**COMSATS University Islamabad,   
Abbottabad Campus**

**Project Proposal   
(SCOPE DOCUMENT)**

**For**

**IoT-Based Honeypot Network for Cybersecurity Threat Detection and Attack Analysis**  
Version 1.0

***By***

**Salim CIIT/FA21-BCS-193/ATD**

**Zakirullah Salar CIIT/FA21-BCS-186/ATD**

**Mohammad Zahid Rahmat CIIT/FA21-BCS-222/ATD**

***Supervisor*Sayed Shahab Zarin**

***Bachelor of Science in Computer Science (2021-2025)***

|  |  |  |
| --- | --- | --- |
| **No.** | **Comment** | **Action** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**SCOPE DOCUMENT REVSION HISTORY**

**Supervisor Signature**

**Date:**

**Table of Contents**

**1.** **Introduction 4**

**2.** **Problem Statement 5**

**3.** **Problem Solution for Proposed System 5**

**4.** **Related System Analysis/Literature Review 5**

**5.** **Advantages/Benefits of Proposed System 5**

**6.** **Scope 6**

**7.** **Modules 6**

7.1 Module 1: Module Name 6

7.2 Module 2: Module Name 6

**8.** **System Limitations/Constraints 6**

**9.** **Software Process Methodology 6**

**10.** **Tools and Technologies 7**

**11.** **Project Stakeholders and Roles 7**

**12.** **Team Members Individual Tasks/Work Division 8**

**13.** **Data Gathering Approach 8**

**14.** **Concepts 8**

**15.** **Gantt chart 9**

**16.** **Mockups 10**

**17.** **Conclusion 11**

**18.** **References 11**

**19.** **Plaragism Report 11**

**Project Category: (**Select all the major domains of proposed project**)**

* **A-**Desktop Application/Information System **B-**Web Application/Web Application based Information System **C-** Problem Solving and Artificial Intelligence ** D-**Simulation and Modeling ** E-** Smartphone Application ** F-** Smartphone Game ** G-** Networks ** H-** Image Processing****Other (specify category) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Abstract**

As more devices connect to the internet, like smart home gadgets and other IoT (Internet of Things) devices, they become targets for hackers. Many of these devices have weak security, making them easy for attackers to exploit. Our project is about building an IoT-based honeypot network, which acts like a "trap" by imitating real IoT devices. This setup attracts attackers, allowing us to safely observe their actions and understand their methods.

By monitoring these fake devices, we can collect useful information on the types of attacks and techniques hackers use. This data will help us understand common threats to IoT devices, which could lead to better security solutions in the future. Our project will also include tools for real-time monitoring and data visualization, making it easier to analyze and learn from the attacks. In short, this project aims to improve cybersecurity by studying attacks on IoT devices.

**Introduction**

Our project, "IoT-Based Honeypot Network for Cybersecurity Threat Detection and Attack Analysis," is about building a special network that will help us study how hackers target IoT devices. With the growing use of IoT devices like smart home cameras, thermostats, and routers, these devices have become a popular target for cyberattacks. Unfortunately, many of these devices lack strong security, which makes them vulnerable to unauthorized access, data theft, malware, and even large-scale attacks like Distributed Denial of Service (DDoS).

This project focuses on creating a honeypot network that simulates various vulnerable IoT devices, such as smart cameras, thermostats, and routers, to attract and log malicious activity. By monitoring and analyzing these interactions, the system aims to provide valuable insights into the tactics, techniques, and procedures (TTPs) commonly used by attackers in IoT environments. Additionally, this project integrates real-time traffic monitoring, anomaly detection, and data visualization to enhance threat detection and support proactive cybersecurity strategies. Ultimately, this honeypot network will contribute significant data to IoT security research, aiding in the development of more effective defenses and preventive security measures for the IoT ecosystem.

**Problem Statement**

IoT devices, such as smart cameras, routers, and sensors, are often built with basic security, which makes them easy targets for cyberattacks like unauthorized access, malware infections, and botnet involvement. While there are some IoT honeypots designed to attract attackers, they typically focus on specific protocols or offer low interaction, limiting their ability to capture a full range of attacker behaviours. Our project seeks to create a more advanced IoT honeypot network that simulates various vulnerable IoT devices, supports multiple protocols (like HTTP, Telnet, MQTT, and SSH), and includes real-time monitoring and data visualization. This setup will help capture and analyze attack patterns, providing valuable insights into IoT security threats and contributing to stronger defences for IoT systems.

