Relationship based Trust Metrics for Securing Edge Computing

Oct 4, 2024

Naresh K. Sehgal[1], John M. Acken[2], Sonali Fernando[2], Divya Bansal[3] and Robert B. Bass[2]

1 Deeply Human AI, Inc; 2 ECE Dept, Portland State Univ; 3 Punjab Engineering College

Content

- Why?
- What?
- How?

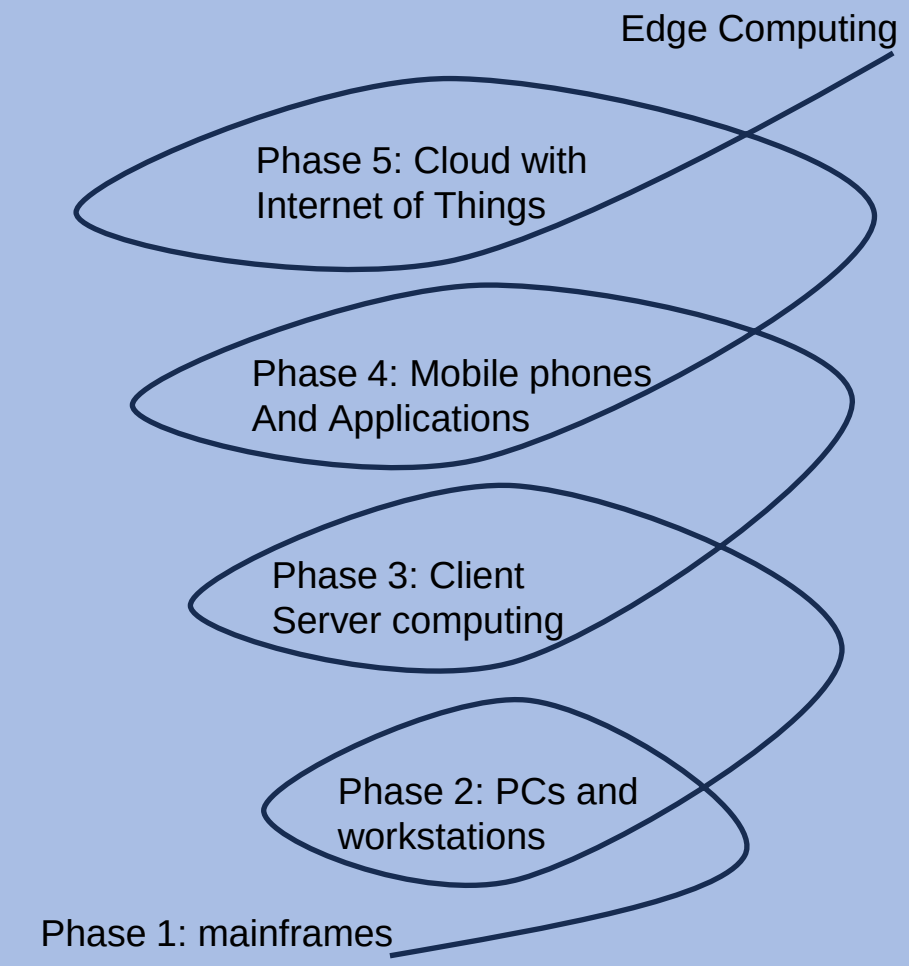
Why: Single evaluation of trust is insufficient

- Trust depends on the nature of a relationship
  - You trust a doctor for medical advice, but will you share your financial details?
  - Trust extends beyond people, includes computers and devices
- Trust is NOT bi-directional between two parties
  - You trust your doctor for medical advice, but would (s)he take your medical advice?
- Trust depends on the content of a transaction
  - Would you undergo cardiovascular surgery under an orthopedic doctor?

