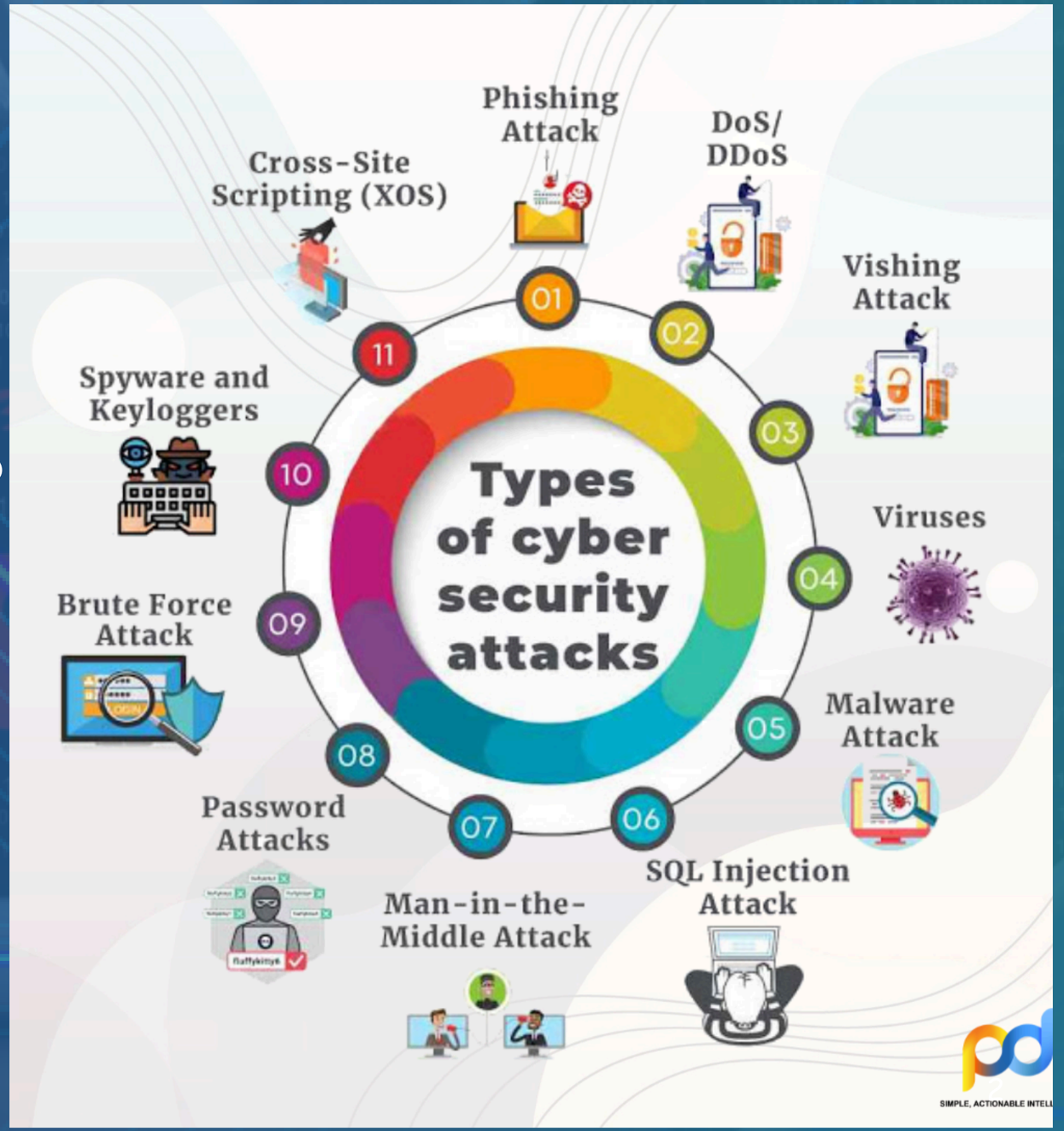
Digital Defenders
(Group 10)

# ANALYSIS ON CYBERSECURITY ATTACKS

By: Huiting Wu,
Sharmeen Kapoorwala

# CYBERSECURITY ATTACKS

- What are Cybersecurity attacks?



# FBI Internet Crime Report 2023

A **42%** increase in cyber attacks?

