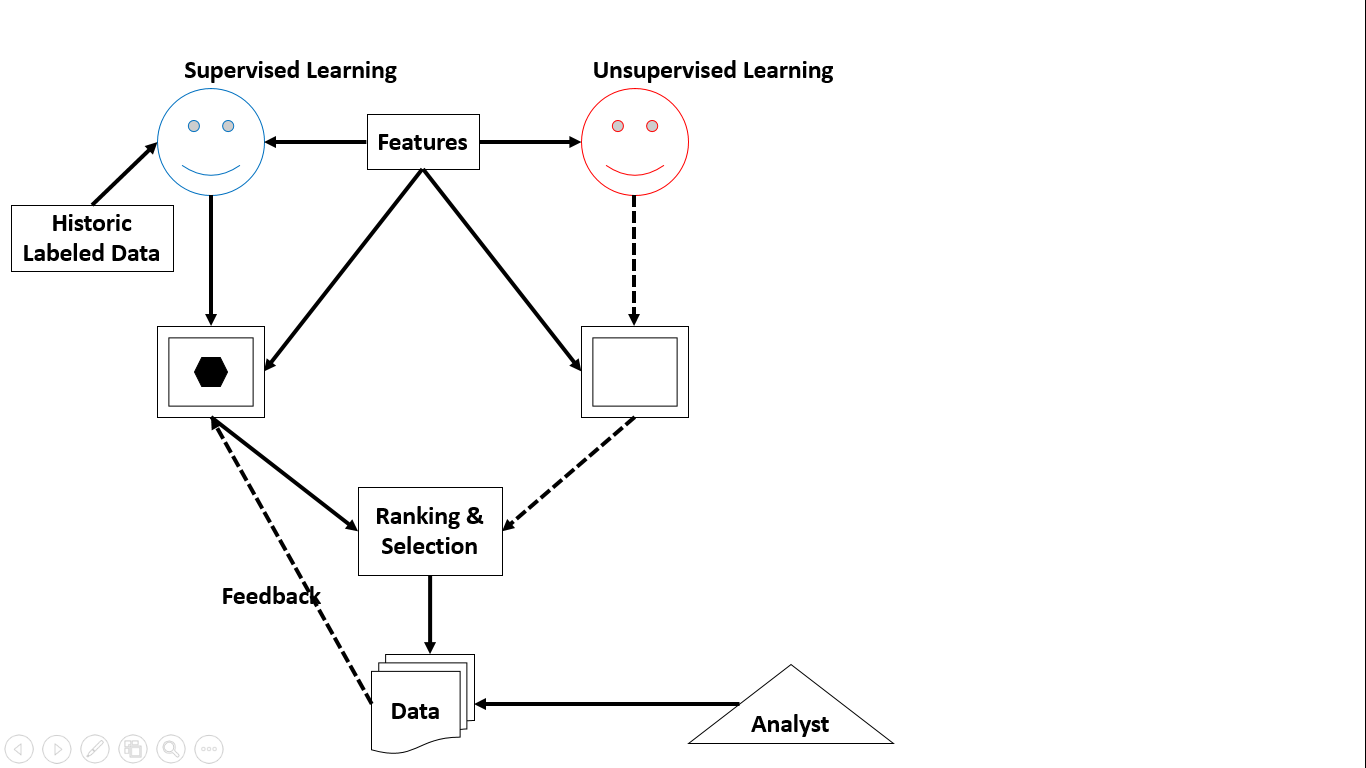
Artificial intelligence has been widely used in decision-making system and for the classification in [computer vision](http://www.scialert.net/asci/result.php?searchin=Keywords&cat=&ascicat=ALL&Submit=Search&keyword=computer+vision) applications. It is utilized in various [processing](http://www.scialert.net/asci/result.php?searchin=Keywords&cat=&ascicat=ALL&Submit=Search&keyword=image+processing) applications including [face, finger or voice recognition](http://scialert.net/asci/result.php?searchin=Keywords&cat=&ascicat=ALL&Submit=Search&keyword=pattern+recognition).

AI can be classified in supervised, unsupervised and hybrid learning methods.

In supervised learning, desired output is used to learn the algorithm for better classification, whereas in unsupervised AI inputs are analyzed without target output. Hybrid approach integrates both supervise and unsupervised learning method to generates specified rules and or signature. The block diagram for AI based intrusion detection system.

