3 Design

Members:

- **Alex Nicolellis**
- **Jung Ho Suh**
- **Muhamed Stilic**
- **Pallavi Santhosh**

3.1 Design Context

3.1.1 Broader Context

Describe the broader context in which your design problem is situated. What communities are you designing for? What communities are affected by your design? What societal needs does your project address?

List relevant considerations related to your project in each of the following areas:

Area	Description	Examples
Public health, safety, and welfare	**How does your project affect the general well-being of various stakeholder groups? These groups may be direct users or may be indirectly affected (e.g., solution is implemented in their communities)**	Hardening the security in the power grid increases the well-being of the users by securing constant power flow. Detecting the anomaly in the power grid to find out potential cyber threat in the early stage is critical to ensure the users private data such as electricity usage. Reducing the risk of cyber attack that could take down the entire power grid, unabling electricity.
Global, cultural, and social	**How well does your project reflect the values, practices, and aims of the cultural groups it affects? Groups may include but are not limited to specific communities, nations, professions, workplaces, and ethnic cultures.**	Proper security is a necessary value of any company, especially for those that heavily use computing resources. Our project provides useful security measures that help an energy company uphold this value. This project indirectly supports renewable energy systems by protecting a system of solar panels. Supporting alternative energy sources is a goal of many cultures in the modern world.

Environmental	**What environmental impact might your project have? This can include indirect effects, such as deforestation or unsustainable practices related to materials manufacture or procurement.**	Our project serves to support a renewable energy source, which provides a comparatively better environmental impact than traditional energy sources. The computing resources of our project consume energy, but that cost should be offset by the protection it grants to the solar panel system.
Economic	**What economic impact might your project have? This can include the financial viability of your product within your team or company, cost to consumers, or broader economic effects on communities, markets, nations, and other groups.**	Our project has a major impact on consumers due to the fact they can regulate their own power. If people tamper with power grids systems there could be loss of service and could increase in price for consumers, so our project is here to mitigate those errors.

3.1.2 User Needs

List each of your user groups. For each user group, list a needs statement in the form of:

User group needs (a way to) do something (i.e., a task to accomplish, a practice to implement, a way to be) because some insight or detail about the user group.

Group: Power-Grid Employees

- Need a way to monitor the entire power grid.
- Need a way to track down the anomalic node to interfere.
- Need a way to communicate with each DER to get the detailed information.
- Need a way to update DER's policy and software remotely.

Group: IDS Algorithm Developers

- Need a way to fix bugs in code
- Need a way to check for logs
- Need a way to run tests

3.1.3 Prior Work/Solutions

Include relevant background/literature review for the project

– If similar products exist in the market, describe what has already been done

– If you are following previous work, cite that and discuss the **advantages/shortcomings**

– Note that while you are not expected to "compete" with other existing products / research groups, you should be able to differentiate your project from what is available. Thus, provide a list of pros and cons of your target solution compared to all other related products/systems.

Detail any similar products or research done on this topic previously. Please cite your sources and include them in your references. All figures must be captioned and referenced in your text.

Background work:

Mirheidari et al: Alert Correlation Algorithms: A Survey and Taxonomy

- This work lists the primary challenges of an anomaly detection algorithm and a categorization and comparison of various types of algorithms, notably including machine learning.

Zang et al: A Survey of Alert Fusion Techniques for Security Incident

- This work describes the process of alert correlation step-by-step.

Sadoddin, Ghorbani: Alert Correlation Survey: Framework and Techniques

- In addition to explaining the process of alert correlation, this paper goes into detail about different alert correlation algorithms and identification of false positives.

