CERIAS

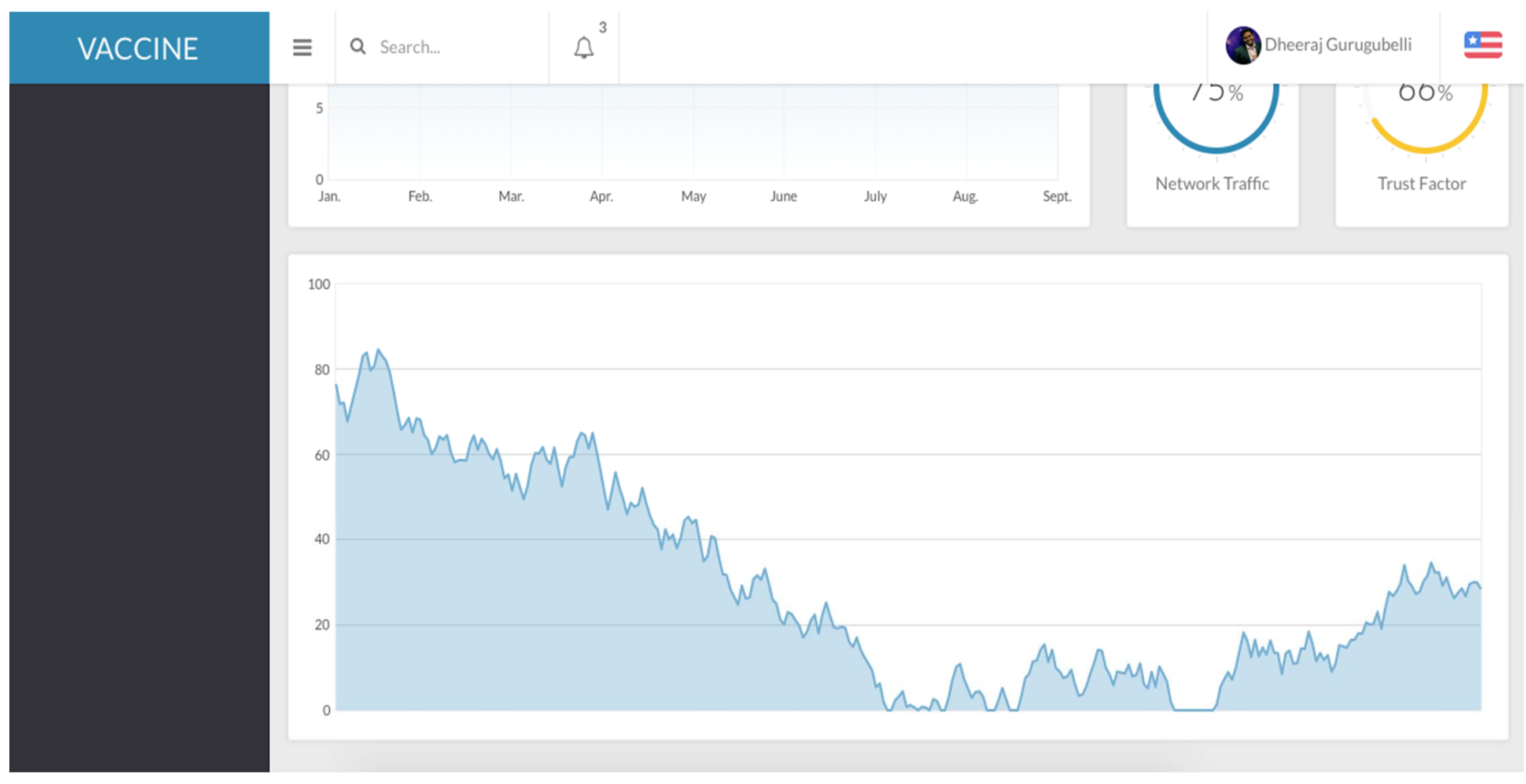
The Center for Education and Research in Information Assurance and Security