**Problem Solution for Proposed System**

Our proposed system aims to improve IoT security by setting up a honeypot network that looks like real, vulnerable IoT devices. This network is designed to attract and record cyberattacks, giving us a better understanding of how attackers target IoT devices. It will simulate common IoT protocols, like HTTP, Telnet, MQTT, and SSH—protocols that attackers often try to exploit. By mimicking these protocols, the system can capture a wide variety of attacks, helping us learn about the tactics and methods used by hackers.

The data collected from these attacks is stored in real time, allowing for ongoing monitoring and analysis. We’ll use visualization tools to show trends in the data, so cybersecurity experts can easily see patterns, spot high-risk areas, and respond quickly. This setup will help reveal specific weaknesses that attackers frequently exploit, making it easier to plan effective defenses. Additionally, we’ll use machine learning models to categorize different attack types and detect unusual behavior, giving us a better chance to identify potential threats before they can do serious harm.

**Related System Analysis/Literature Review**

**Related System Analysis/Literature Review**

1. **Cowrie**  
   Cowrie is a honeypot that interacts with attackers through SSH and Telnet, capturing their actions and logging everything from commands to file transfers. It’s effective for studying attacks over these specific protocols, but it has a limited focus, primarily targeting SSH and Telnet threats. This means it may miss other types of attacks common in IoT environments. Additionally, Cowrie can be demanding on system resources, which makes it less practical for deployment on low-power IoT devices.
2. **Dionaea**  
   Dionaea is a honeypot that tries to attract and capture malware by simulating vulnerable services, allowing analysts to collect malware samples for further study. However, it has limited compatibility with IoT protocols, which can reduce its usefulness in an IoT-focused setting. Another challenge with Dionaea is that it generates a lot of data, which can be overwhelming to manage and analyze effectively.
3. **IoT-Honeypot**  
   IoT-Honeypot is a honeypot designed specifically for IoT devices, supporting protocols like MQTT and CoAP to attract and record attacks on IoT systems. While it’s effective in simulating IoT vulnerabilities, it doesn’t cover all possible IoT protocols, which can limit the range of threats it captures. Additionally, it lacks advanced analytics features, making it harder to gain in-depth insights from the data collected. Setting up IoT-Honeypot can also require considerable networking knowledge, which might make it less accessible for users without technical experience.

**Table 1 Related System Analysis with proposed project solution**

|  |  |  |
| --- | --- | --- |
| **Application Name** | **Weakness** | **Proposed Project Solution** |
| Cowrie | |  | | --- | |  |  |  | | --- | | Cowrie mainly focuses on SSH and Telnet attacks and can use too many resources, making it hard to run on smaller IoT devices. | | We will create a flexible honeypot that can handle different protocols important for IoT and is designed to work efficiently on low-powered devices. |
| Dionaea | Dionaea struggles with connecting to IoT devices and has issues managing large amounts of data. | Our solution will be an easy-to-use honeypot system that improves data collection and management while supporting a wider range of IoT protocols. |
| IoT-Honeypot | IoT-Honeypot might not support all IoT protocols and lacks strong analytics features. | We aim to develop a complete honeypot that not only captures and analyzes attacks on various IoT protocols but also offers detailed analytics and insights into IoT security threats. |

**Advantages/Benefits of Proposed System**

Advantages of the system is mentioned as follow:

1. **Better Detection of IoT Attacks**: Our system enhances the ability to spot attacks and malware specifically targeting IoT devices, helping to safeguard critical assets.
2. **Real-Time Attack Visualization**: With instant visuals of attack data, users can quickly understand what's happening and respond right away, making security management much more effective.
3. **Insights into Attacker Behavior**: We provide valuable information about how attackers operate, which is essential for advancing IoT security research and helping everyone in the community stay safer.
4. **Development of Effective Defense Strategies**: By identifying specific threats, our system supports the creation of targeted defense strategies that are more effective against IoT vulnerabilities.
5. **Predictive Analysis with Machine Learning**: Leveraging machine learning, we can predict potential threats and spot unusual behavior, giving users an edge in proactive security.
6. **A Safer IoT Ecosystem**: By identifying vulnerabilities before they can be exploited, our solution contributes to building a safer IoT environment for everyone.
7. **Scalable Architecture**: Our flexible system can easily simulate various IoT devices and scenarios, allowing users to test and prepare for a wide range of real-world situations.

