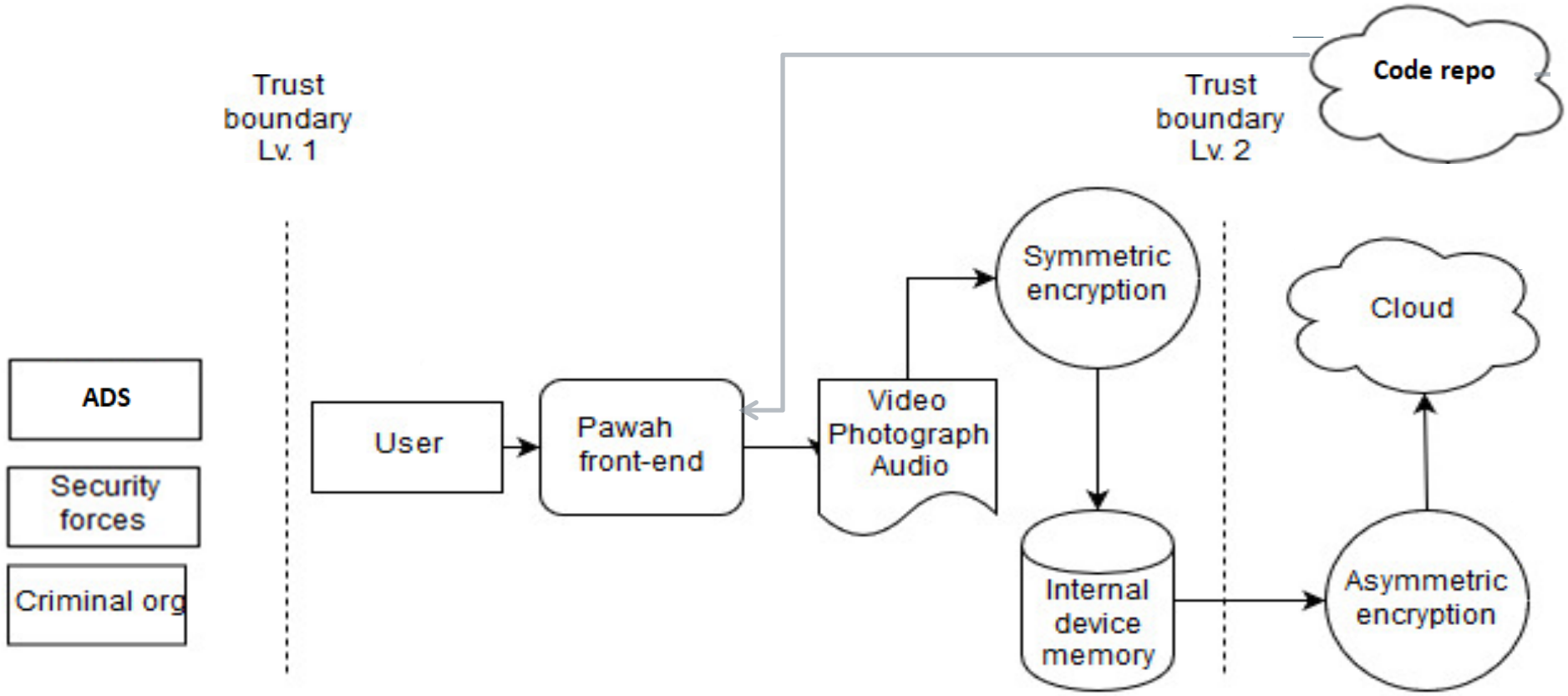


Threats

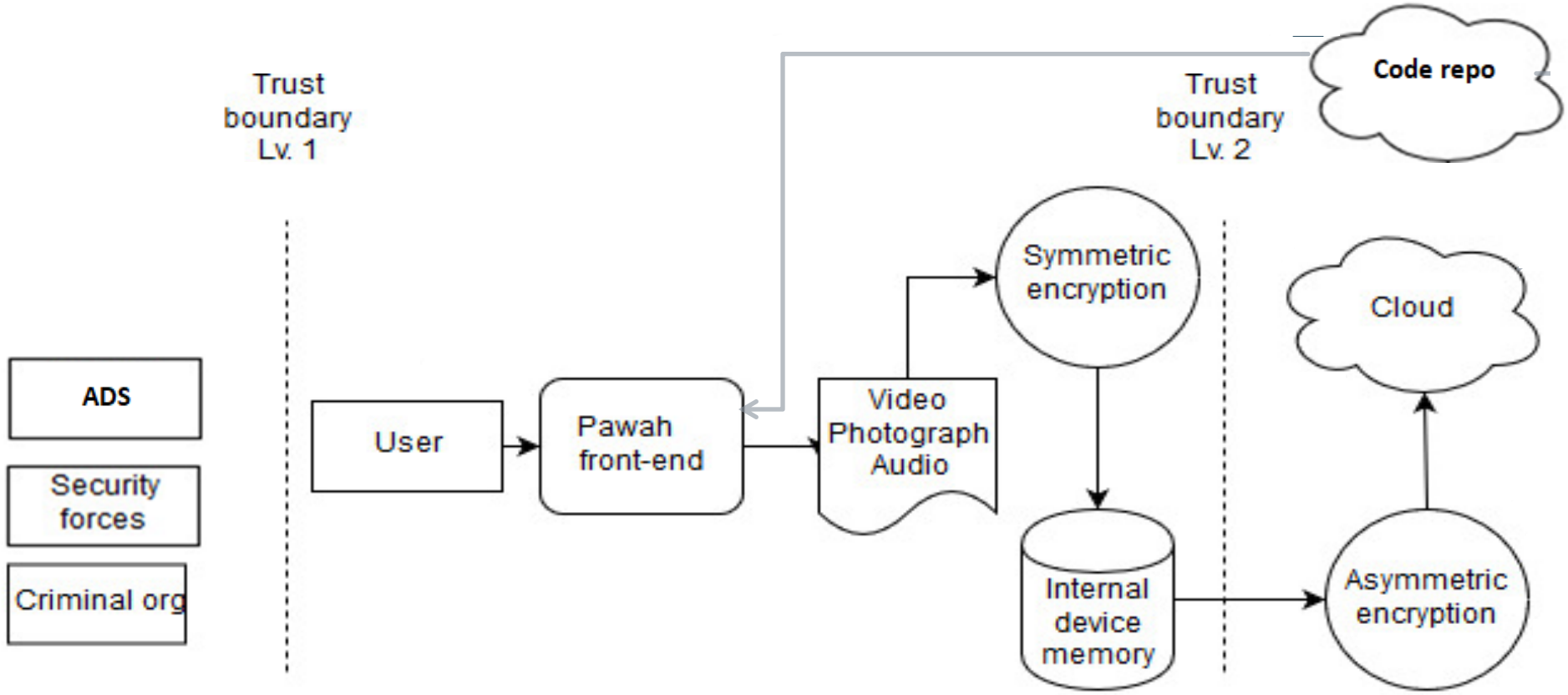
- External attacker impersonating user to access app
-
-
-

