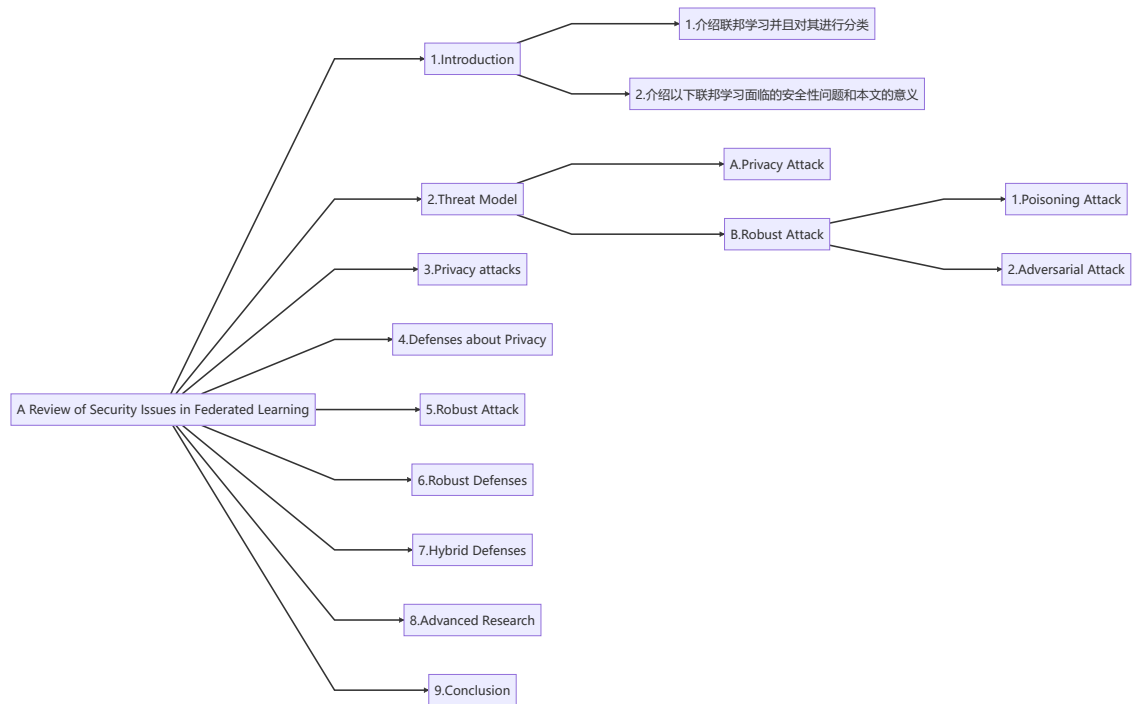


1. A-Review-Of-Security-Issues-In-Federated-Learning

This is our first paper, which is called A Review Of Security Issues In Federated Learning.



另一种结构是：

```
``mermaid
graph LR
    a[A Review of Robust Issues in Federated Learning]
    a ---> b1[1.Introduction]
    b1 ---> b1a[1.介绍联邦学习并且对其进行分类]
    b1 ---> b1b[2.介绍以下联邦学习面临的鲁棒性问题及本文的意义]

    a ---> b2[2.Threat Model]
    b2 ---> b2a[A.Poisoning Attack]
    b2 ---> b2b[B.Adversarial Attack]
    a ---> b3[3.Poisoning Attack]
    a ---> b4[4.Defenses about Poisoning Attack]
    a ---> b5[5.Adversarial Attack]
    a ---> b6[6.Adversarial Defenses]
    a ---> b7[7.Hybrid Defenses]
    a ---> b8[8.Advanced Research and Problems]
    a ---> b9[9.Conclusion]
```

