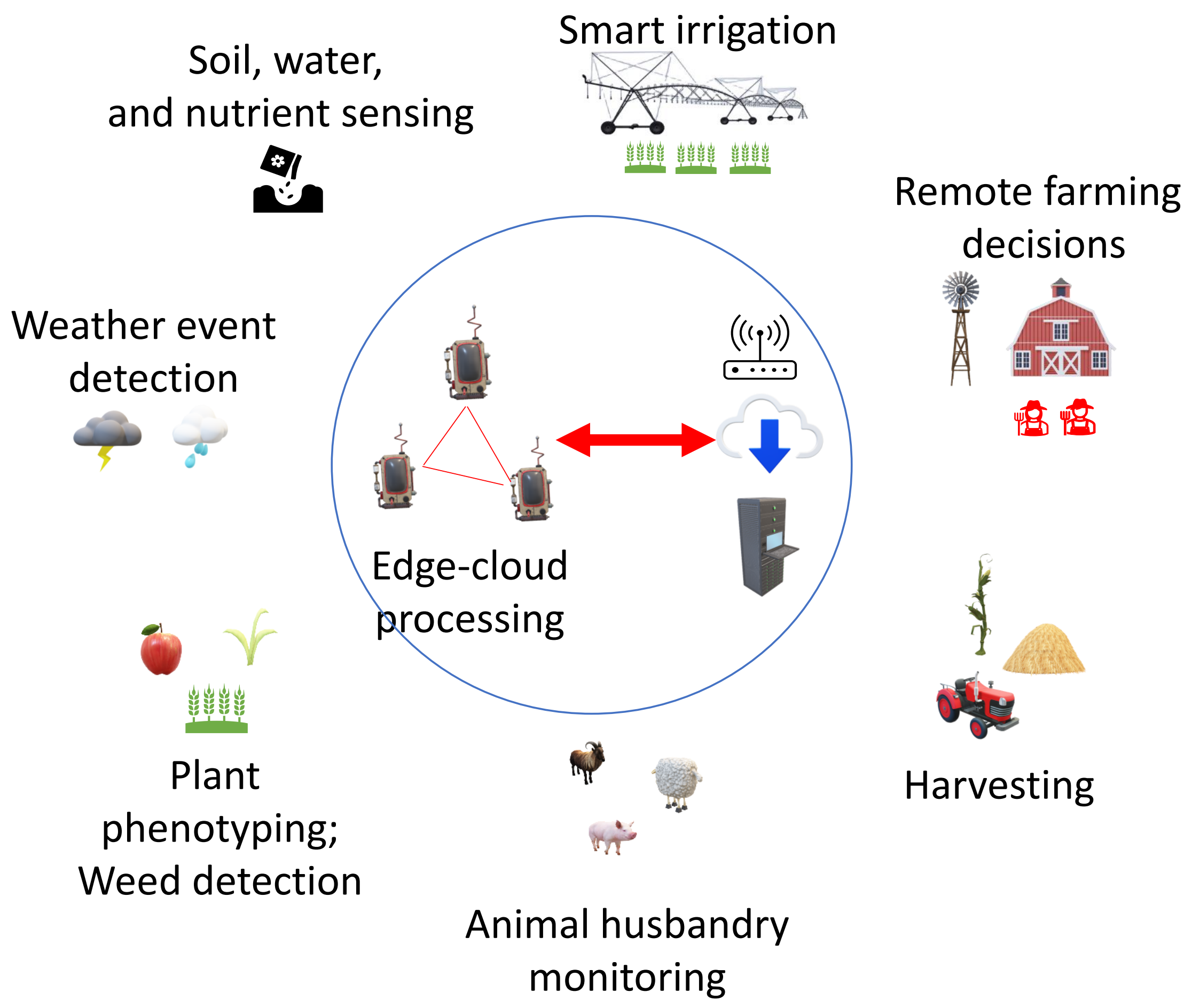
Ag-IoT Security through and Network Analysis Hardware-assisted Encryption

Sai Lamba Karanam and Dr. Byrav Ramamurthy
School of Computing at UNL

NATIONAL STRATEGIC RESEARCH INSTITUTE
at the University of Nebraska

Ag-IoT: Why is security important?