**Scope**

This project aims to create an IoT-Based Honeypot Network to improve how we detect and analyze attacks on Internet of Things (IoT) devices. Here’s what we plan to do and what we won’t do:

#### Do's:

* **Simulate IoT Communication**: The system will mimic various IoT communication methods like MQTT, CoAP, and HTTP to attract a wide range of cyberattacks.
* **Real-Time Attack Visualization**: We will provide live visuals of attack data, helping users understand and respond to security threats as they happen.
* **Use Machine Learning**: The project will use machine learning techniques for predicting potential issues and detecting unusual behaviour, making it easier to spot vulnerabilities.
* **User-Friendly Web Application**: We will create an easy-to-use web application so that users of all skill levels can access monitoring and analysis features without difficulty.
* **Gather Insights on Attacker Behaviour**: The system will collect valuable information about how attackers operate, supporting ongoing IoT security research and helping to develop better defense strategies.

#### Don'ts:

* **No Mobile App Development**: We will not create mobile applications for Android or iOS platforms.
* **No Physical Hardware Provided**: We won't provide any physical devices for capturing attacks; the honeypot will operate in a controlled, simulated environment.
* **Focus on IoT Only**: Our focus will be strictly on IoT devices and their protocols, so we won’t analyze cyber threats that don’t relate to IoT.
* **No Real-Time Response Actions**: The honeypot will not actively counteract attacks but will focus on collecting data for analysis and research.
* **No Analysis of Non-IoT Protocols**: We won’t analyze or simulate attacks on protocols that are not specifically used in IoT environments.

**Modules**

This system consists of three main parts: the IoT Protocol Simulation Module, the Attack Monitoring Module, and the Machine Learning Analysis Module. Each part has smaller sections that help carry out various tasks.

#### Module 1: IoT Protocol Simulation Module

This module simulates different IoT communication methods to attract and analyze cyberattacks.

* **Sub-Module 1: Protocol Configuration**  
  This section sets up various IoT protocols, like MQTT and CoAP, to create an effective honeypot environment.
* **Sub-Module 2: Traffic Generation**  
  this part generates fake traffic patterns that mimic real IoT device interactions, making the honeypot more realistic.
* **Sub-Module 3: Vulnerability Simulation**  
  This section simulates known weaknesses within these protocols to draw in potential attackers and gather information on their methods.
* **Sub-Module 4: Logging Interactions**  
  This part logs all interactions and attack attempts, which is important for later analysis and reporting.

#### Module 2: Attack Monitoring Module

This module focuses on collecting and displaying data about attacks captured by the honeypot.

* **Sub-Module 1: Attack Data Collection**  
  This section collects detailed logs of all attack interactions, including timestamps, types of attacks, and source IP addresses.
* **Sub-Module 2: Real-Time Dashboard**  
  this provides a user-friendly interface that shows attack metrics and alerts users to ongoing incidents.
* **Sub-Module 3: Incident Alerts**  
  this section generates alerts for serious attack incidents, notifying users to take immediate action.
* **Sub-Module 4: Historical Data Access**  
  this allows users to view past attack data for trend analysis and research.

#### Module 3: Machine Learning Analysis Module

This module uses machine learning to analyze attack data and improve detection abilities.

* **Sub-Module 1: Anomaly Detection Algorithms**  
  This part implements machine learning to spot unusual patterns in attack data that could indicate new threats.
* **Sub-Module 2: Predictive Analysis**  
  this section uses past data to predict potential future attack methods, helping the honeypot be better prepared for threats.
* **Sub-Module 3: Model Training and Testing**  
  this conducts training and testing of machine learning models to ensure they accurately detect threats.
* **Sub-Module 4: Integration with Monitoring Module**  
  This part connects the findings from the machine learning analysis with the Attack Monitoring Module for real-time threat assessment.

### Explanation of a Module

The **IoT Protocol Simulation Module** is crucial for creating a realistic environment to attract and analyze cyberattacks on IoT devices. This module includes several sections, such as Protocol Configuration, which sets up the different IoT communication methods, and Traffic Generation, which simulates real interactions with these protocols. The Vulnerability Simulation section is important because it mimics known weaknesses, encouraging attackers to engage with the honeypot. Finally, the Logging Interactions section captures all the data from these interactions, allowing for a thorough analysis of attack methods and patterns. Overall, this module is key to understanding the nature of threats against IoT environments and helps in developing effective defense strategies.

**System Limitations/Constraints**

The system and its modules will have the following limitations and constraints:

* **Focus on Specific IoT Protocols**: The honeypot is designed to target certain IoT protocols, which means it may not capture every possible type of attack that could affect other systems or protocols.
* **Dependence on Network Stability**: For the system to work well, it needs a stable and reliable network environment. Any interruptions in the network could affect performance and disrupt data collection.
* **Client-Server Model Delays**: The architecture will use a client-server model, which might lead to some delays in processing data and monitoring attacks in real-time, especially if the server is handling a lot of traffic.
* **Limited Data Parameters**: The data collected by the honeypot will be restricted to specific parameters, which might limit how much we can learn about attack patterns that could occur in a broader context.
* **Not a Complete Defense**: While the honeypot aims to identify and analyze attacks on IoT devices, it won't provide full protection against all types of cyber threats. Its primary goal is to understand and mitigate risks relevant to IoT environments.