Threats

-
-
-
-

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
-
-
-



Threats

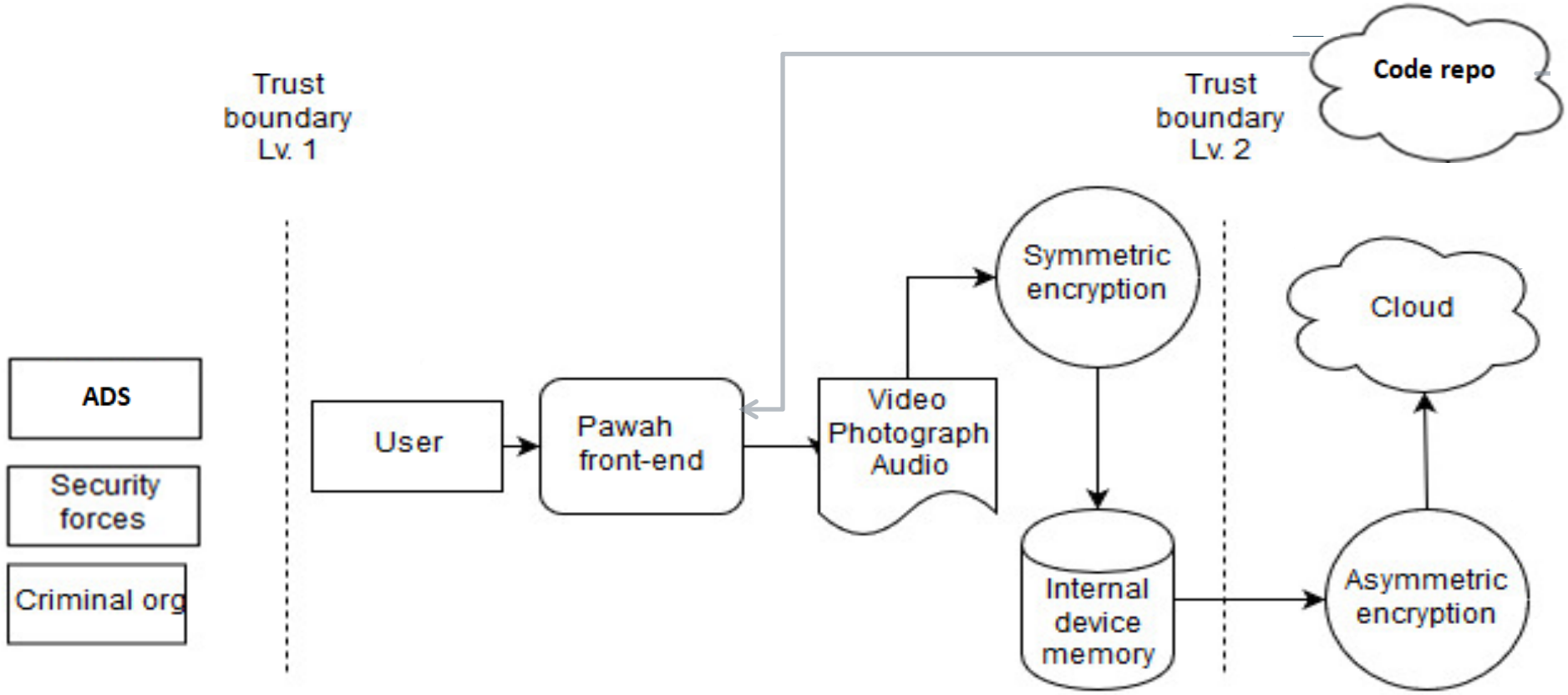
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
-