Ag-IoT [1] automates the agricultural process such as smart irrigation, abnormal weather detection, crop monitoring, plant phenotyping, animal husbandry, and others. Edge-IoT [1] is the primary means of smart agriculture deployment.



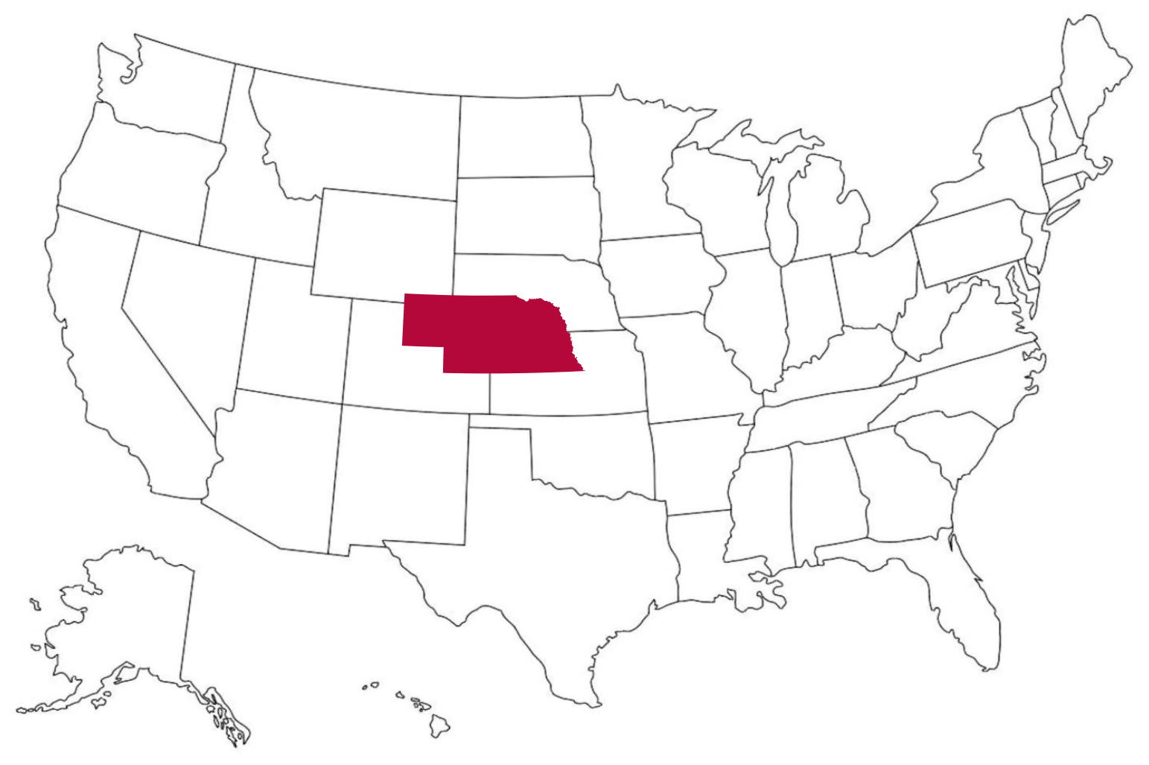
Food security is a major strategic initiative for the US. Ag-IoT can help facilitate the food security processes via automation of agricultural processes which improve the productivity.

Wired and Wireless communication is a core component in AG-IoT and any potential attacks on the network can lead to the following consequences:

Potential consequences of an attack include

1. Control of the irrigation operations
2. Compromise the network and important data
3. Tampering with sensor readings
4. Monetary consequences

Agriculture in Nebraska



Total GDP: ~$161 B. [4]
% of total employment by agriculture: 25%
%of total GDP: ~25% [5]

Contributions

Protection techniques need to be more complex than the threats themselves. Security measures begin with (i) threat prevention and (ii) detection.