## 2023 CRIME TYPES continued

**By Complaint Loss**

| *Crime Type* | *Loss* | *Crime Type* | *Loss* |
|---|---|---|---|
| Investment | $4,570,275,683 | Extortion | $74,821,835 |
| BEC | $2,946,830,270 | Employment | $70,234,079 |
| Tech Support | $924,512,658 | Ransomware* | $59,641,384 |
| Personal Data Breach | $744,219,879 | SIM Swap | $48,798,103 |
| Confidence/Romance | $652,544,805 | Overpayment | $27,955,195 |
| Data Breach | $534,397,222 | Botnet | $22,422,708 |
| Government Impersonation | $394,050,518 | Phishing/Spoofing | $18,728,550 |
| Non-payment/Non-Delivery | $309,648,416 | Threats of Violence | $13,531,178 |
| Other | $240,053,059 | Harassment/Stalking | $9,677,332 |
| Credit Card/Check Fraud | $173,627,614 | IPR/Copyright and Counterfeit | $7,555,329 |
| Real Estate | $145,243,348 | Crimes Against Children | $2,031,485 |
| Advanced Fee | $134,516,577 | Malware | $1,213,317 |
| Identity Theft | $126,203,809 | | |
| Lottery/Sweepstakes/Inheritance | $94,502,836 | | |

# WHICH DEVICE DO YOU THINK IS MORE SECURE?

**which device do you think is more secure?**

- Apple Devices
- Non Apple Devices
- none of them
- both of them (equally)

Your name will not be shared | 0 votes


# CYBERSECURITY DATASET

## About

- Synthetic dataset created through Algorithm
- Generated by the Incribo data generation company
- Cybersecurity attacks in India from January 1st, 2020, to October 11th, 2023

## Why

- Privacy Regulations
- To improve the intelligent models for cybersecurity


# CYBERSECURITY DATASET

## Algorithms

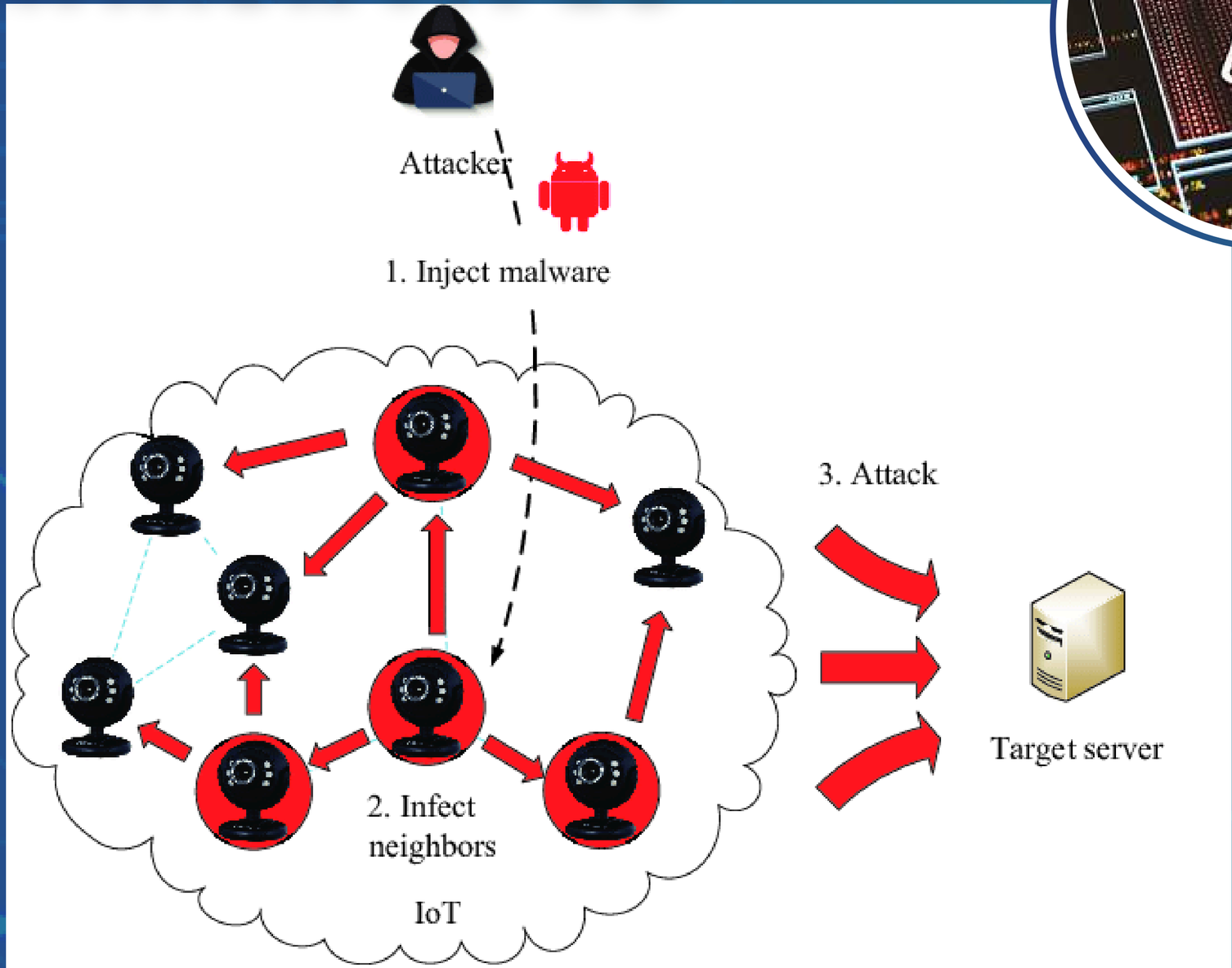
- Oversampling
- Categorical latent Gaussian process
- GAN
- Data Augmentation
- Reinforsec