Threats

-
-
-
-

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
-
-
-



Threats

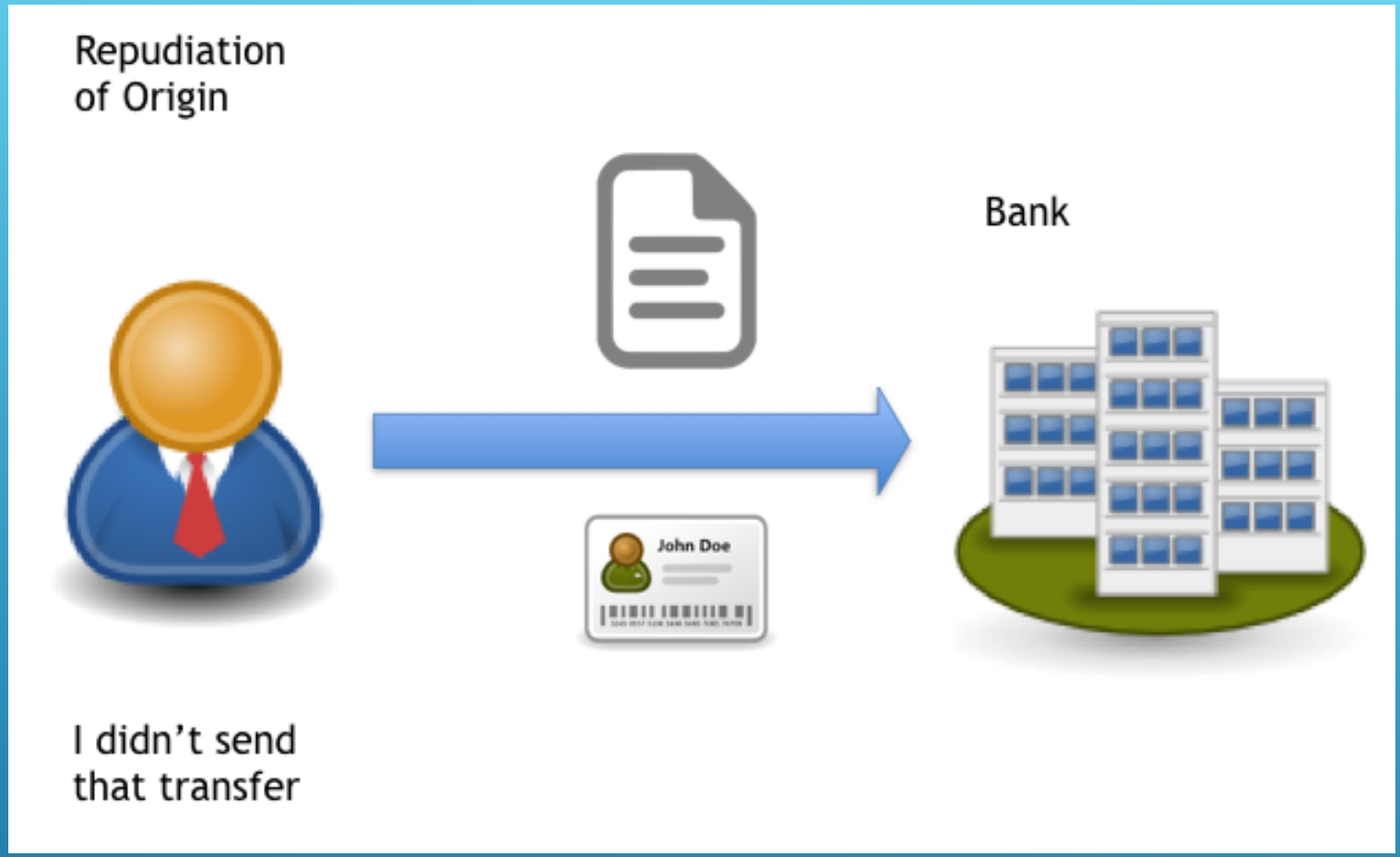
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
-

Threats

-
-
-
-

Threats

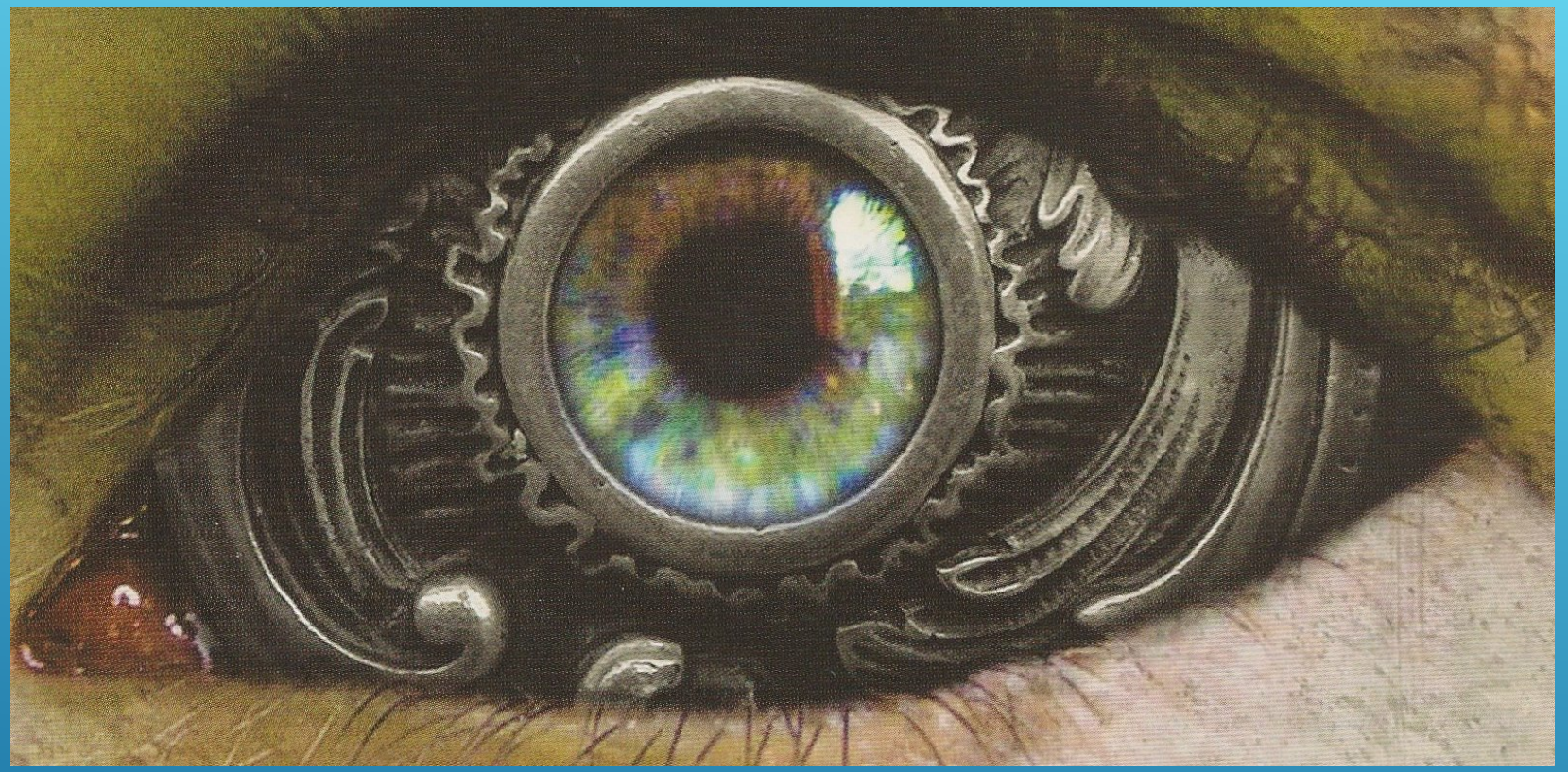
- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
-