Previous work:

- Using RED (Reconstruction Error Distribution) and HPCs (Hardware Performance Counters) to detect and protect against cyber attacks and issues in the power grid.Focuses on zero-day attacks to prevent against previously undetected gaps in security an attacker may use to shut down the system (He et al., 2019)
- Analyzes the restrictions on detection methods for anomalies that electricity suppliers have to deal with. Focuses on cloud computing and prevention of internalized errors such as design flaws rather than external infiltrators. (Feng et al., 2020)
- Uses Micro-MPUs to better detect anomalies in power grid security as well as expand on the type of anomalies being detected. Additionally, they used this new algorithm to increase the speed and accuracy of detection with phasor measurement. (Chamie et al., 2018)
- This is last year's paper written by our clients about their work to design the system of sensors we will be creating a master control for. (Ravikumar et al., 2021)

3.1.4 Technical Complexity

Provide evidence that your project is of sufficient technical complexity. Use the following metric or argue for one of your own. Justify your statements (e.g., list the components/subsystems and describe the applicable scientific, mathematical, or engineering principles)

1. The design consists of multiple components/subsystems that each utilize distinct scientific, mathematical, or engineering principles –AND–
2. The problem scope contains multiple challenging requirements that match or exceed current solutions or industry standards.

3. The design consists of multiple layers of components. Intrusion Detection System, machine learning algorithm, establishing stable relationships between the IDS master and sensors(nodes), and utilizing cloud computing to calculate the data.

4. The problem scope exceeds the solutions because we will be using anomaly detection systems using machine learning algorithms, not only utilizing existing cyber-attack databases. With that said, we must match multiple requirements that must protect the users safety and be able to function on its own with no errors.

3.2 Design Exploration

3.2.1 Design Decisions

List key design decisions (at least three) that you have made or will need to make in relation to your proposed solution. These can include, but are not limited to, materials, subsystems, physical components, sensors/chips/devices, physical layout, features, etc.

1. Must use AWS-Cloud for cloud computing.
2. Must use 4 VM's(ATTACKER,TARGET,SNORT,SECURITY ONION).
3. Must use a Machine Learning Algorithm.
4. Must use an appropriate visual aid for the frontend.

3.2.2 Ideation

For one design decision, describe how you ideated or identified potential options (e.g., lotus blossom technique). List at least five options that you considered.

The design we chose:

Must use a machine learning algorithm

Identification method:

Lotus blossom technique

The options we considered:

Alert correlation classifications: Similarity-based (sim), Knowledge-based (K), Statistical-based (stat)

Sub-classifications:

1. Simple rules (sim)
2. Hierarchical rules (sim)
3. Scenario (K)
4. Casual Relationship Estimation (stat)
5. Statistical Traffic Estimation (stat)

3.2.3 Decision-Making and Trade-Off

Demonstrate the process you used to identify the pros and cons or trade-offs between each of your ideated options. You may wish to include a weighted decision matrix or other relevant tool. Describe the option you chose and why you chose it.

Weighted Decision Matrix:

H- High A- Average L - Low	Accuracy	Flexibility	Extendability	Required Memory	Computation Power	Parallelizing
Machine Learning	A	A	A	A	A	A
Simple Rules	A	H	H	A	A	H
Hierarchical Rules	A	H	H	A	A	H
Scenario	H	H	H	A	A	L
Casual Relationship Estimation	A	L	L	A	A	H
Statistical Traffic Estimation	A	H	A	L	H	H

We chose Machine Learning(decision-tree) over the other ideates due to the fact it matches our requirements perfectly. Machine Learning uses multi-step clustering to detect alreats and attack sequences. We can use a certain set of examples for the system to comprehend the types of alerts that will occur. That way the algorithm can find a relationship between the attacks and not create false positives. The other ideas may have a bit better weight than the Machine Learning algorithm, but they don't match our requirements.

3.3 Proposed Design

Discuss what you have done so far – what have you tried/implemented/tested?