## Important Variables

- Attack type
- Severity Type
- Action Taken
- Device Information
- Location

# CYBER ATTACK TYPES

- DDoS
- Malware
- Intrusion

# RESEARCH QUESTIONS

1. Are the attack types (Malware. DDoS, Intrusion) associated with severity levels (low, medium, high)?

2. Does a non-apple device have a greater proportion of high severity level attacks than an Apple device?

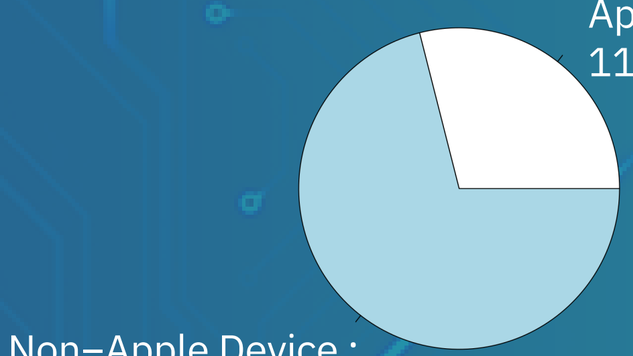
3. Is the action taken associated with high-severity level attacks?


# SUMMARY TABLE

| | Apple Device. N = 11,587 | Non-Apple Device N = 28,413 |
|---|---|---|
| **Attack Type** | | |
| DDoS | 3,838 (33%) | 9,590 (34%) |
| Intrusion | 3,902 (34%) | 9,363 (33%) |
| Malware | 3,847 (33%) | 9,460 (33%) |
| **Severity Level** | | |
| High | 3,894 (34%) | 9,488 (33%) |
| Low | 3,825 (33%) | 9,358 (33%) |
| Medium | 3,868 (33%) | 9,567 (34%) |
| **Action Taken** | | |
| Blocked | 3,926 (34%) | 9,603 (34%) |
| Ignored | 3,832 (33%) | 9,444 (33%) |
| Logged | 3,829 (33%) | 9,366 (33%) |