Any trust-based solution needs to accommodate multi-directional considerations

Emergence of Edge Computing

- Edge computing refers to data processing, and actions in real time closer to the source of the data.
- With IOT devices, use cases require localized compute power and data storage.
- An Edge based threat model spans multiple actors and a large attack surface.
- High level of security is required in accessing hospital databases, online financial transactions and operating factories etc.
- Lack of trust is limiting the adoption of Cloud computing, and efficacy of AI models due to limited data sharing between the parties

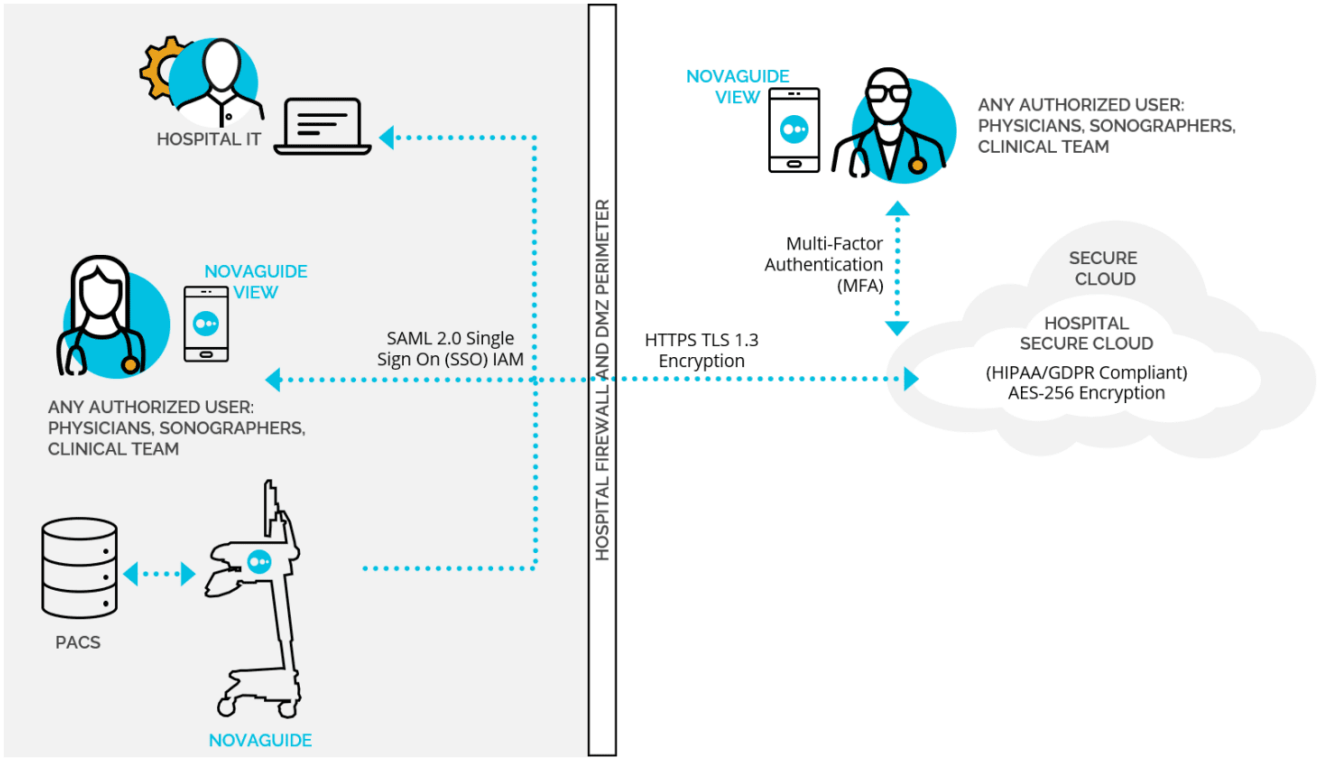


A growing segment of customers want local storage and AI/ML processing, such as hospitals, lawyers and accountants etc.

Edge Computing Security Challenges

- Definition of Cloud has been expanding, getting out of a data center
- Resources on Edge need to be adaptive, for varying amount of compute
- Perimeter defense is insufficient, as no fixed perimeter for Security
- A fixed universal security policy is inadequate, each party owns their data
- Fixed protocols for boundaries of security fail, need shared security model

