Project Portfolio: Location Intelligence & Cybersecurity 2025

**Introduction**

The dataset provides insights into cybersecurity threats affecting IoT devices across various locations and infrastructure types. It includes geospatial data (latitude, longitude, and elevation), environmental factors (temperature, humidity, rainfall), infrastructure types, and cyberattack records on IoT devices. By analyzing this dataset, we can identify high-risk areas, potential correlations between environmental conditions and cyber threats, and strategies for improving cybersecurity.

**Objective:**

The primary objective of this study is to analyze the relationship between **location intelligence, environmental factors, and cybersecurity threats targeting IoT devices**. The study aims to identify high-risk areas, understand attack patterns, and recommend effective cybersecurity measures based on geospatial and environmental data.

e

**Data Source:**

The data was downloaded from Kaggle.com and was loaded into Excel.

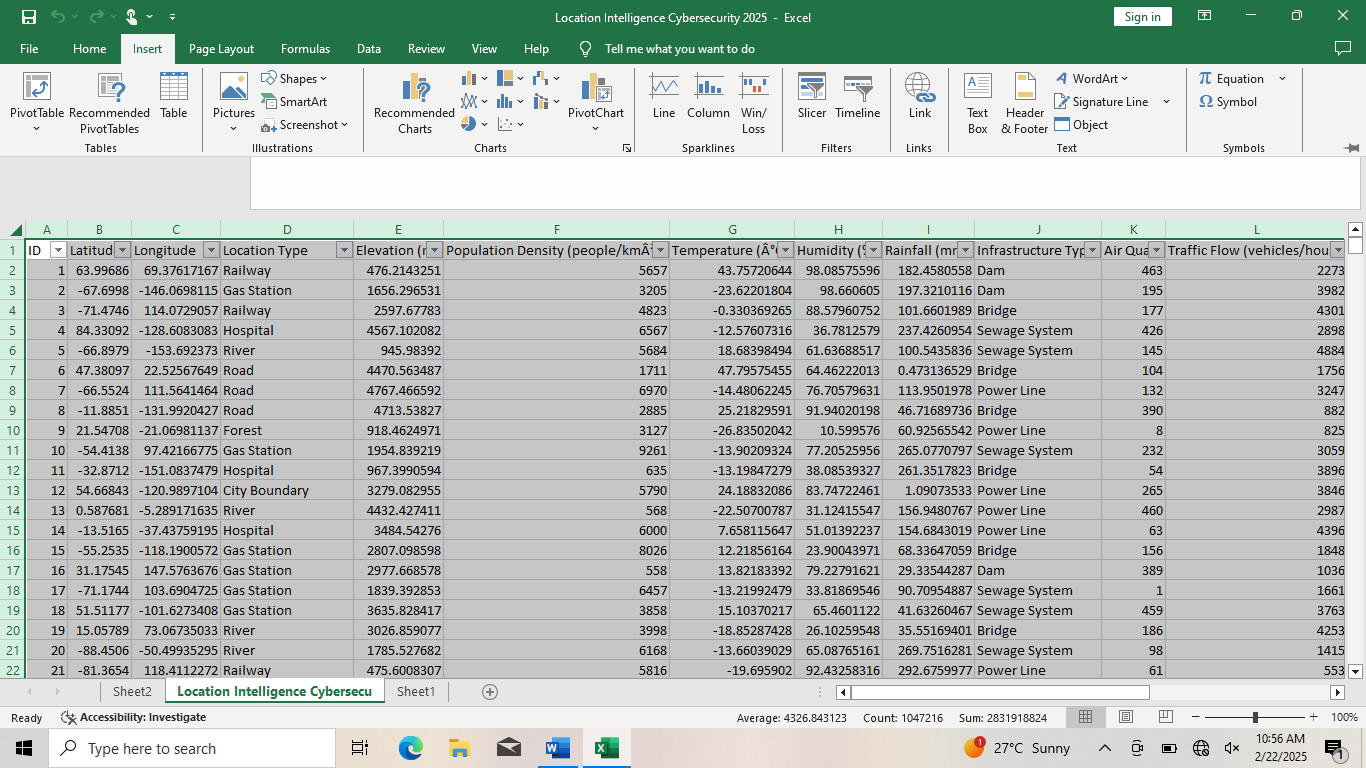
It contains 16 columns and 10,000 rows.

The following are the information on the dataset used.