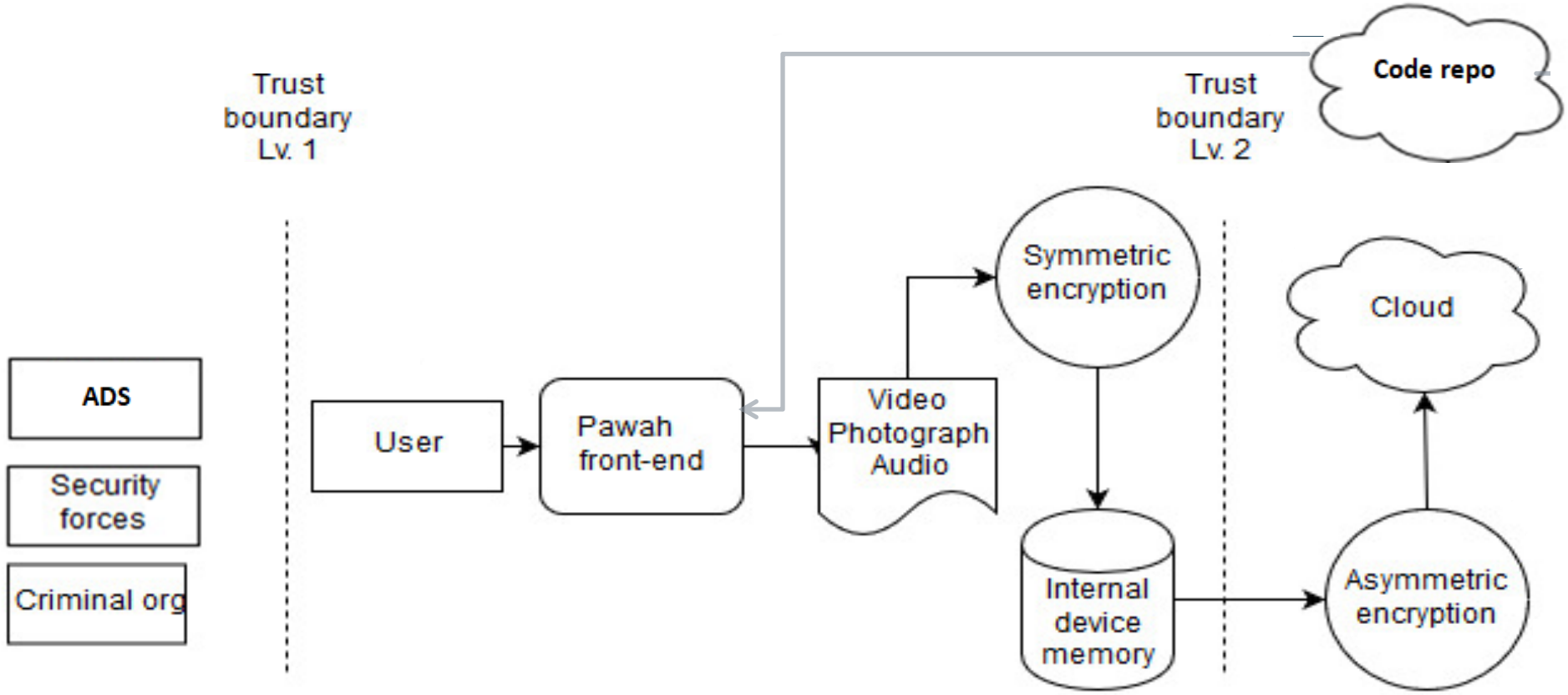
STRIDE - REPUDIATION

THIS IS A HARD ONE

- Someone claims the footage is false or of someone else
  - Other than a forensic chain of custody we can't do much about that
- For your app could someone perform an action and claim it wasn't them?