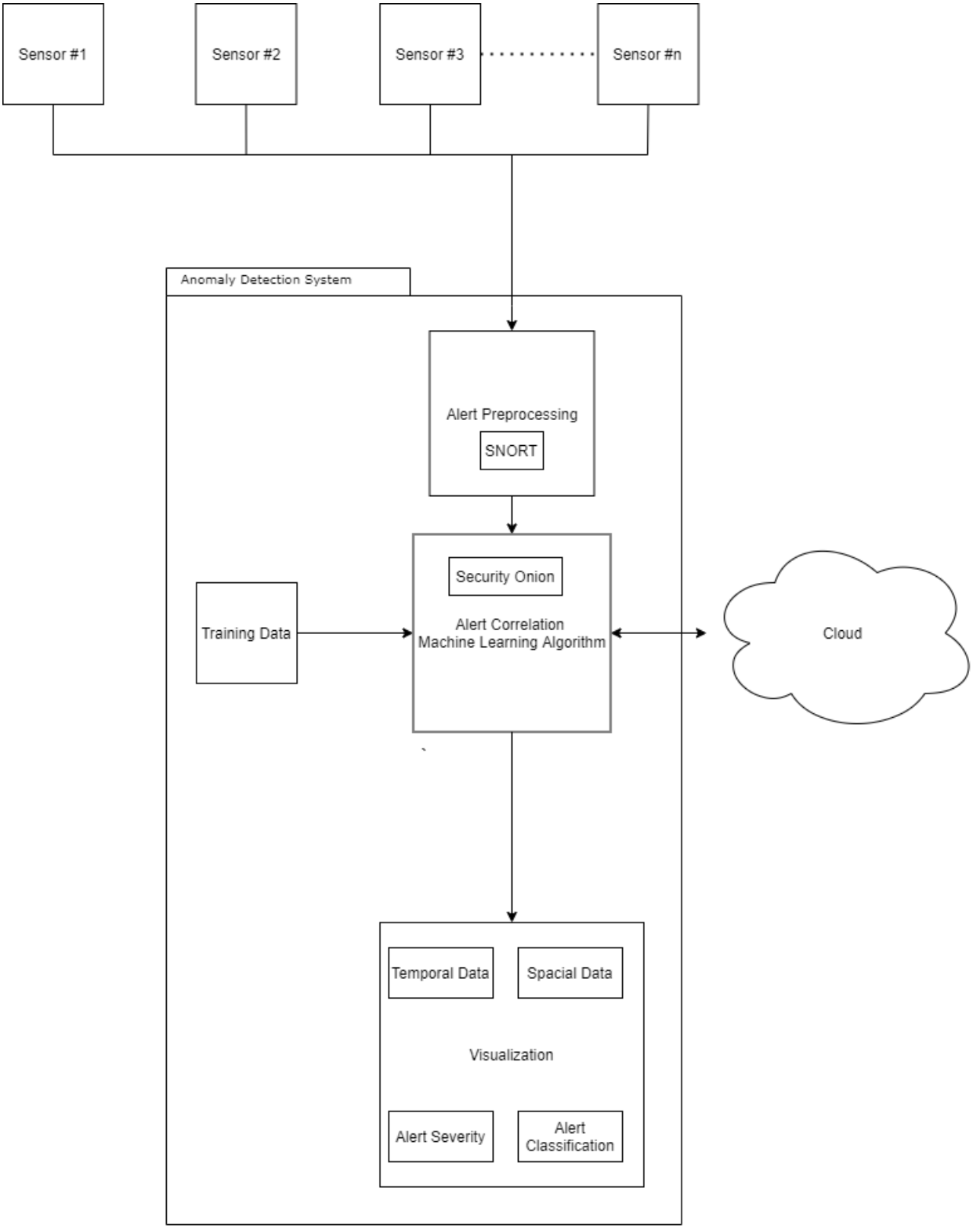
So far we have implemented 4 virtual machines, attacker, IDS master, victim, IDS Sensor. Attacker using Kali VM, victim using Windows, IDS master and sensor using Ubuntu for Security Onion.

3.3.1 Design Visual and Description

Include a visual depiction of your current design. Different visual types may be relevant to different types of projects. You may include: a block diagram of individual components or subsystems and their interconnections, a circuit diagram, a sketch of physical components and their operation, etc.

Describe your current design, referencing the visual. This design description should be in sufficient detail that another team of engineers can look through it and implement it.

BLOCK DIAGRAM:



Description:

Our design accepts many alerts as input, originating from a variety of sensors. These alerts will be processed, ensuring that they enter the alert correlation algorithm with a uniform format and contain all the necessary information (time, location, type) for future analysis. Then, our algorithm will perform correlation on the alerts via the Cloud. Our machine learning model will be trained by a dataset to draw relationships between alerts. The conclusions will then be presented to users through a variety of visualizations, allowing alerts to be filtered by time, space, type, and severity.