**Software Process Methodology**

For the development of the IoT-Based Honeypot Network project, we will adopt the **Object-Oriented Methodology**. This approach is ideal for our project as it allows for modularity and reuse of code, which is essential given the multiple components involved, such as the attack monitoring and data analysis modules. By using object-oriented programming, we can create distinct classes for each aspect of the system, making it easier to manage and maintain. This methodology also aligns well with our team's expertise, as it supports the use of modern programming languages and frameworks that facilitate the development of complex simulations and integrations. Overall, this choice enhances our ability to build a scalable and efficient system while allowing for future enhancements as our project evolves.

**Tools and Technologies**

Mention all the hardware/software tools and technologies with version number which will be used in implementation of the project. Write about the APIs, language(s), SDK(s) etc. which you will use for implementation.

Example:

**Table 2Tools and Technologies for Proposed Project**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tools**  **And**  **Technologies** | **Tools** | **Version** | **Rationale** |
| Visual Studio | 2019 | IDE |
| PyCharm | 2021 | IDE |
| MySQL | 8.0 | DBMS |
| MongoDB | 4.4 | DBMS |
| MS Word | 2019 | Documentation |
| MS Power Point | 2019 | Presentation |
| Anaconda | Latest | IDE |
| **Technology** | **Version** | **Rationale** |
| Python | 3.9 | Machine learning model development |
| Wireshark | Latest | Network Monitoring |
| tcpdump | Latest | Network Monitoring |
| Cowrie | Latest | Honeypot Framework |
| Node.js | Latest | Backend server for dashboard |
| TensorFlow | 2.6 | Machine learning library |
| Elasticsearch and Kibana | 7.x | Data storage and visualization |
|  | NumPy | 1.19 | Machine learning library |
|  | Pandas | 1.2 | Machine learning library |
|  | Wireshark | 3.4 | Network traffic monitoring |
|  | Kali Linux | Latest | Honeypot and penetration testing |
|  | Virtual Box/VMware | Latest | Virtualization of IoT honeypots |
|  | Mosquitto | 2.0 | IoT Frameworks |
|  | Eclipse IoT | 0.11 | IoT Frameworks |

**Project Stakeholders and Roles**

Write down the project stakeholders and their roles.

**Table 3 Project Stakeholders for Proposed Project**

|  |  |
| --- | --- |
| **Stakeholder** | **Role** |
| COMSATS University, Islamabad | Project Sponsor |
| Salim | Cybersecurity Analysis and Machine Learning |
| Zakirullah Salar | Network Configuration, Honeypot Setup |
| M Zahid Rahmat | Web Dashboard and Data Visualization |
| Mr. Sayed Shahab Zarin | Oversees the project, provides guidance, and evaluates progress. |
| Final Year Project Committee | Evaluates the project and provides feedback during presentations and assessments. |

**Team Members Individual Tasks/Work Division**

**Table 4Team Member Work Division for Proposed Project**

|  |  |  |
| --- | --- | --- |
| **Student Name** | **Student Registration Number** | Responsibility/Modules |
| Salim | FA21-BCS-193 | **Module 3: Machine Learning Analysis** |
| Zakirullah Salar | FA21-BCS-186 | Module 1: IoT Protocol Simulation |
| M Zahid Rahmat | FA21-BCS-222 | **Module 2: Attack Monitoring Module** |

**Data Gathering Approach**

We will collect data in several ways to get a clear picture of attacks on IoT devices:

* **Network Logs from Honeypots**: Our honeypots will keep track of all the interactions and attacks that happen. These logs will help us learn what types of attacks are being targeted at our simulated IoT devices and how attackers behave.
* **Attack Simulations**: We will run tests that simulate attacks using tools like Hydra and Metasploit. These tests will help us see how our honeypot handles different kinds of threats in real-time, allowing us to improve our defenses.
* **Research Data**: We will look at previous studies on IoT honeypots to learn about known attack patterns. This information will help us train our machine learning models to better recognize new threats.
* **User Feedback**: As we develop the project, we will ask users for their thoughts and experiences with our honeypot system. Their feedback will help us improve our data collection and analysis.