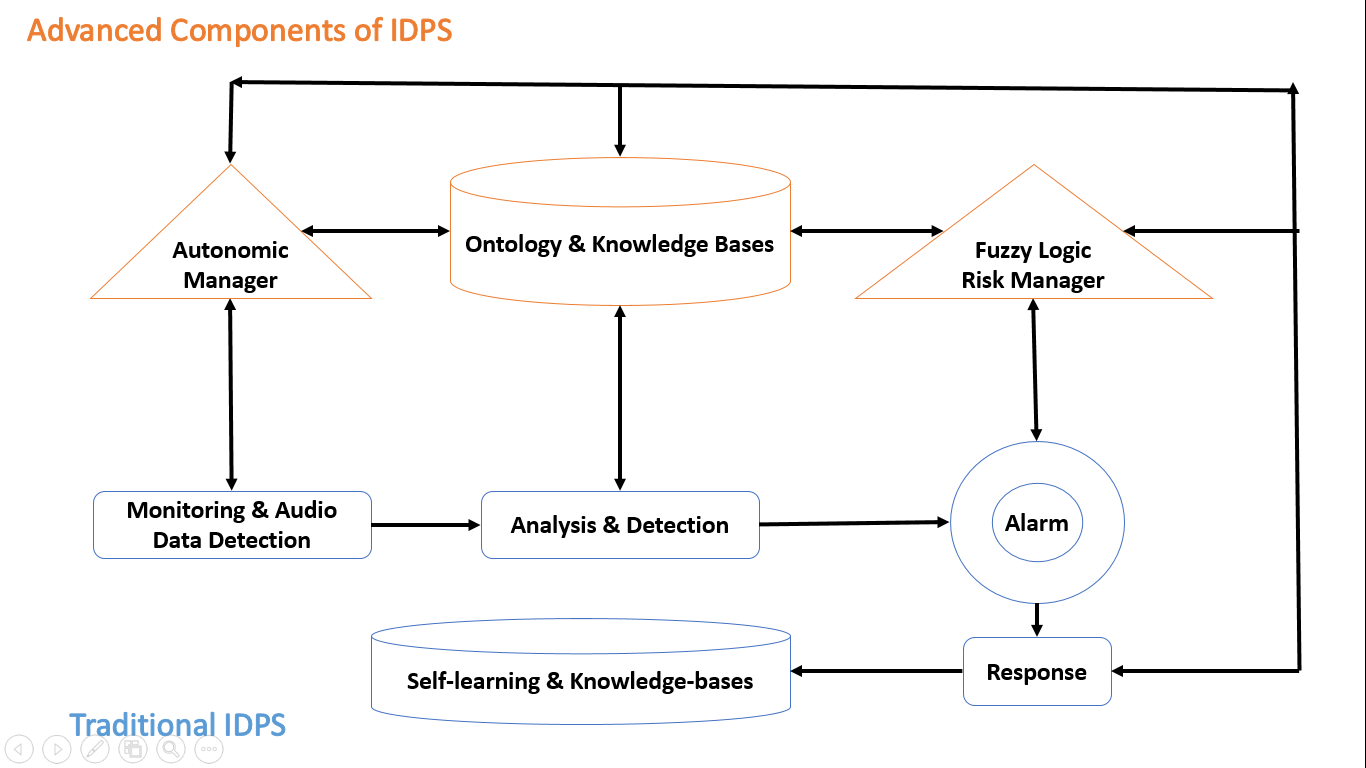






# Intrusion Detection and Prevention Systems (IDPS)

IDPS components, including sensors (alarm), event databases, and management consoles must integrate with a network-wide monitoring capability.



# REFERENCES

* <https://www.tatvasoft.com/blog/top-12-software-development-methodologies-and-its-advantages-disadvantages/#anchor1>
* <https://www.7sec.com/blog/the-purpose-of-intrusion-detection-and-prevention-systems/>
* <https://link.springer.com/chapter/10.1007/978-3-642-35197-6_29>
* <https://www.slideshare.net/MahendarReddy1/nids-ppt>
* <https://www.slideshare.net/raghavbisht9/intrusion-detection-system-project-report>

GITHUB

* Saaransh Sharma – <http://github.com/500069713webscope>
* Varun Gupta – <http://github.com/500066119webscope>