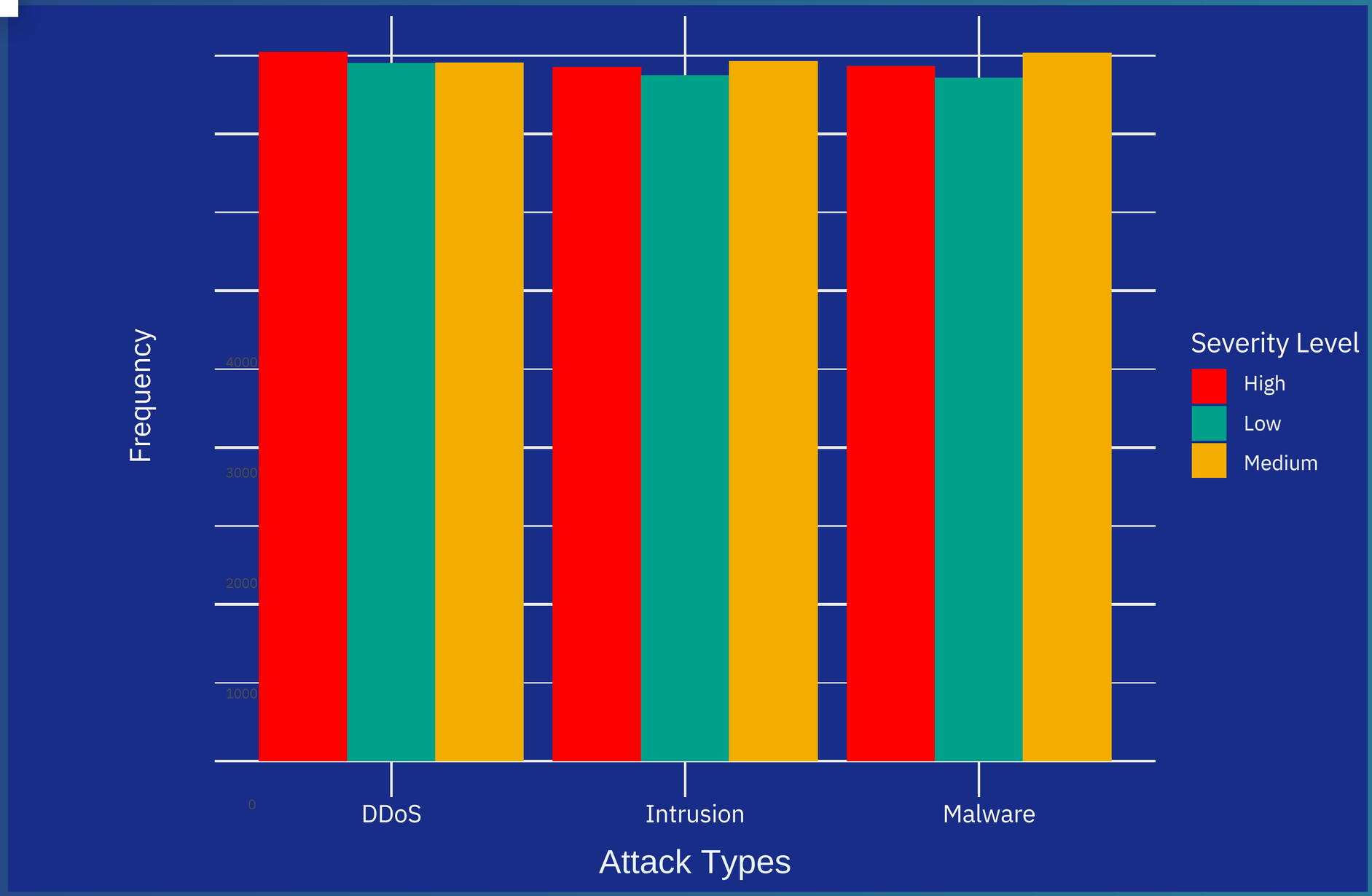
[1] n (%)

**Pie Chart of Device**



# PLOT 1

## Relationship Of Attack Types And Severity Level



# HYPOTHESIS TEST

01

Relationship between attack types and severity levels

$H_0$: Attack types are independent of their severity level

$H_A$ : Attack types are associated with their severity level

# CHECK CONDITIONS

1. Independence:

The data is a random sample generated by the algorithm.