**Concepts**

1. **IoT Security**: This involves learning about the weaknesses in Internet of Things (IoT) devices and how honeypots can help spot potential threats. We want to understand what makes these devices vulnerable and how to protect them.
2. **Machine Learning**: We will use machine learning to teach our system how to identify and predict different types of attacks on IoT devices. By training our models, we can improve our ability to recognize threats and respond quickly.
3. **Network Protocols**: We will work with various communication methods, such as MQTT, Telnet, and SSH, to create realistic honeypot simulations. These protocols are essential for making our honeypots mimic real IoT devices and attract attackers.
4. **Threat Intelligence**: This is about sharing information about threats with other cybersecurity groups. By collaborating and exchanging data, we can strengthen our defenses and help others stay safe from attacks.
5. **Honeypots**: Honeypots are fake systems set up to lure attackers. They help us understand attack methods and gather information about threats without risking real devices.
6. **Data Analysis**: We will analyze the data collected from our honeypots to find patterns in attack behavior. This will help us learn more about how attacks happen and how to defend against them.
7. **Incident Response**: This is the process of responding to security incidents. We will develop strategies to quickly deal with attacks when they are detected, minimizing damage and restoring security.
8. **Vulnerability Assessment**: This involves identifying weaknesses in our IoT systems. By regularly checking for vulnerabilities, we can fix them before they are exploited by attackers.
9. **Cybersecurity Best Practices**: We will explore effective methods for keeping IoT devices secure, such as strong passwords, regular updates, and monitoring network traffic.