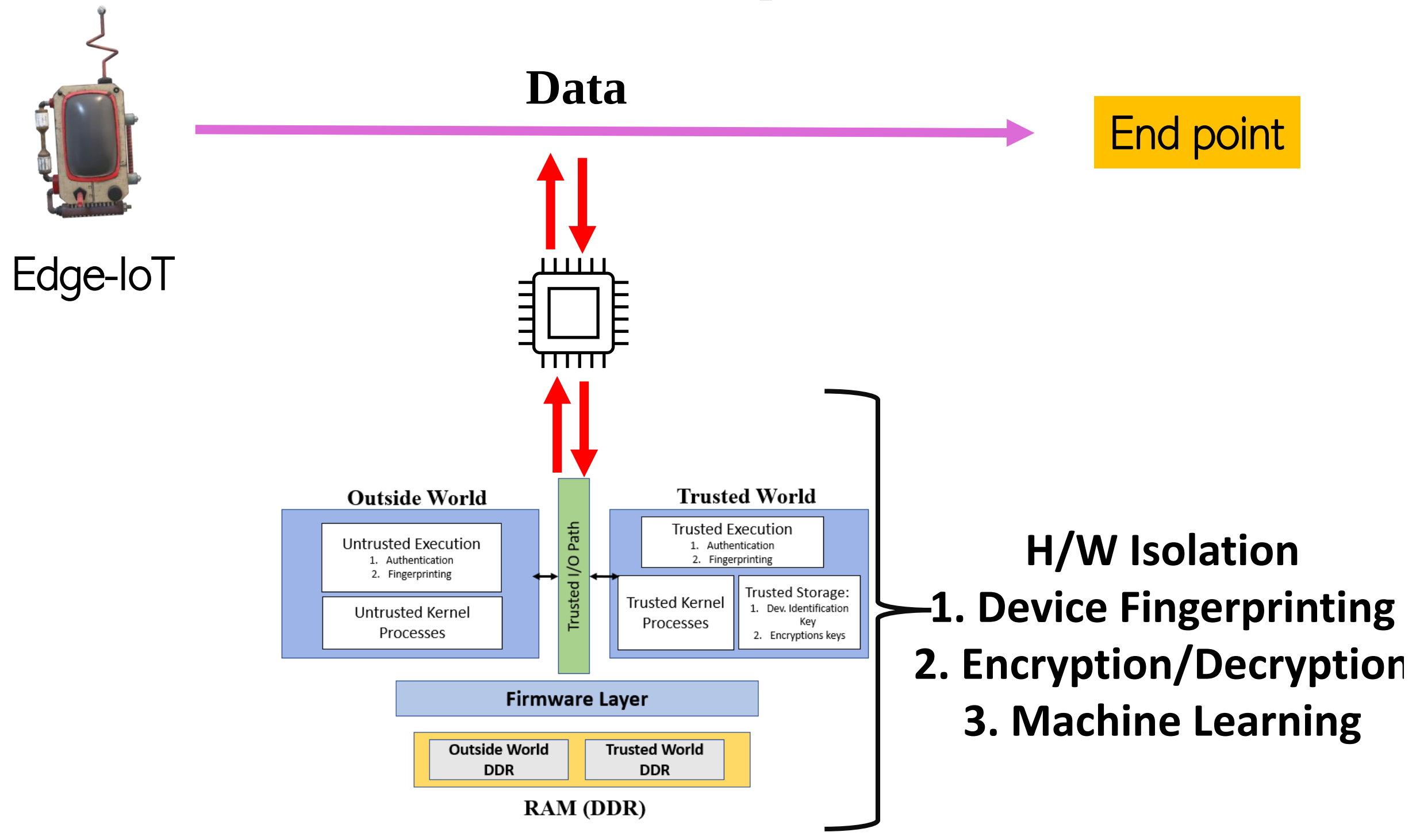
We propose two major contributions to secure Ag-IoT:

1. Network packet analysis at multiple points in the network formed by the IoT devices, servers, and the cloud/storage.
2. Novel hardware isolated security to complement the network analysis to:
    - Protect the data encryption/decryption process. The data encryption and decryption is done inside the protected zone. This means that an attacker cannot “sniff” the decrypted data at the receiver end.
    - Perform device fingerprinting is a technique to identify potentially malicious IoT devices. An attacker can masquerade as a harmless device and compromise the edge-IoT network. Device fingerprinting analyzes the communication between the IoT devices and/or the outside network to classify the device as potentially malicious or safe.

