Problem definition and database design

Cybersecurity is an undeniably growing field where the globe is trying day by day to defend against cyber attacks. Companies often have their own cyber teams and platforms that conduct, run, and provide security measures to their company, information, and sensitive data. Although there are many different kinds of attacks there is often a viable approach to prevent data loss and victimization from different threats. Creating a database of threats and vulnerabilities, as well as their according indicators and possible solutions would be beneficial to many users within the Internet of Things (IOT).

Cyber attacks also come from a variety of different locations. Based on these locations the database may alter its responses and provide solutions that may block out incoming attacks from a specific region or area.

This database should have many different functions. From real-time data it is expected to show the most common cyber attacks and list them from most to least prevalent. It will also include the indicators of each attack, such as an example of what may happen to a user’s device if the device has been impacted by the threat or attack. This information will also include signs of the attack taking place and concurrent themes to watch out for. If a system has been successfully attacked, the database will also, through search, provide clear steps on how to mitigate the attack, recover, and prevent it from happening again in the future. Although there are many packages that provide safety from a variety of cyber attacks, this database will not only include packages, but individual services and products that are trusted to keep the device safe from future attacks.

The database will be capable of conducting distinct queries regarding many different aspects of cyber attacks and security. Some examples of distinct queries are “Display a list of the most common cyber attacks and threats,” “display a solution to a phishing attack,” or “display a preventative measure to DDoS attacks,” and many others.

**Entity Relation diagram**

Diagram

Description automatically generated

Translation of ERD into relational model as relational schemas

The database is a relation that most importantly includes the name of the cyber-attack/threat, which will be used as the primary key. The foreign key would also be the type of cyber attack or threat because its threat actors and services would revolve around what kind of threat the attack is. Its attribute includes its indicators of compromise, how to recover from this attack, how to prevent this specific attack in the future, and its prevalence amongst other forms of attacks. Two other relations include defense suites/services and threat actors. The defense suite relation includes information on solutions to particular threats and services or packages that can provide the proper solutions. Threat actors include attributes such as geographic region, their common attacks, and actions that one may need to take in order to block out incoming attacks from this region.

Identification of Functional Dependencies

In relational database theory, a function dependency is a constraint between two sets of attributes in relation. For example, two attributes that would be included within this project are Indicators of Compromise and Prevalence.