STRIDE - INFORMATION DISCLOSURE



Threats

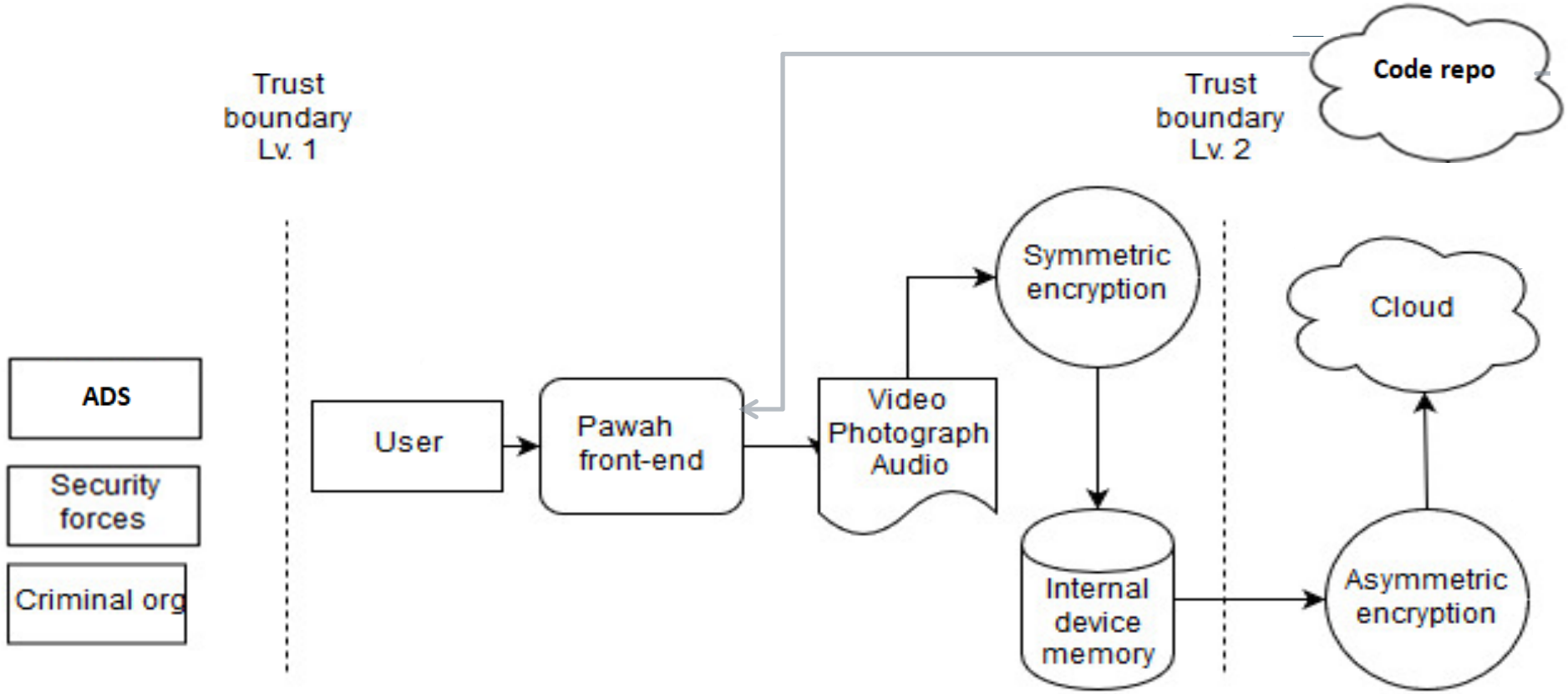
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
-