2. Expected Counts:

| | High | Low | Medium |
|---|---|---|---|
| DDoS | 4523 | 4450 | 4455 |
| Intrusion | 4427 | 4374 | 4464 |
| Malware | 4432 | 4359 | 4516 |

# RESULTS

## Test Statistic

z = 1.797

## p-value

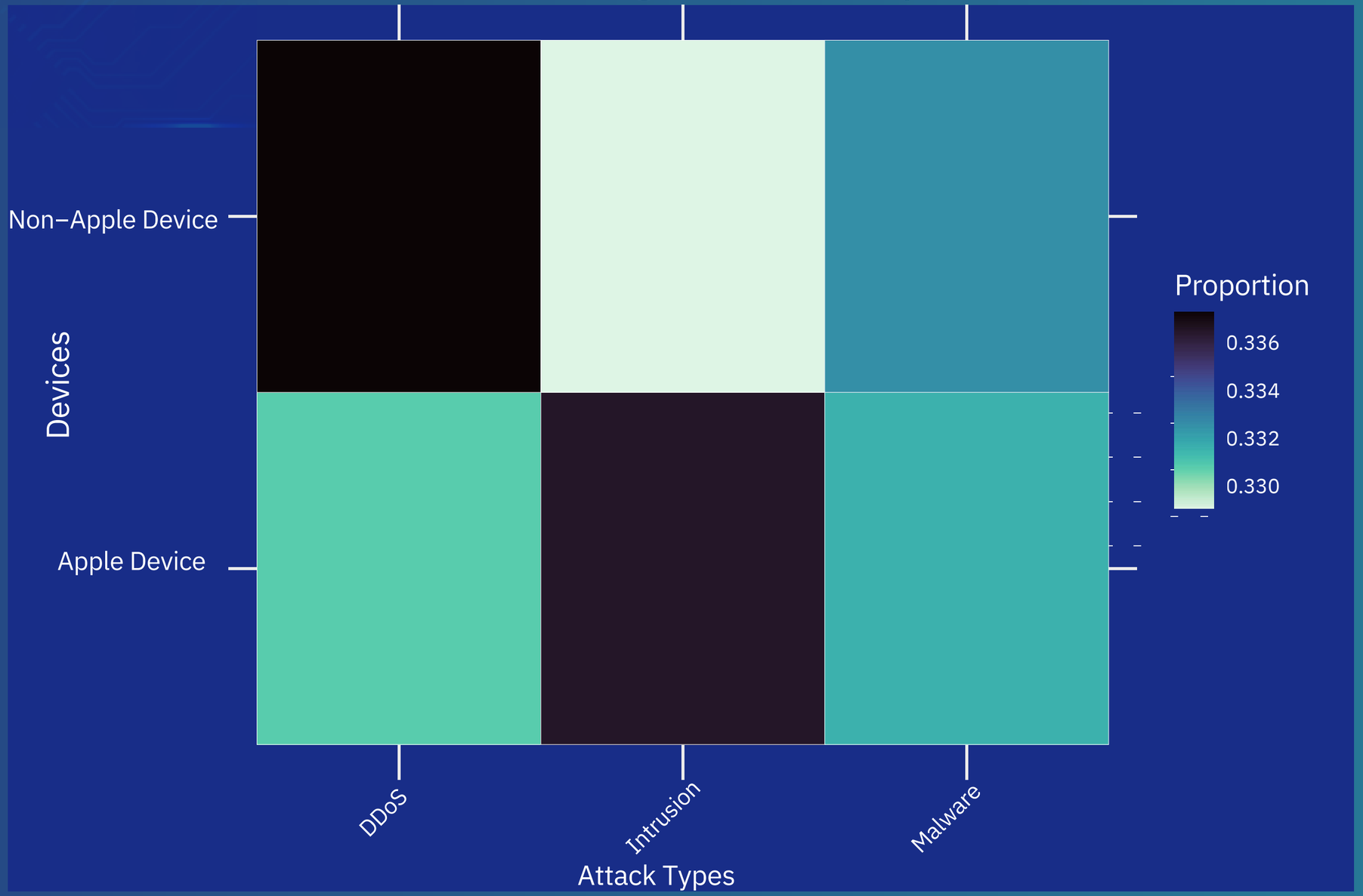
p-value = 0.773


## Conclusion

**Decision:** Fail to reject the null hypothesis.
**Context:** We have no enough evidence that there is an association between attack type and severity level.

# PLOT 2

## Relationship between Devices and Attack Type through heatmap



# HYPOTHESIS TEST

02

Does a non-apple device have a greater proportion of high severity level attacks than an Apple device?