- Test our approaches on the testbed and in an agricultural setting.

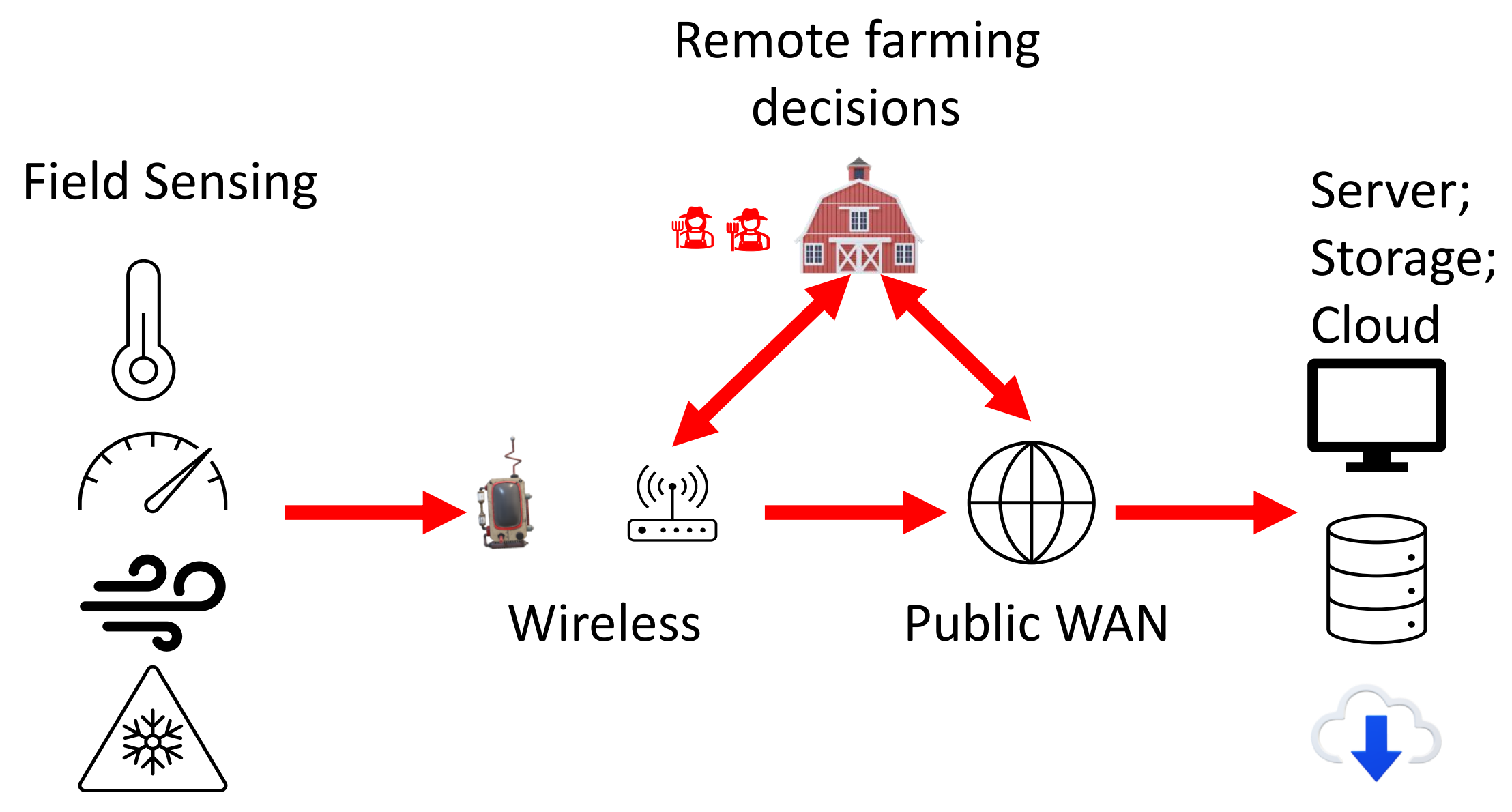
Hardware Security Design

Hardware Isolation [3] provides a highly-secured environment that is hard for an attacker to compromise.