Threats

-
-
-
-

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
-



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

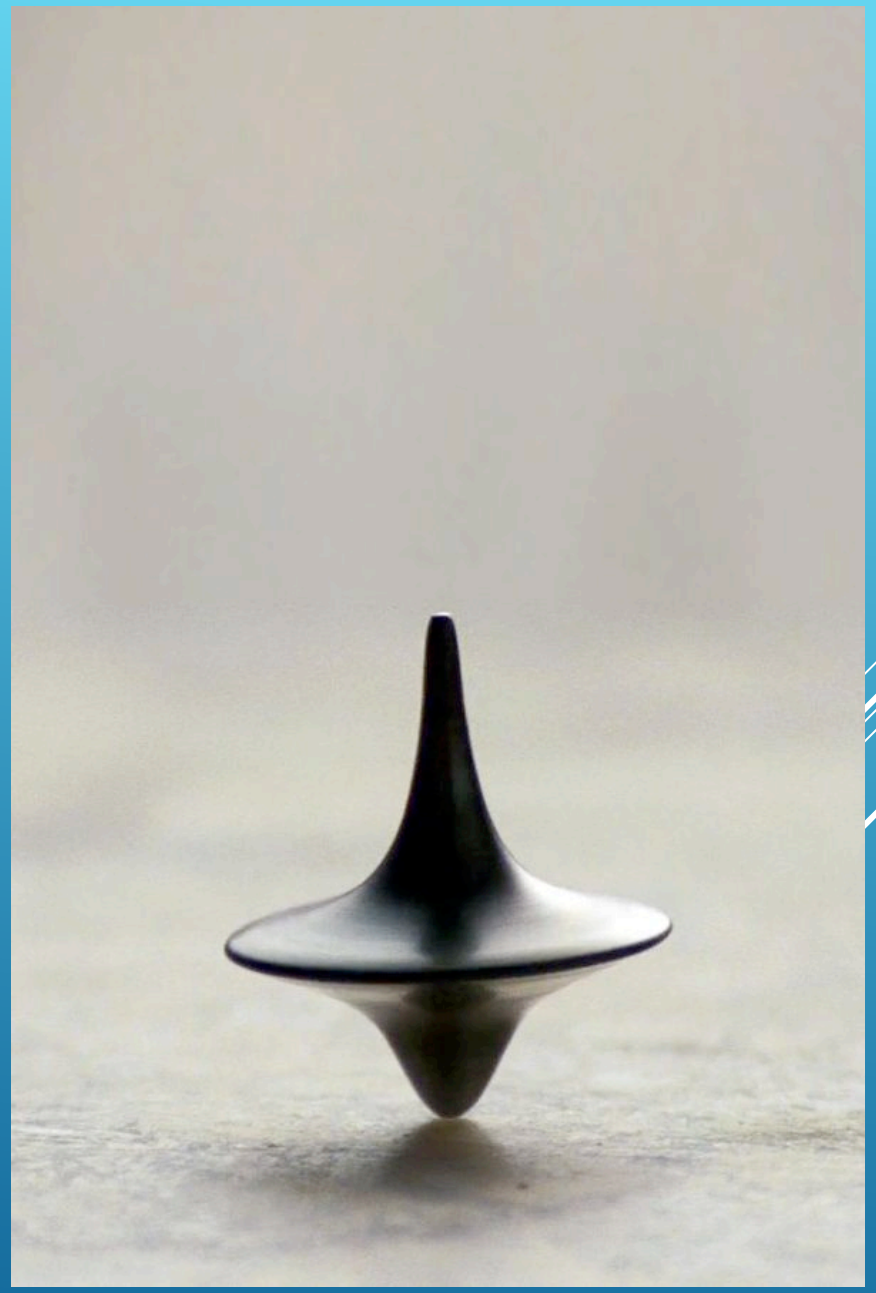
Threats

Threats

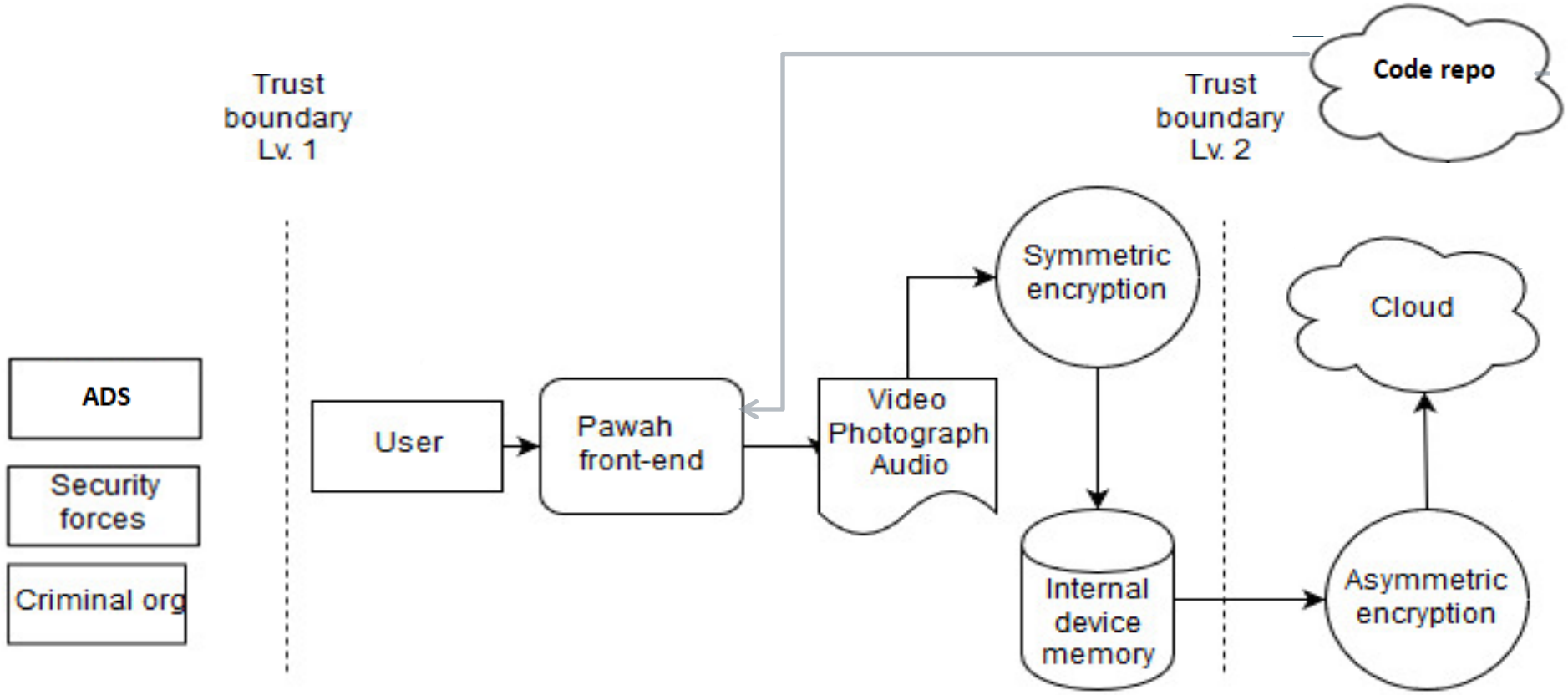
- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information

WE NEED TO GO DEEPER

- Enumerate
  - Technology
  - Protocols
  - Functionality that can be abused (PIN reset)
- Flesh out connected systems
  - Code repository
  - Cloud storage
  - Log server



STRIDE - DENIAL OF SERVICE



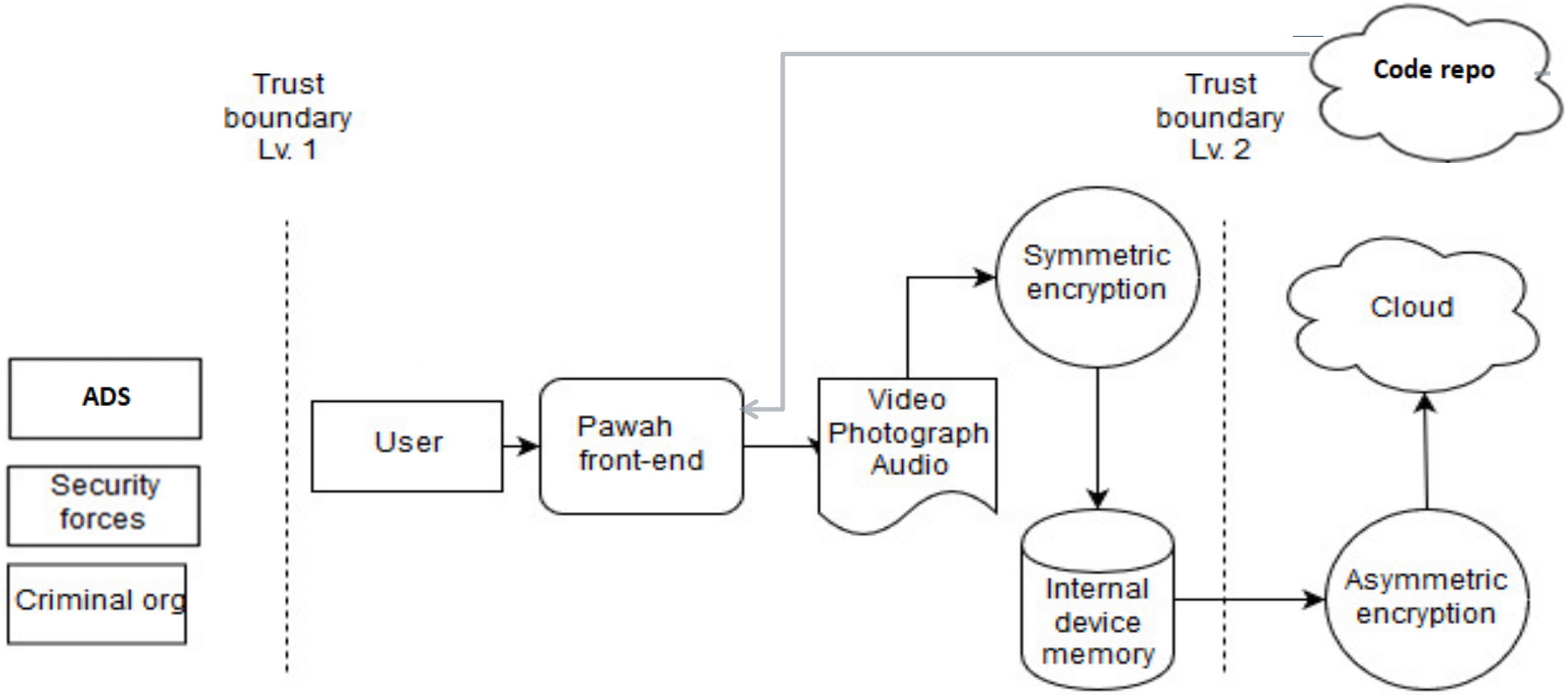
Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information