3.3.2 Functionality

Describe how your design is intended to operate in its user and/or real-world context. This description can be supplemented by a visual, such as a timeline, storyboard, or sketch.

Our design is intended to work by controlling and monitoring the sensor network already built by our client. It will analyze information collected by the sensors and check for any false positive alerts completely autonomously.

How well does the current design satisfy functional and non-functional requirements?

Currently, the design satisfies the non-functional requirements decently, but needs to further develop for the functional requirements. As we are still in our Sprint 2, we have not yet begun implementing anything for the project and are still working on research. Because of this we haven't had the opportunity to test our design and see how well it fits the functional requirements and what needs to be done to improve or adapt it.

Visual: Our design is intended to monitor & control a set of sensors. This design satisfies the functional requirements by having good visualization of log results for easy analysis. This design satisfies the non-functional requirements by being accessible and having a strong user interface.

3.3.3 Areas of Concern and Development

Based on your current design, what are your primary concerns for delivering a product/system that addresses requirements and meets user and client needs?

Our primary concern for the system is that it needs many functions to develop. It has to gather all alerts, filter the duplicate, flag the important one, create an automated analysis of attack using machine learning, give the visualized result to the user such as graph to assist analysis, and communicate with the nodes to fetch detailed information and update firmware/software. We may not have enough time to build the whole environment.

What are your immediate plans for developing the solution to address those concerns? What questions do you have for clients, TAs, and faculty advisers?

For the solution, we are using an existing Intrusion detection system such as Snort to help implement the Anomaly Detection System. Snort already has the basic structure of IDS so we can use it and add the machine learning algorithm to fit our needs.

Our immediate plans are to install SecurityOnion to get a more well-rounded view of the technology we are using and how it works. Our current questions are how to install SecurityOnion on our virtual machine because most of the examples we have researched describe how to install it on a new one.

NOTE: The following sections will be included in your final design document but do not need to be completed for the current assignment. They are included for your reference. If you have ideas for these sections, they can also be discussed with your TA and/or faculty adviser.

3.4 Technology Considerations

Highlight the strengths, weaknesses, and trade-offs made in technology available.

Discuss possible solutions and design alternatives

Our strengths in the available technologies are vsphere virtual machines and aws. Our weaknesses in the available technologies are old operating systems/applications. The tradeoffs we can make in the available technologies is that the vm's run fast but on old operating systems..

Our alternatives designs and solutions are to...

3.5 Design Analysis

- Did your proposed design from 3.3 work? Why or why not?
- What are your observations, thoughts, and ideas to modify or iterate over the design?

Our proposed design DID/DIDN'T work. It worked because..

We have observed... We should change....

3.6 Design Plan

Describe a design plan with respect to use-cases within the context of requirements, modules in your design (dependency/concurrency of modules through a module diagram, interfaces, architectural overview), module constraints tied to requirements.

References

Chamie, M. E., Lore, K. G., Shila, D. M., & S, A. (2018, July 31). *Physics-based features for anomaly detection in power grids with Micro-PMUs*. IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8423024

Feng, L., Xu, S., Zhang, L., Wu, J., Chu, J., Wang, Z., & Shi, H. (2020, October 7). *Anomaly detection for electricity consumption in cloud computing: Framework, methods, applications, and challenges*. Springer Open. https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-020-01807-0

He, Z., Raghavan, A., Hu, G., Chai, S., & Lee, R. (2019, June 23). *Power-Grid Controller Anomaly Detection with Enhanced Temporal Deep Learning*. arXiv.org e-Print archive. https://arxiv.org/pdf/1806.06496.pdf

Ravikumar, G., Singh, A., Babu, J. R., Abdelkhalek, M. M., & Govindarasu, M. (2021, September 16). *D-IDS for cyber-physical DER Modbus system - Architecture, modeling, testbed-based evaluation*. IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9241259