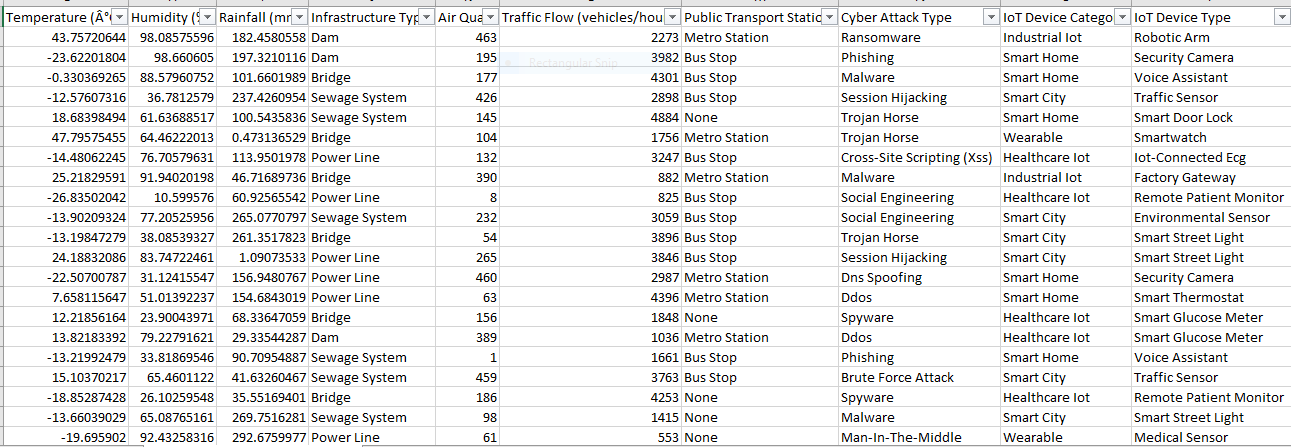
1. User\_ID
2. Latitude
3. Longitude
4. Location type
5. Elevation
6. Population density
7. Temperature
8. Humidity
9. Rainfall
10. Infrastructure type
11. Air quality index
12. Traffic flow
13. Public transport station
14. Cyber attack type
15. IoT device category
16. IoT device type

**Data Processing and Cleaning**

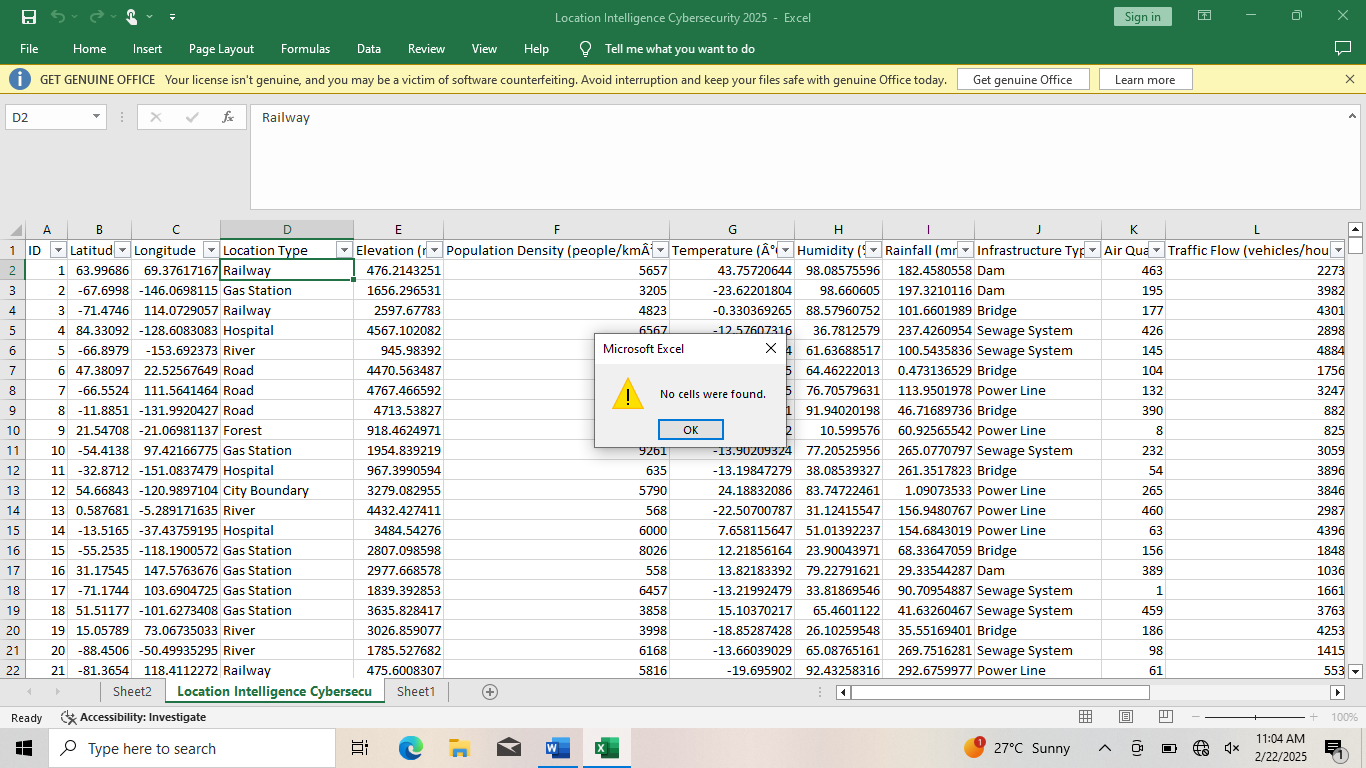
Loading the data in Excel;