$H_0$ : Non-Apple devices have the same proportion of attacks as the Apple devices

$$P_1 = P_2$$

$H_A$: Non-Apple devices have a greater proportion of attacks than the Apple devices

$$P_1 > P_2$$

# CHECK CONDITIONS

1. Independence:

The data is a random sample generated by the algorithm.

2. Large Counts SUCCESS & FAILURE

| | | VALUE ≥ 5 |
|---|---|---|
| $N_2P_2$ | = 3894 | TRUE |
| $N_1P_1$ | = 9488 | TRUE |
| $N_2(1-P_2)$ | = 7693 | TRUE |
| $N_1(1-P_1)$ | = 18925 | TRUE |

# RESULTS


## Test Statistic

z = 0.168

## p-value

p-value = 0.659

## Confidence Interval 95%

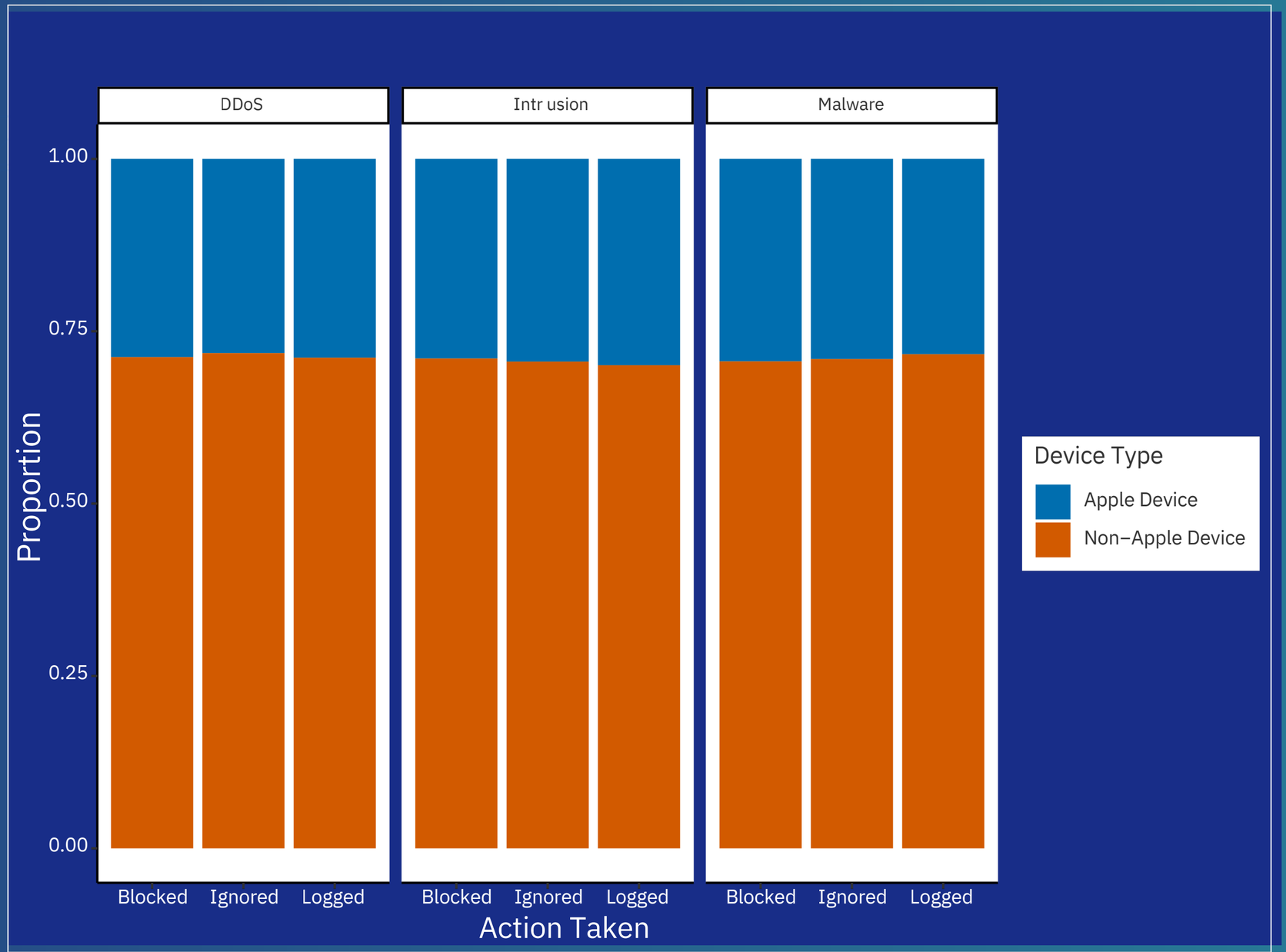
95% confidence interval is (-0.0123, 0.00807).
We are 95% confident that the difference in proportions of high severity level attacks between the Non-Apple devices and Apple devices is between -0.0124 and 0.00813.