- Any processing inside the hardware isolated zone is not available to the programs outside.
- Hardware isolated zone is like a **black box** once deployed.
- Running security measures inside the hardware isolated zone protects them from tampering etc.

Typical Ag-IoT Topology



Experimental Setup

For the first contribution, we performed preliminary analysis on large network datasets to identify patterns and understand the typical network traffic behavior. We plan to extend this work to an Ag-IoT setting.

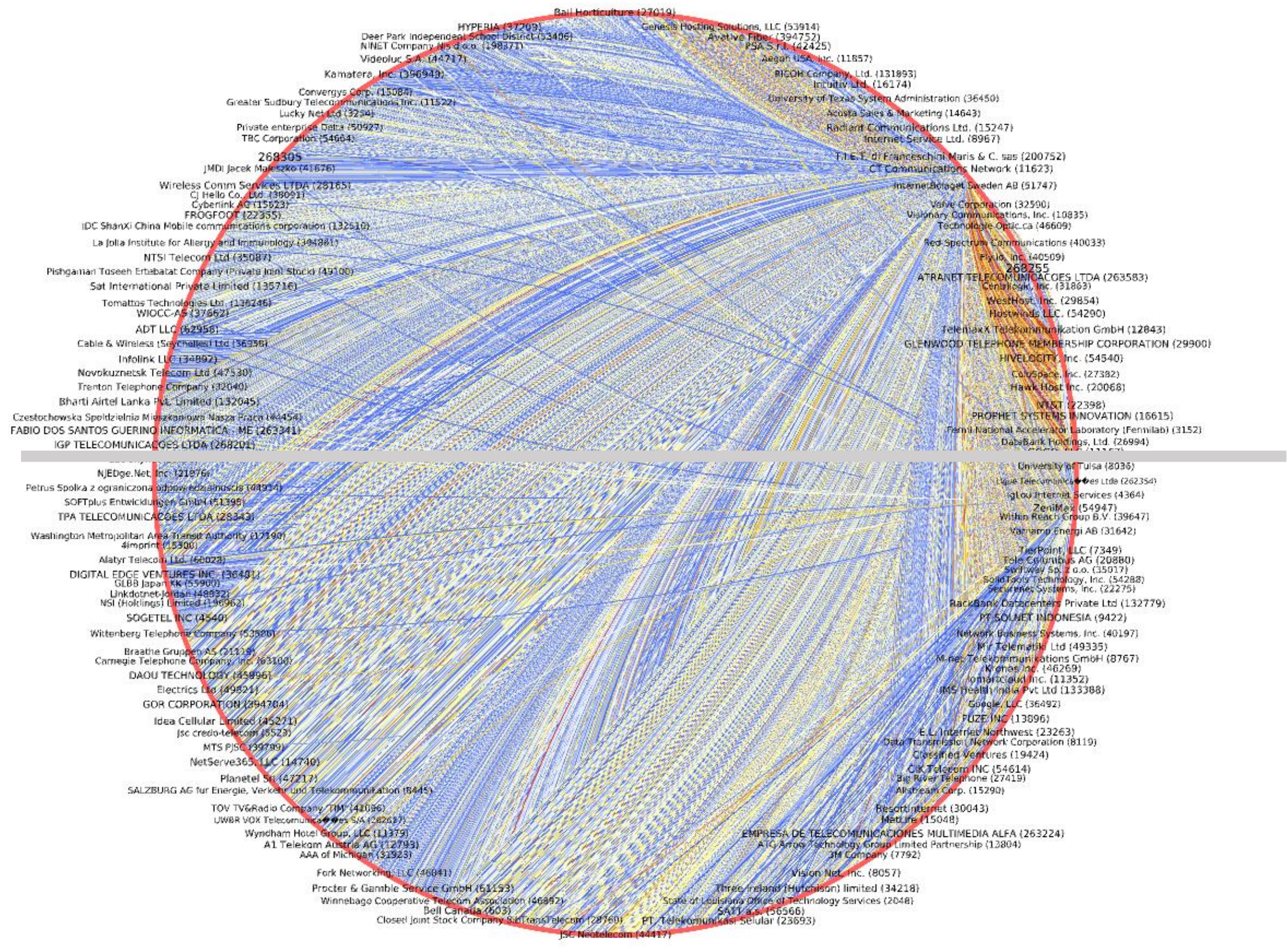
For the second contribution, we are currently implementing hardware security solutions using FPGAs and IoT devices for device identification. We are also developing a simulation model using NS-3 [3] for Ag-IoT network simulations.