 The dataset contains 16 columns and 10,000 rows. The data look good.

1. I used Removed duplicates to check for duplicates, the data did not contain duplicates.



1. I checked for blanks, the data did not contain blanks



**Questions guiding our analysis:**

1. Which locations are most vulnerable to cyber threats?
2. Are certain infrastructure types (e.g., bridges, hospitals, or gas stations) more prone to cyberattacks?
3. Do temperature, humidity, or rainfall levels influence the frequency or type of cyberattacks?
4. How does air quality relate to cyberattack occurrences on IoT devices?
5. Which cyberattacks (e.g., ransomware, phishing, malware) are most common?
6. What IoT device categories (e.g., smart home, smart city, healthcare) are most targeted?
7. Are certain public transport hubs (bus stops, metro stations) more associated with cyber threats?

**Insights:**

1. Which locations are most vulnerable to cyber threats?

|  |  |
| --- | --- |
| **Row Labels** | **Count of Cyber Attack Type** |
| City Boundary | 7993 |
| Road | 7965 |
| Railway | 7959 |
| Hospital | 7904 |
| Gas Station | 7900 |
| Forest | 7886 |
| River | 7843 |
| Social Network Data | 5000 |
| Smartphone Data | 5000 |
| **Grand Total** | **65450** |

City Boundary, Road, Railway, Hospital, Gas station, Forest and River are the most locations vulnerable to cyber threats, follow by Social network data and Smartphone data who has the lowest cyber threats.

1. Are certain infrastructure types (e.g., Sewage system, Dam, or Bridge) more prone to cyberattacks?

|  |  |
| --- | --- |
| **Row Labels** | **Count of Cyber Attack Type** |
| Sewage System | 14048 |
| Power Line | 13815 |
| Dam | 13815 |
| Bridge | 13772 |
| Wifi Hotspot | 2525 |
| Cell Tower | 2522 |
| Data Center | 2478 |
| Mobile Tower | 2475 |
| **Grand Total** | **65450** |

Sewage system, Powerline, Dam and Bridge has more prone on cyberattacks then Wifi hotspot, Cell tower, Data center and Mobile tower.

1. Do temperature, humidity, or rainfall levels influence the frequency or type of cyberattacks?

|  |  |  |  |
| --- | --- | --- | --- |
| **Row Labels** | **Sum of Temperature (Â°C)** | **Sum of Humidity (%)** | **Sum of Rainfall (mm)** |
| Brute Force Attack | 44246.13648 | 243580.6268 | 665512.821 |
| Credential Stuffing | 43170.35544 | 234834.6362 | 648579.8174 |
| Cross-Site Scripting (Xss) | 42535.38625 | 243223.6569 | 655988.8722 |
| Ddos | 41951.12225 | 235291.0174 | 643227.9003 |
| Dns Spoofing | 42564.13386 | 236646.763 | 666788.1635 |
| Malware | 44099.57191 | 241694.358 | 674601.5733 |
| Man-In-The-Middle | 44191.81432 | 244011.8689 | 665907.5267 |
| Phishing | 42823.15325 | 239365.2771 | 643661.2682 |
| Ransomware | 43287.32955 | 239847.6245 | 646111.4658 |
| Session Hijacking | 42214.44442 | 243518.4716 | 666889.6441 |
| Social Engineering | 43272.38866 | 239861.2433 | 642378.7121 |
| Spyware | 45838.77809 | 238855.2475 | 661590.6651 |
| Sql Injection | 43867.23942 | 238563.7994 | 658059.3056 |
| Trojan Horse | 43271.7728 | 236561.3457 | 649537.4875 |
| Zero-Day Exploit | 45078.77581 | 243932.7071 | 670265.0358 |
| **Grand Total** | **652412.4025** | **3599788.644** | **9859100.259** |

Temperature, Humidity, Rainfall levels has influence on the cyberattack type.