An Healthcare Example*



Need a distributed trust model comprising of trust and mistrust scores

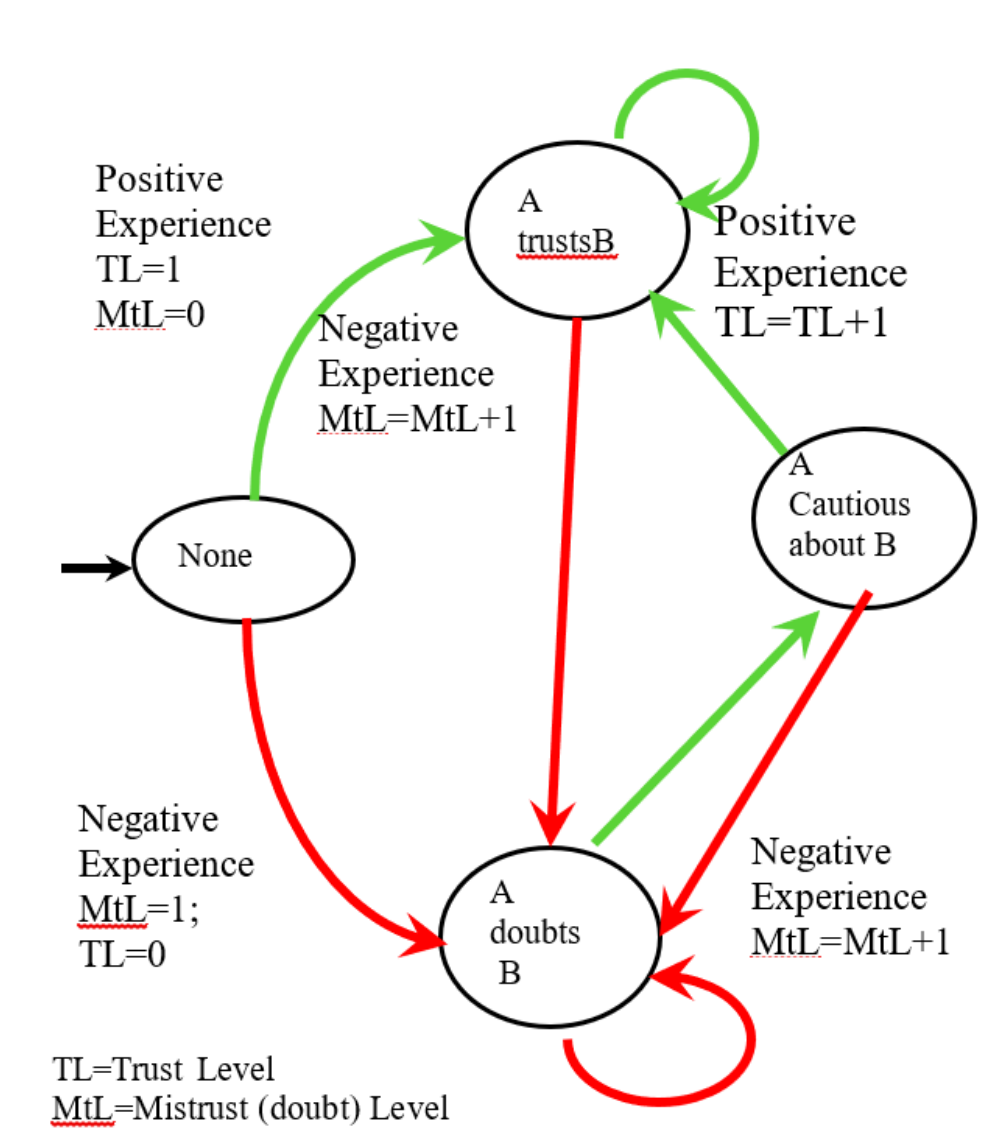
*https://www.neurasignal.com/support/security