Threats

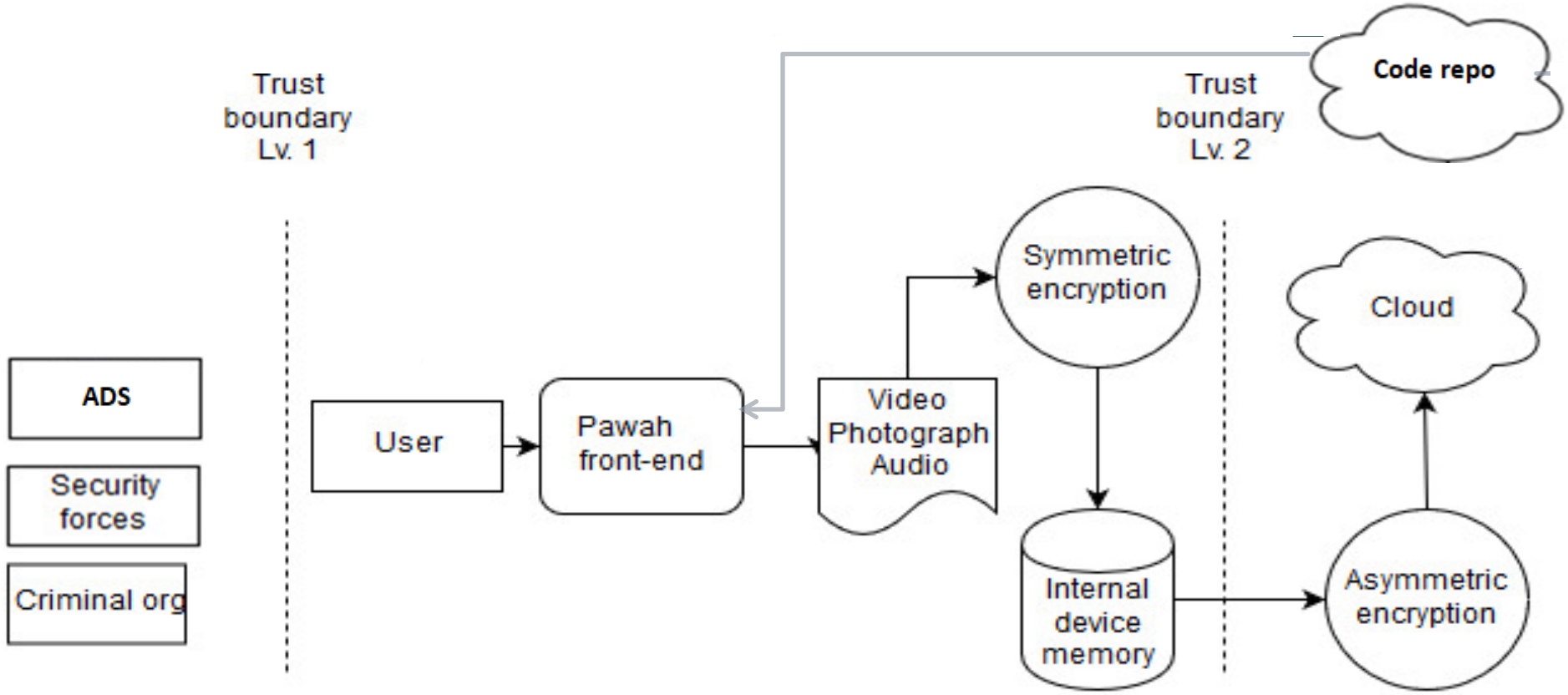
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