1. How does air quality relate to cyberattack occurrences on IoT devices?

|  |  |
| --- | --- |
| **Row Labels** | **Sum of Air Quality Index (AQI)** |
| Traffic Sensor | 1104402 |
| Iot-Connected Ecg | 1101939 |
| Smart Street Light | 1091203 |
| Environmental Sensor | 1089606 |
| Smartwatch | 1088768 |
| Remote Patient Monitor | 1083805 |
| Medical Sensor | 1075560 |
| Fitness Tracker | 1070107 |
| Smart Glucose Meter | 1067933 |
| Voice Assistant | 852023 |
| **Grand Total** | **10625346** |

Traffic sensor has the highest number of air quality on IOT devices, follow by Iot-connected Ecg, Smart street light, Environmental sensor, Smartwatch, Remote patient monitor, Medical sensor, Fitness tracker etc.

1. Which cyberattacks (e.g., ransomware, phishing, malware) are most common?

|  |  |
| --- | --- |
| **Row Labels** | **Sum of ID** |
| Brute Force Attack | 145027508 |
| Credential Stuffing | 141391268 |
| Cross-Site Scripting (Xss) | 144153656 |
| Ddos | 140579369 |
| Dns Spoofing | 142073376 |
| Malware | 143164166 |
| Man-In-The-Middle | 142833168 |
| Phishing | 140801286 |
| Ransomware | 144158103 |
| Session Hijacking | 144531777 |
| Social Engineering | 142893514 |
| Spyware | 140770218 |
| Sql Injection | 143767228 |
| Trojan Horse | 141219525 |
| Zero-Day Exploit | 144519813 |
| **Grand Total** | **2141883975** |

Brute Force Attack is the most common cyberattack type, follow by Session Hijacking and Zero Day Exploit who are second most common cyberattack, follow by others.

1. What IoT device categories (e.g., smart home, smart city, healthcare) are most targeted?

|  |  |
| --- | --- |
| **Row Labels** | **Sum of ID** |
| Smart City | 430876702 |
| Smart Home | 430424317 |
| Wearable | 427936619 |
| Healthcare Iot | 427577586 |
| Industrial Iot | 425068751 |
| **Grand Total** | **2141883975** |

Smart City are most targeted IOT device, follow by Smart Home, Wearable and others.

1. Are certain public transport hubs (bus stops, metro stations) more associated with cyber threats?

|  |  |
| --- | --- |
| **Row Labels** | **Count of Cyber Attack Type** |
| Bus Stop | 21697 |
| Metro Station | 21929 |
| None | 21824 |
| **Grand Total** | **65450** |

Metro Station are more associate with cyber threats, follow by Bus station.

**Insights:**

1. City Boundary, Road, Railway, Hospital, Gas station, Forest and River are the most locations vulnerable to cyber threats, follow by Social network data and Smartphone data who has the lowest cyber threats.
2. Sewage system, Powerline, Dam and Bridge has more prone on cyberattacks then Wifi hotspot, Cell tower, Data center and Mobile tower.
3. Temperature, Humidity, Rainfall levels has influence on the cyberattack type.
4. Traffic sensor has the highest number of air quality on IOT devices, follow by Iot-connected Ecg, Smart street light, Environmental sensor, Smartwatch, Remote patient monitor, Medical sensor, Fitness tracker etc.
5. Brute Force Attack is the most common cyberattack type, follow by Session Hijacking and Zero Day Exploit who are second most common cyberattack, follow by others.
6. Smart City are most targeted IOT device, follow by Smart Home, Wearable and others.
7. Metro Station are more associate with cyber threats, follow by Bus station.

**Recommendations:**

**.** Implement stronger security protocols for IoT devices in high-risk areas, especially in smart city, smart home and industrial IoT.

**.** Deploy real-time monitoring for traffic sensors and smart city infrastructure to prevent cyber intrusions.

**.** Prioritize cybersecurity investments in hospitals, gas stations, and railway hubs with high cyberattack rates.

**.** Consider the impact of weather conditions on IoT security, implementing additional safeguards for extreme climates.

**.** Educate users on the risks of IoT cybersecurity in urban areas.