## Conclusion

**Decision:** Fail to reject the null hypothesis.
**Context:** We have no enough evidence that Non-Apple devices have a greater proportion of high severity level attacks than Apple devices.

# PLOT 3

## Relationship Of Device Types, Attack Types and Action Taken



# HYPOTHESIS TEST

03

Is the action taken associated with high-severity level attacks for Devices

$H_0$ : There is independence between Devices and actions taken for high-severity level attacks

$H_A$ : There is an association between Devices and actions taken for high-severity level attacks

# CHECK CONDITIONS

1. Independence:

The data is a random sample generated by the algorithm.

2. Expected Counts:

| | Blocked | Ignored | Logged |
|---|---|---|---|
| Apple Device | 1318.175 | 1297.806 | 1278.019 |
| Non-Apple Device | 3211.825 | 3162.194 | 3113.981 |

# RESULTS


## Test Statistic

z = 2.884

## p-value

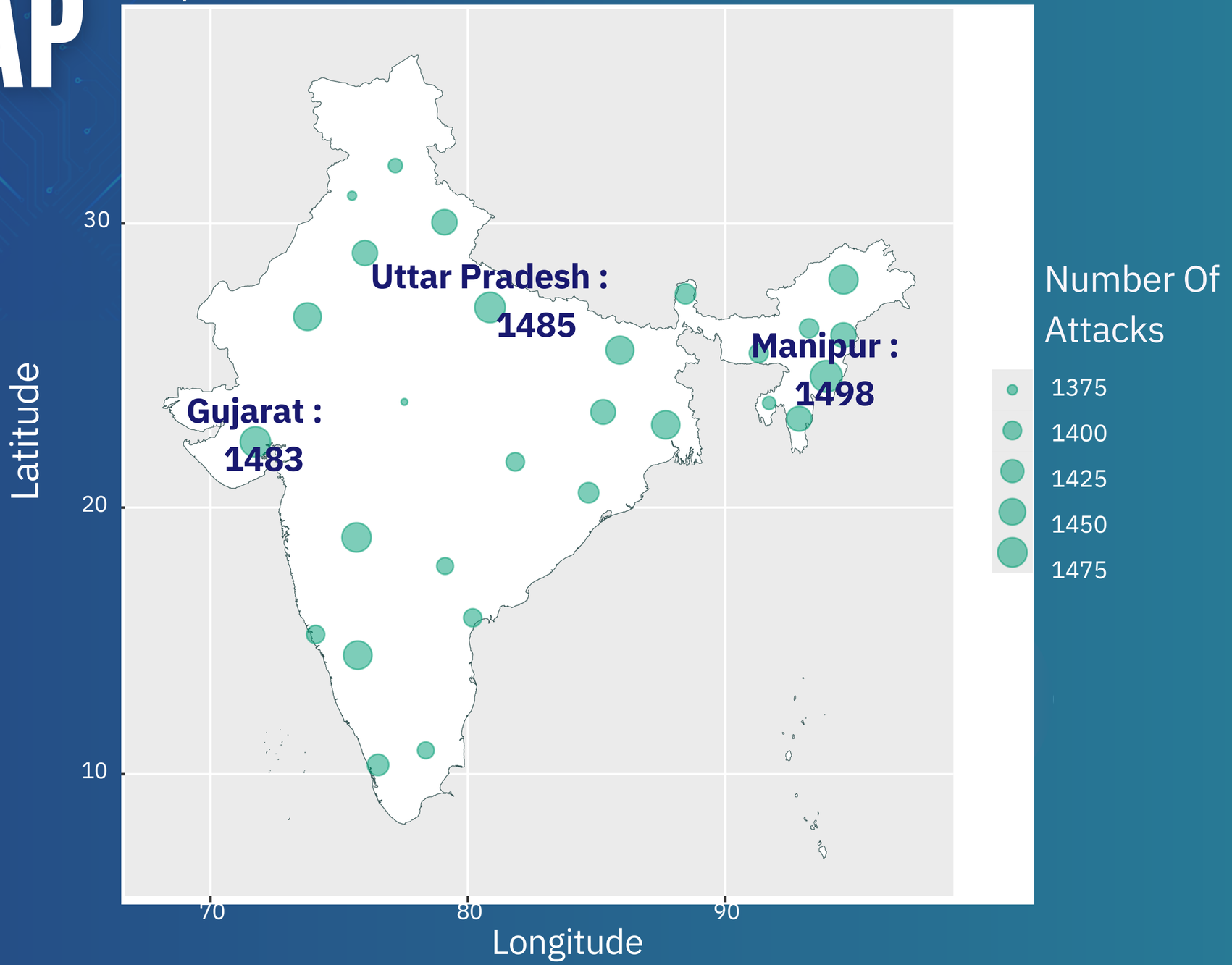
p-value = 0.236

## Conclusion

**Decision:** Fail to reject the null hypothesis.
**Context:** We have no enough evidence that the device types and actions taken to the high severity level attacks are associated.

# INDIA MAP

## Map Of State In India With Number Of Attacks



# CONCLUSION OF HYPOTHESIS TESTS

- Attack type is not associated with the severity level.