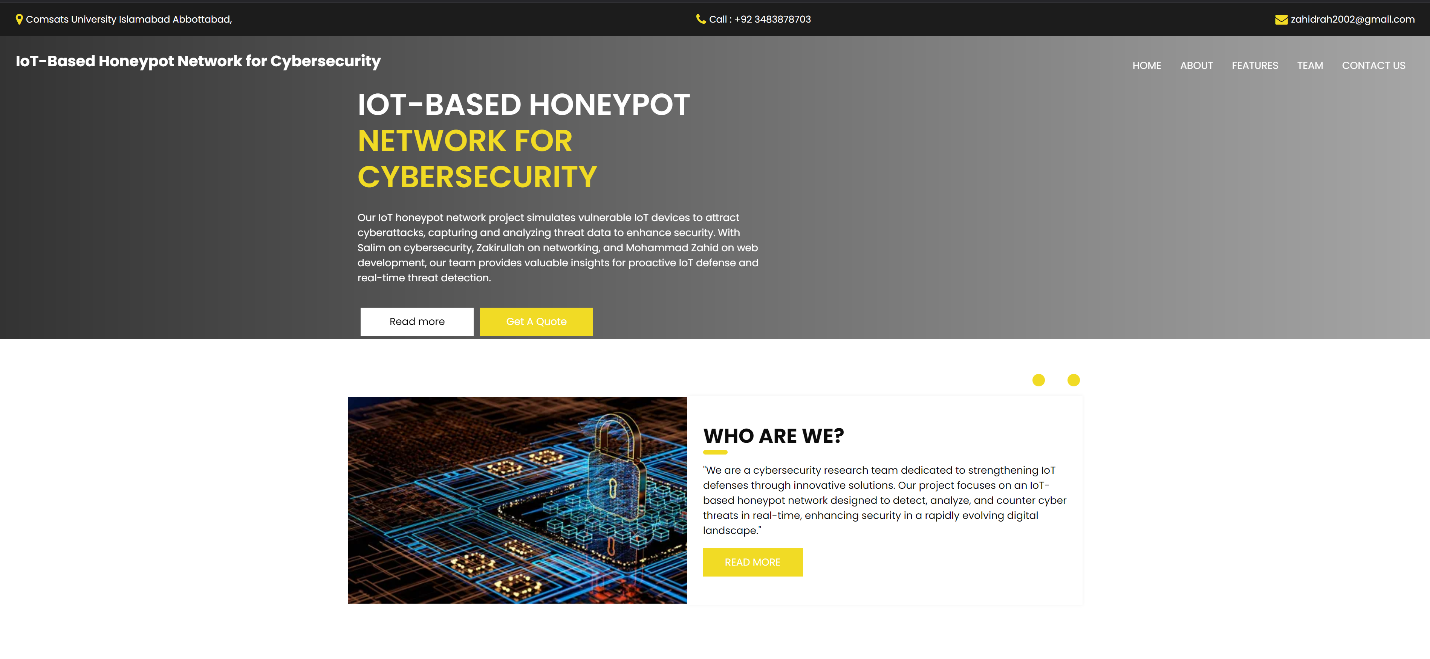
**Gantt chart**

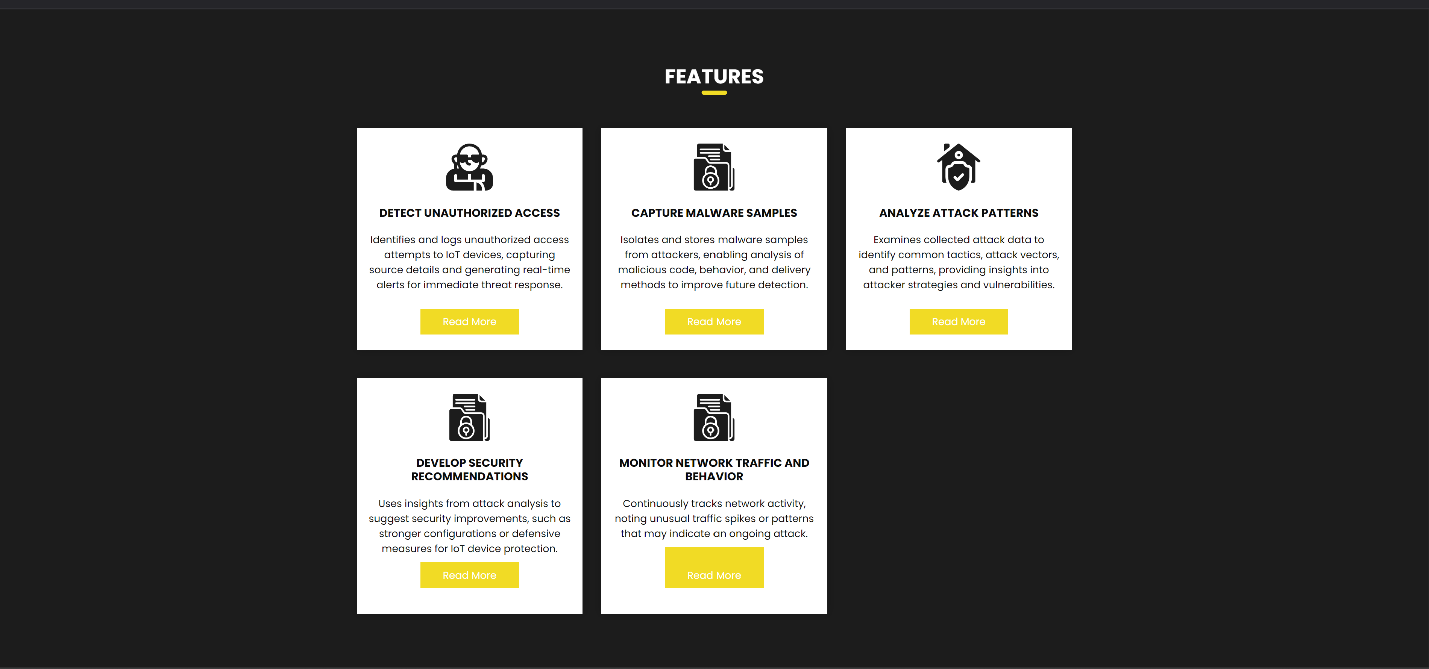
Create the Grant Chart and provide estimated start and end dates of all proposed modules/tasks for each team member. Also identify the dependencies (which tasks cannot be started/completed, until the dependent task is completed). Gantt chart can be created using MS Project.