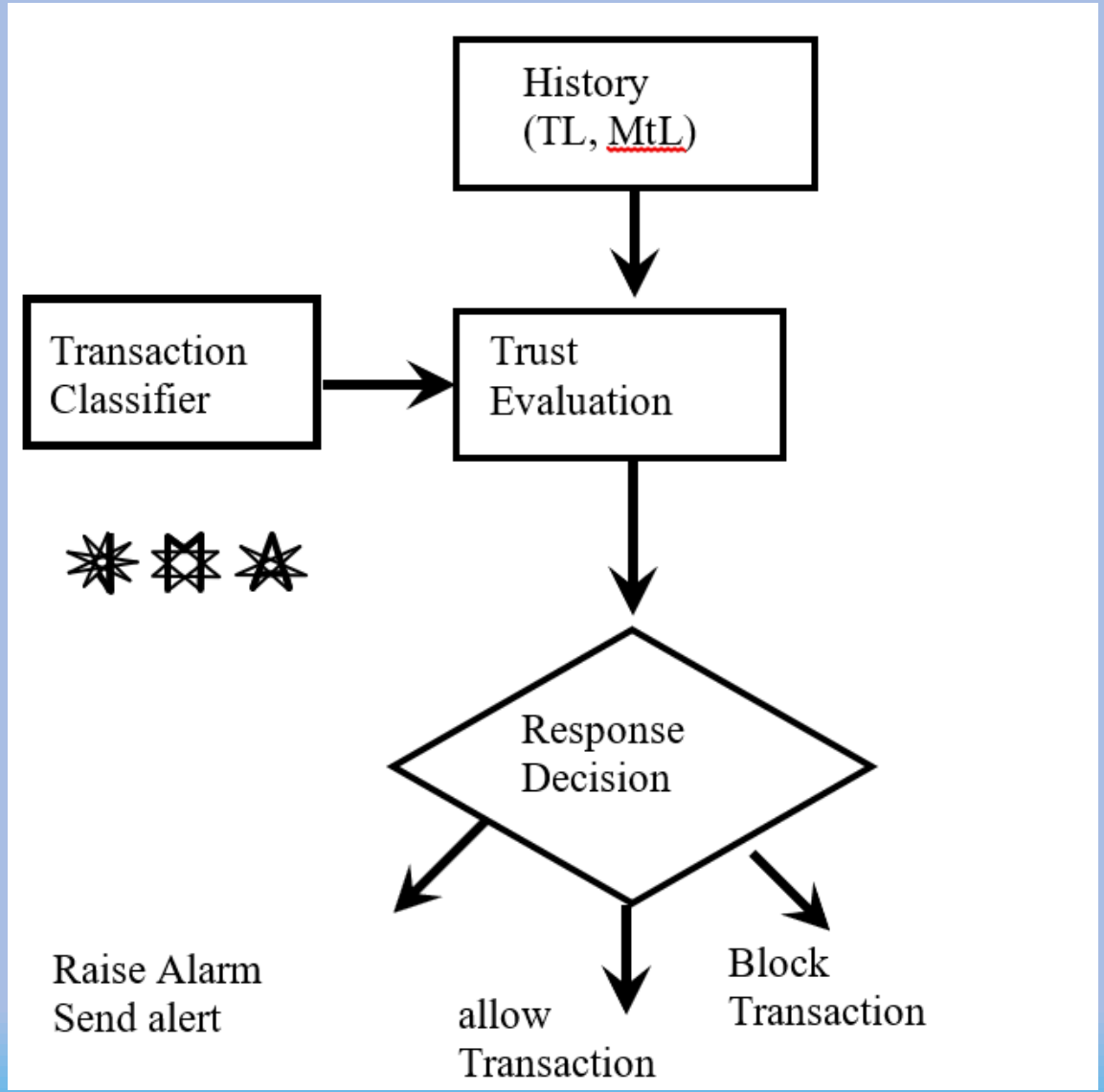
Trust between Pairs is Not Mutual

Trust Relationships	Trusted party			
Trusting Party ↓	Sonographer	Reviewing Physician	Referring Physician	Patient
Sonographer	X	Yes	Yes	NA
Reviewing Physician	Yes	X	Yes	NA
Referring Physician (or PCP = Primary Care Physician)	Yes, to conduct the exam, but not to interpret its results	Yes	X	Yes
Patient	Yes	Yes	Yes	X