- Non-Apple Devices does not have a greater proportion of attacks for high severity level than Apple Devices
- Device types and actions taken for the high severity level attacks are not associated.

# LIMITATIONS

- Lack Of Realism
- Limited types of attacks
- Resource and knowledge limitation
- Great amount of missing values in other variables

# SECONDARY ANALYSIS

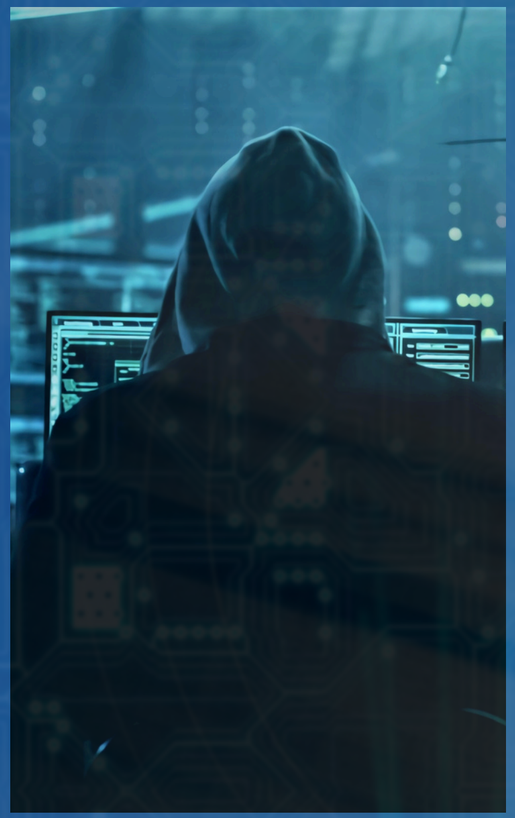

- Reduced missing values
- Include longer period data ; more attack types
- Investigate the generation process of the dataset
- Develop models for detecting attacks

# PERSONAL TIPS

- Keep Software updated for known vulnerabilities
- Use firewall and WAF
- Services like AWS shield can absorb excess traffic data to avoid DDoS attacks
- Use MFA and install antiviruses
- Maintain Backups

# NEVER BELIEVE THIS!!!

# REFERENCES




- https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf
- https://www.kaggle.com/datasets/teamincribo/cyber-security-attacks
- https://incribo.com/
- https://pmc.ncbi.nlm.nih.gov/articles/PMC9920136/#sec6-sensors-23-01231
- https://rpubs.com/DeclanStockdale/799284
- https://github.com/JLSteenwyk/ggpubfigs
- https://en.wikipedia.org/wiki/List_of_states_and_union_territories_of_India_by_population

# THANK YOU AND FEEL FREE TO ASK ANY QUESTION!