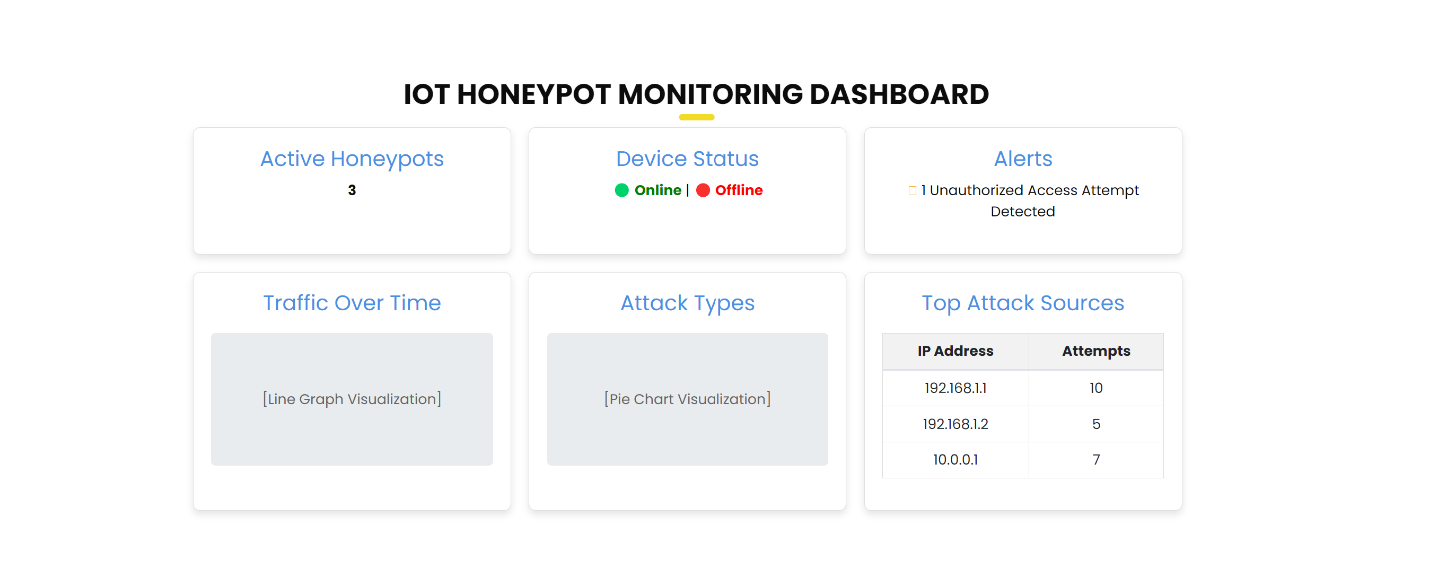
******

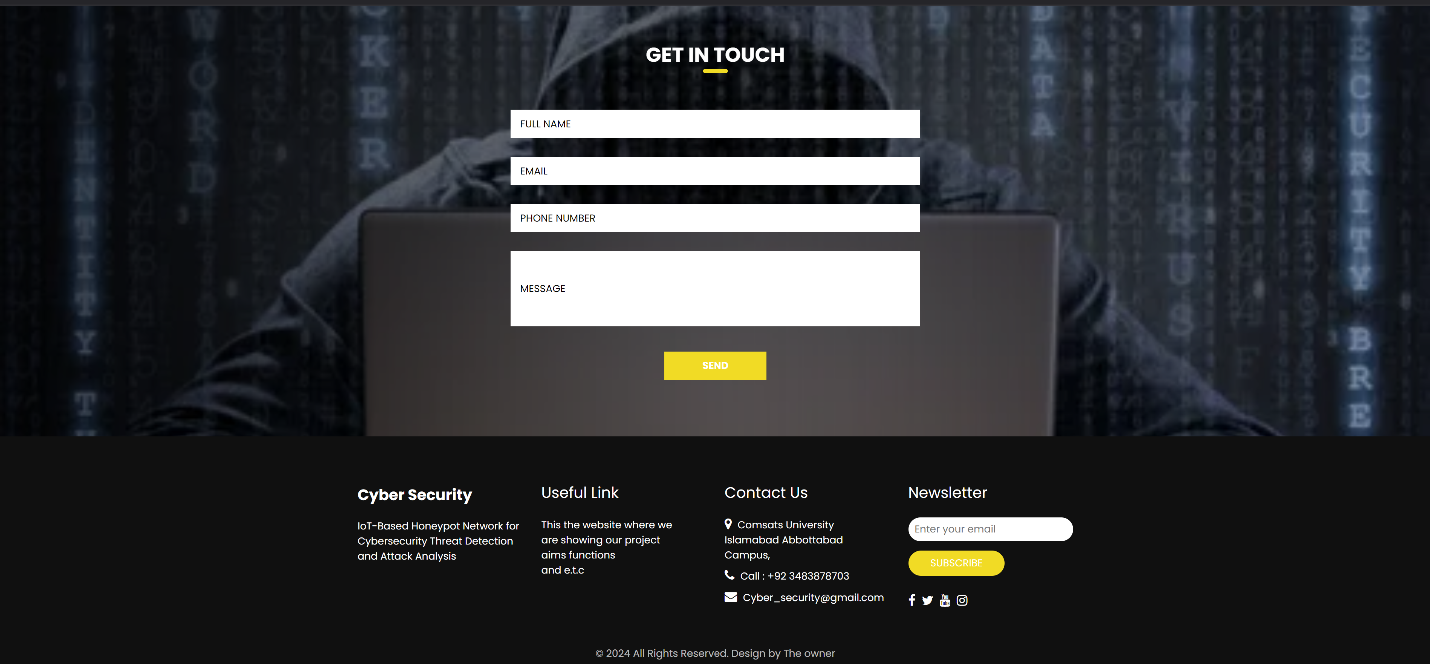
Figure 1Sample Gantt chart

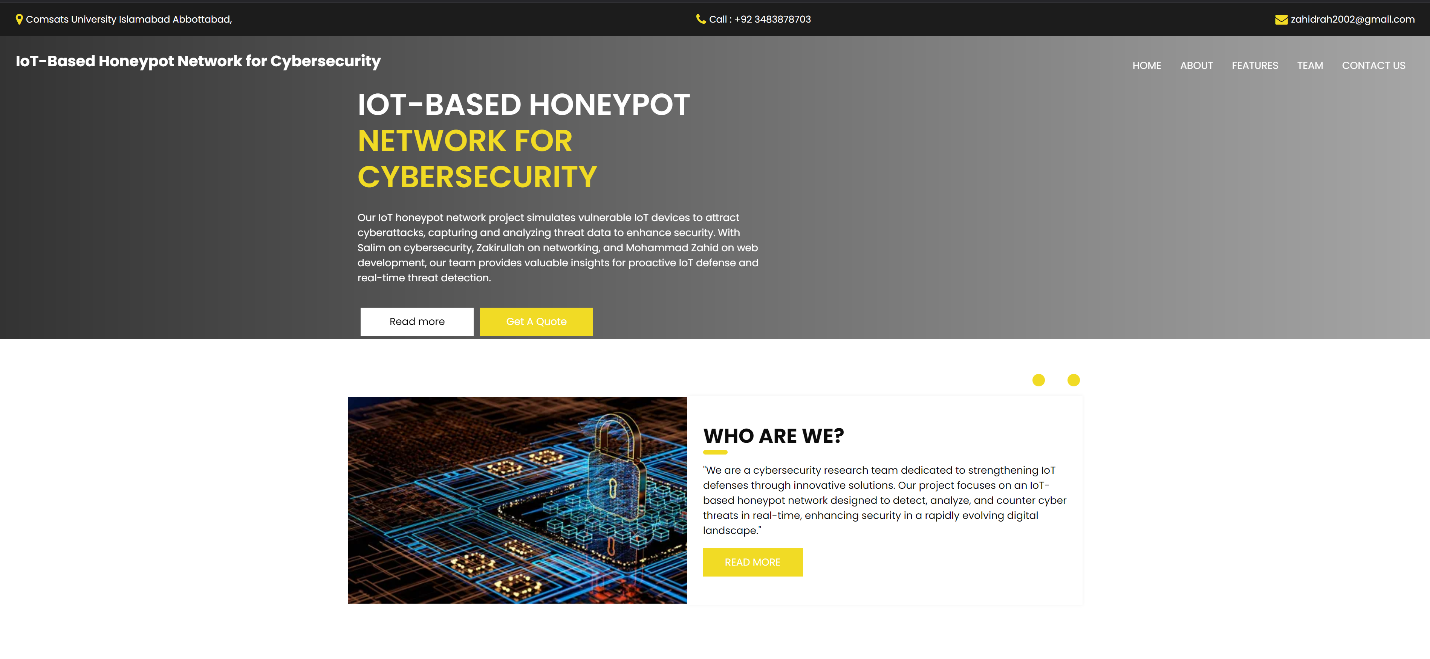
**Mockups**

****

****

****

****



**Conclusion**

This proposal presents an exciting plan to create an IoT-based honeypot network that will help us monitor, analyze, and detect cyber threats aimed at IoT devices. As more devices connect to the internet, keeping them secure is crucial.

By using machine learning and easy-to-understand visuals, our system will track attacks and provide helpful insights into how they work. This information will help us and others in the cybersecurity community build stronger defenses and better strategies to protect IoT devices.

Our goal is to make the digital world safer, allowing IoT technology to grow and improve our lives without constant worry about cyber threats. Together, we can create a future where innovation and safety go hand in hand, ensuring everyone can enjoy the benefits of IoT without fear. Let’s work towards a more secure connected world!

**References**

"Internet of Things: Security and Privacy" by J. D. DeCuir and A. C. O’Donnell

"Honeypots: Tracking Hackers" by Lance James

https://www.iotsecurityfoundation.org

<https://www.kaspersky.com/resource-center/definitions/honeypot>

[https://ieeexplore.ieee.org](https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6488907)

**Plagiarism Report**

Attach the Plagiarism report of your project scope document from library staff of turnitin tool (http://turnitin.com