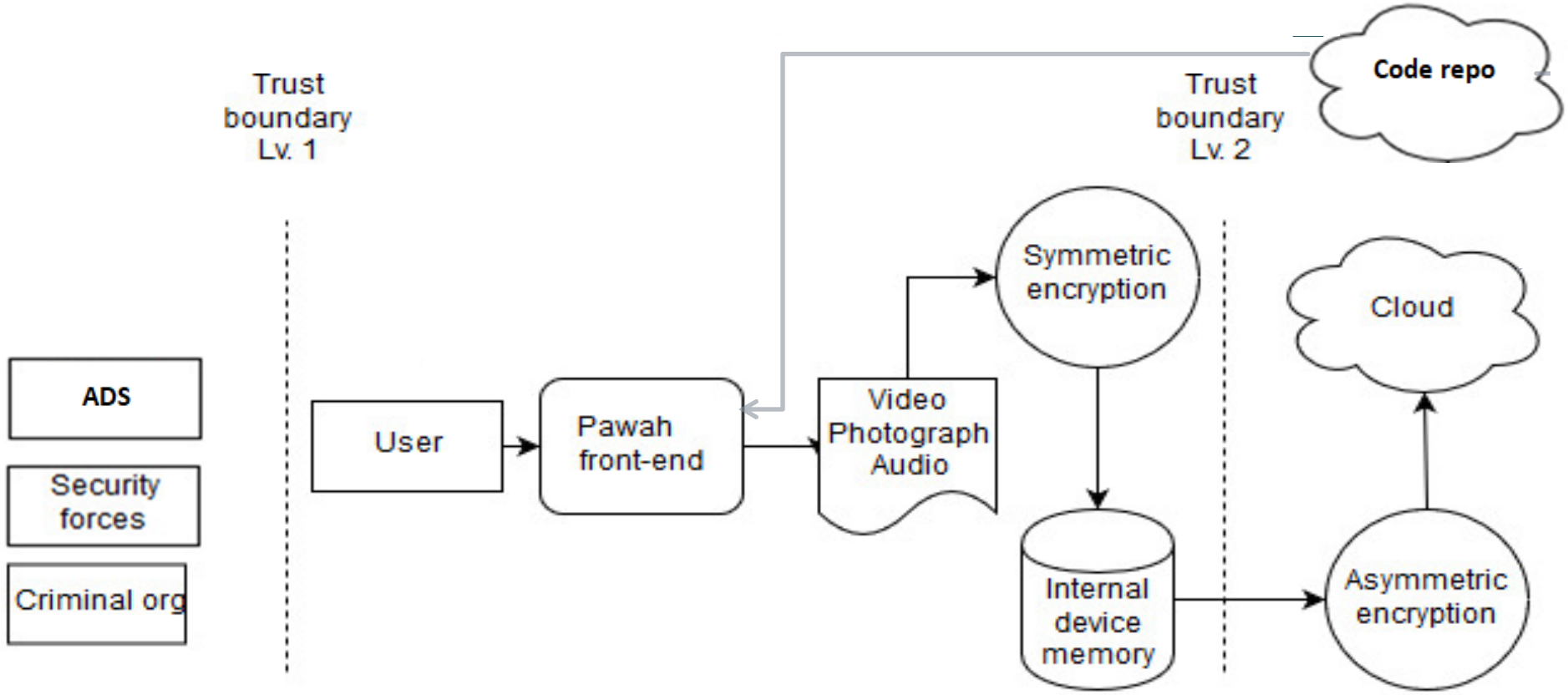
Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information

STRIDE – ELEVATION OF PRIVILEGES



Threats

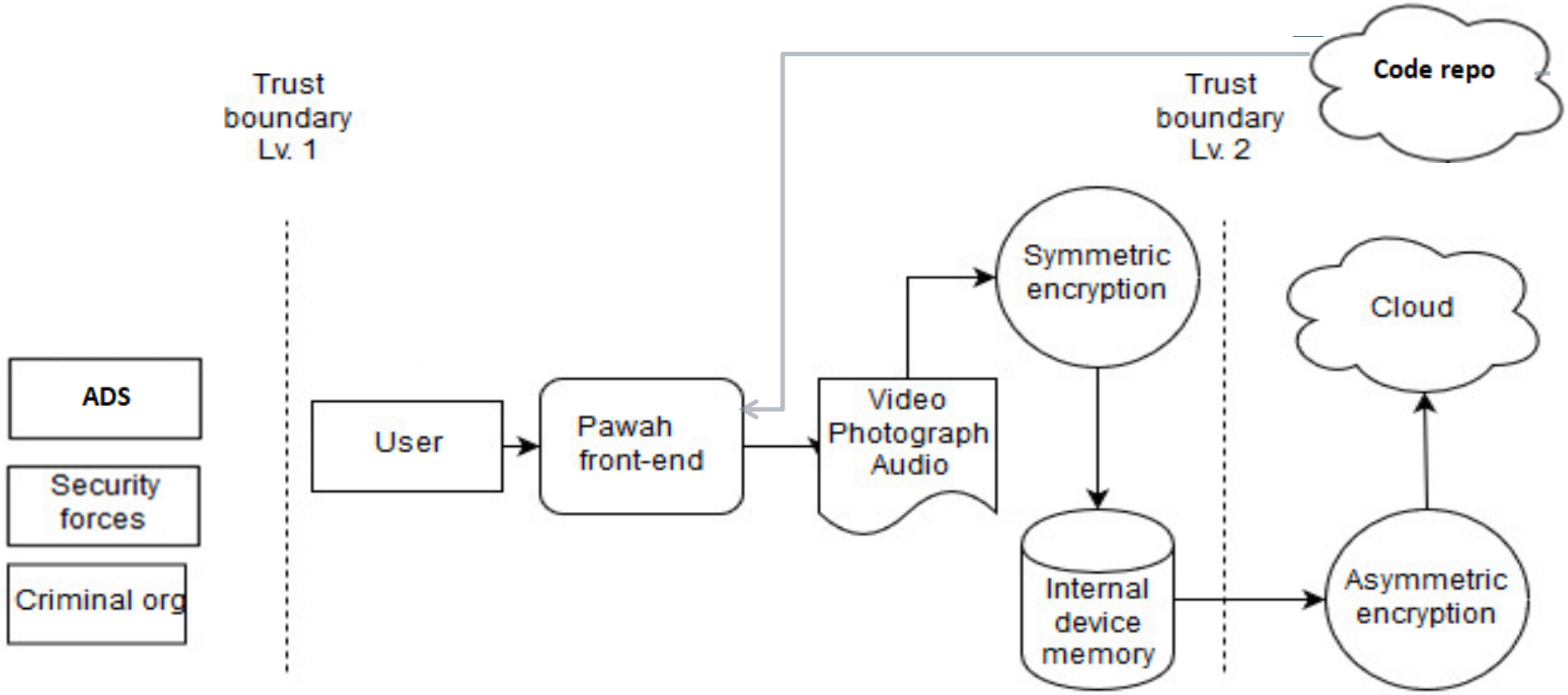
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information



Threats

- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

Threats

- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats

- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
-