excludes parties trusting devices

Trust Evaluation between two entites

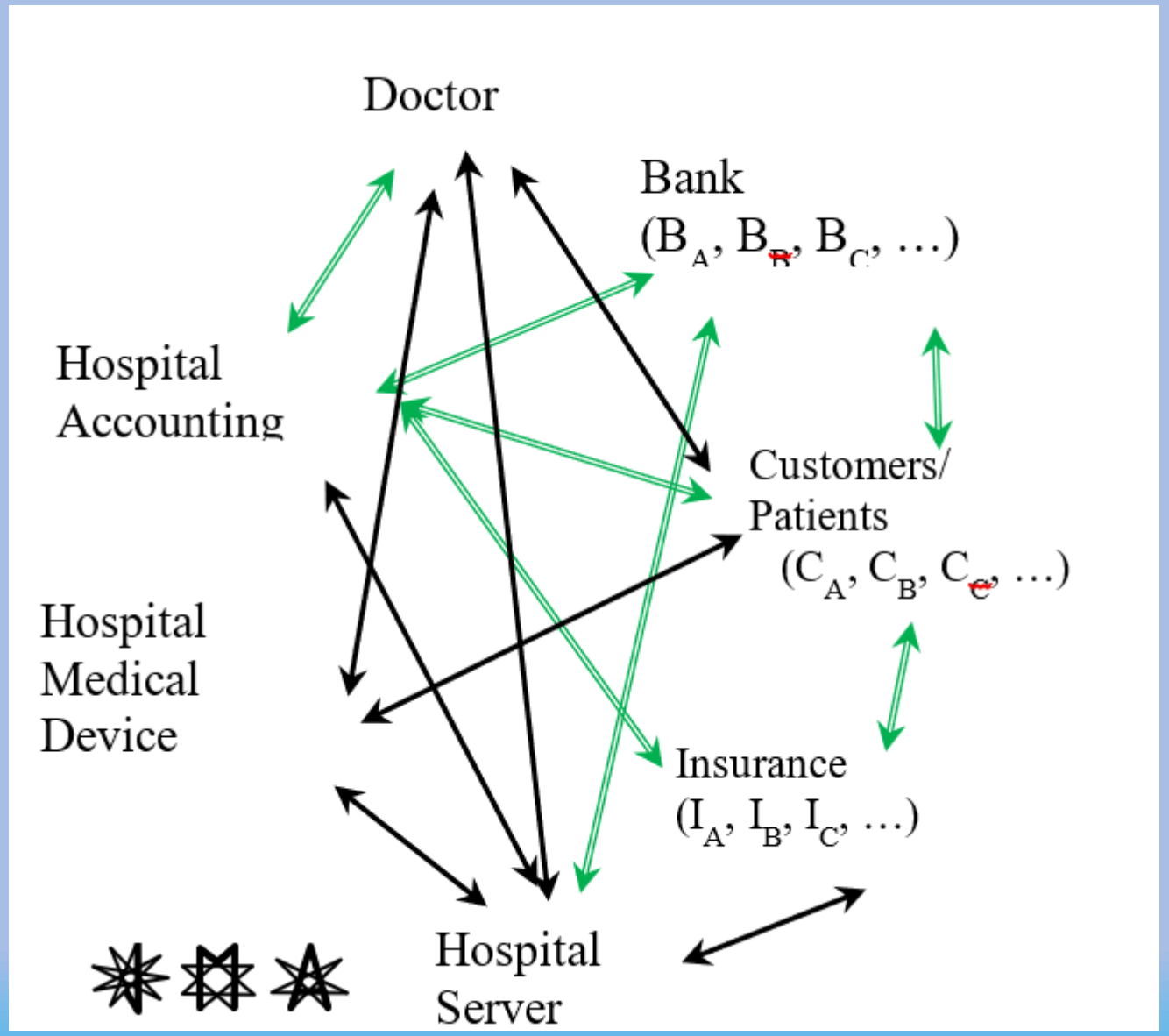




A distributed Trust model can be built by extending the trust relationship between a pair of entities

A Distributed Trust Model

- Identify the type of relationship, e.g., Medical or Financial?
- Medical: Information, tests results and advice etc.
- Financial: billing and payments etc.
- A Patient can set TL (trust level) for a doctor based on the care given.
- A Patient can set TL for a hospital upon billing, dealing with insurance, and payment experiences etc.
- Similarly, a hospital can trust a bank or credit card company for sharing relevant patient information to do financial transactions but not share any private health information.
- A bank or credit card company may use additional information to decide, e.g., origination location of the message



Trust depends on the context and is not bi-directional

Conclusions

1. **Edge Computing is a multi-dimensional environment**
2. **Trust extends beyond people, includes computers and devices**
3. **Traditional approaches of identifying a threat and defending against it are not sufficient**
4. **Solution require a learning, responsive, varied, and individualized approach**
5. **Need a distributed trust model comprising of trust and mistrust scores**