Preliminary Work

We previously developed large scale network data analysis frameworks to observe patterns in network traffic.

The figure below visualizes the aggregated traffic between cities across the globe, The network dataset was collected over a time period of 3 months, with the size of the dataset being ~170GB per day.

We will utilize our network analysis framework to achieve our stated goals with Ag-IoT.



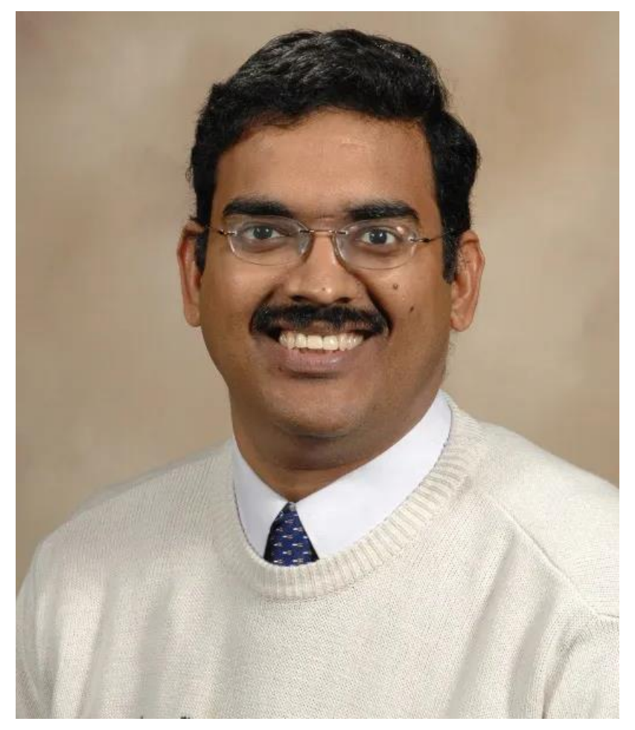
Conclusion & Future Work

- Increasing integration of automation and IoT to improve food production opens up several vulnerable components in the communication aspect i.e., wherever data is involved.
- Motivated by the weaknesses in the current state-of-the-art in Ag-IoT, we propose and are currently developing Ag-IoT security measures to ensure the food safety:
- Network packet analysis in Ag-IoT to identify suspicious network traffic patterns to detect malicious traffic.
- Hardware isolation to not only implement smart security measures but also to ensures their security. Hardware isolation technology is now available on the edge-IoT devices that are used in the smart agriculture.

Team

Sai Lamba Karanam

Dr. Byrav Ramamurthy



References

1. Nadig, Deepak, Sara El Alaoui, Byrav Ramamurthy, and Santosh Pitla. "ERGO: A scalable edge computing architecture for infrastructureless agricultural internet of things." In *2021 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*, pp. 1-2. IEEE, 2021.
2. Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." *IEEE Communications Surveys & Tutorials* 2, no. 8 (2006): 2-23.
3. Riley, George F., and Thomas R. Henderson. "The ns-3 network simulator." *Modeling and tools for network simulation* (2010): 15-34.
4. Institute of Agriculture and Natural Resources. University of Nebraska-Lincoln. Accessed April 11, 2023. https://ianr.unl.edu/growing/report-agriculture-critical-nebraska-economy-states-resilience.
5. “Gross Domestic Product: All Industry Total in Nebraska.” Federal Reserve Bank of St. Louis. ECONOMIC RESEARCH-Federal Reserve Bank of St. Louis, March 31, 2023. https://fred.stlouisfed.org/series/NENGSP.