Achieving a Cyber-Secure Smart Grid through Situation Aware Visual Analytics

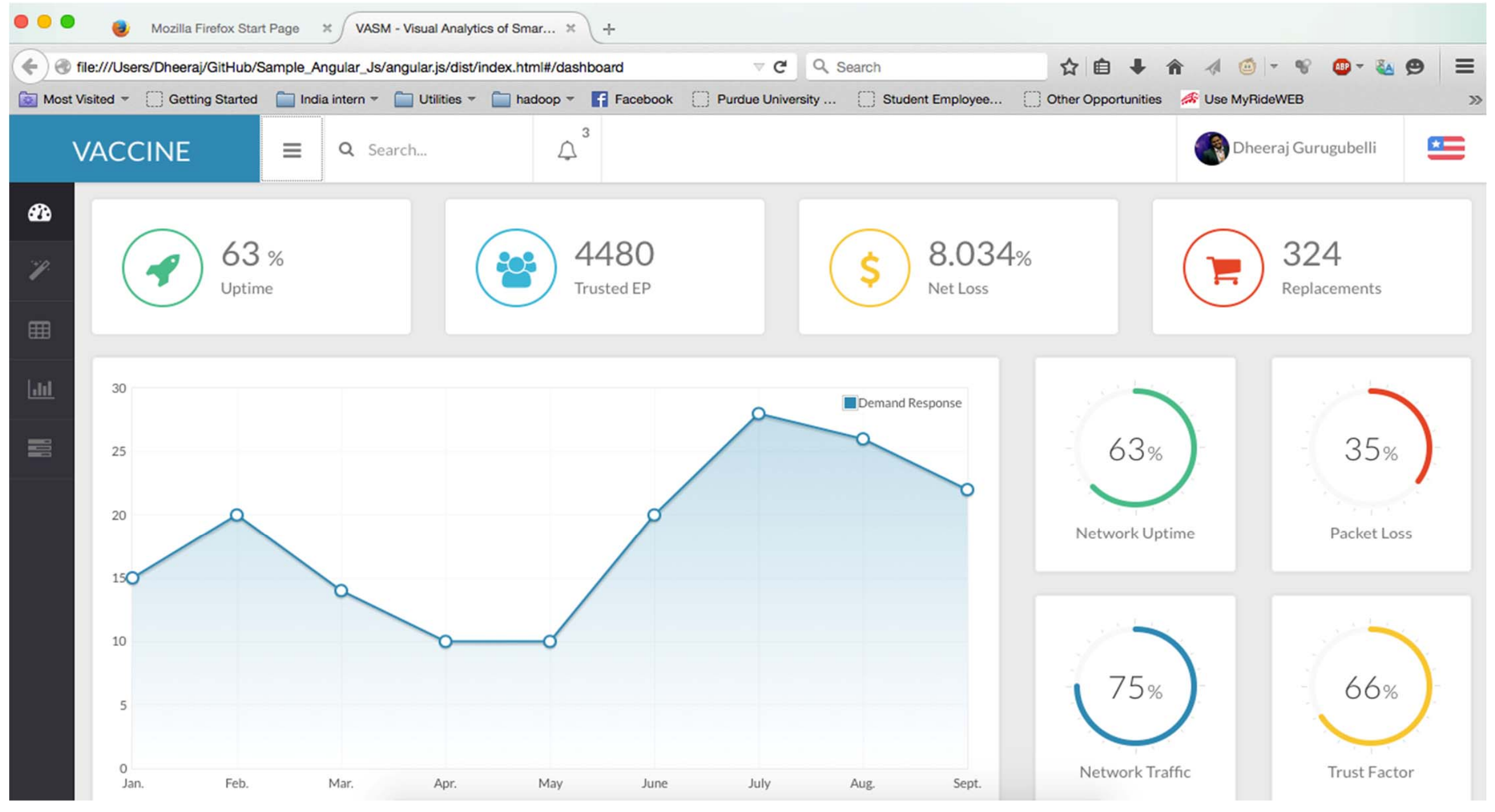
Dheeraj Gurugubelli[1], Dr. Chris Foreman[2] and Dr. David Ebert[3]
[1]Department of Computer and Information Technology
[2]Department of Electrical Engineering Technology
[3]VACCINE Labs
Purdue University

Abstract

Utilities face enormous pressure to streamline their operations and provide consumption information to the consumers for better energy management. Smart meters have been instrumental to achieve better energy management. But alike any new deployment of technology, smart meters are prone to cyber attacks. Except, in this case they are part of critical infrastructure of the nation. The goal of this project would be to leverage visual analytics for delivering near-to-real-time visual insights on smart meter data that will help make quicker in times of a cyber response need. Cybersecurity of the Advanced Metering Infrastructure (AMI) continues to be one of the top research priorities in the industry right now. Securing the smart grid is about managing a continuum of risk across all the components in the grid within the right timeline. Performing analytics and making decisions based on large volumes of network data in real-time would boost the response time significantly. This research aims at visualizing network data obtained from processing the end-component profile data and network data from the AMI networks through a distributed data processing model.



Monitor network traffic and anomalies real-time

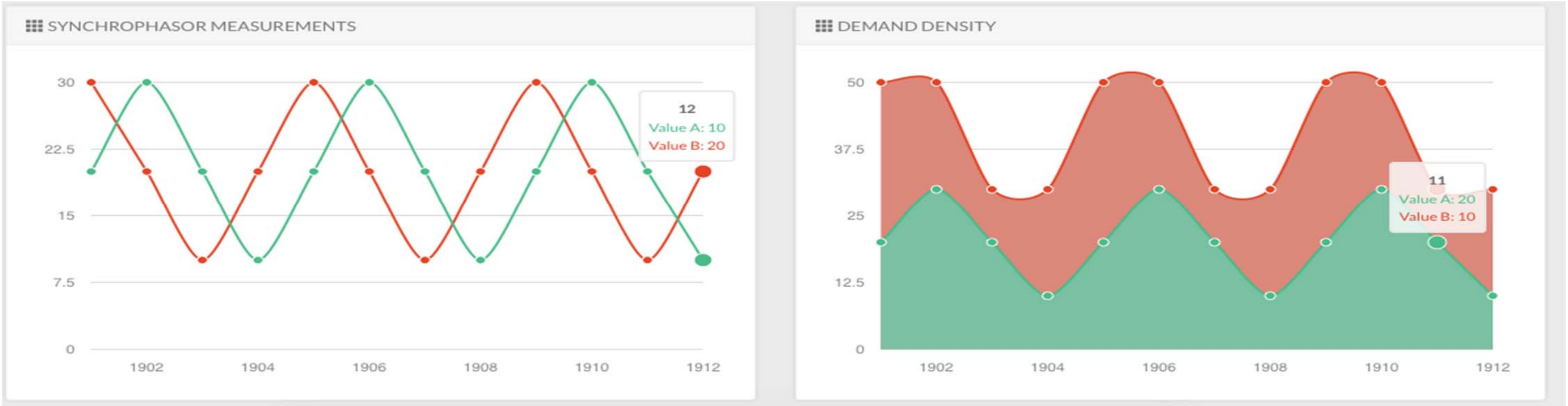


A few snapshots of the web based Grid Dashboard built

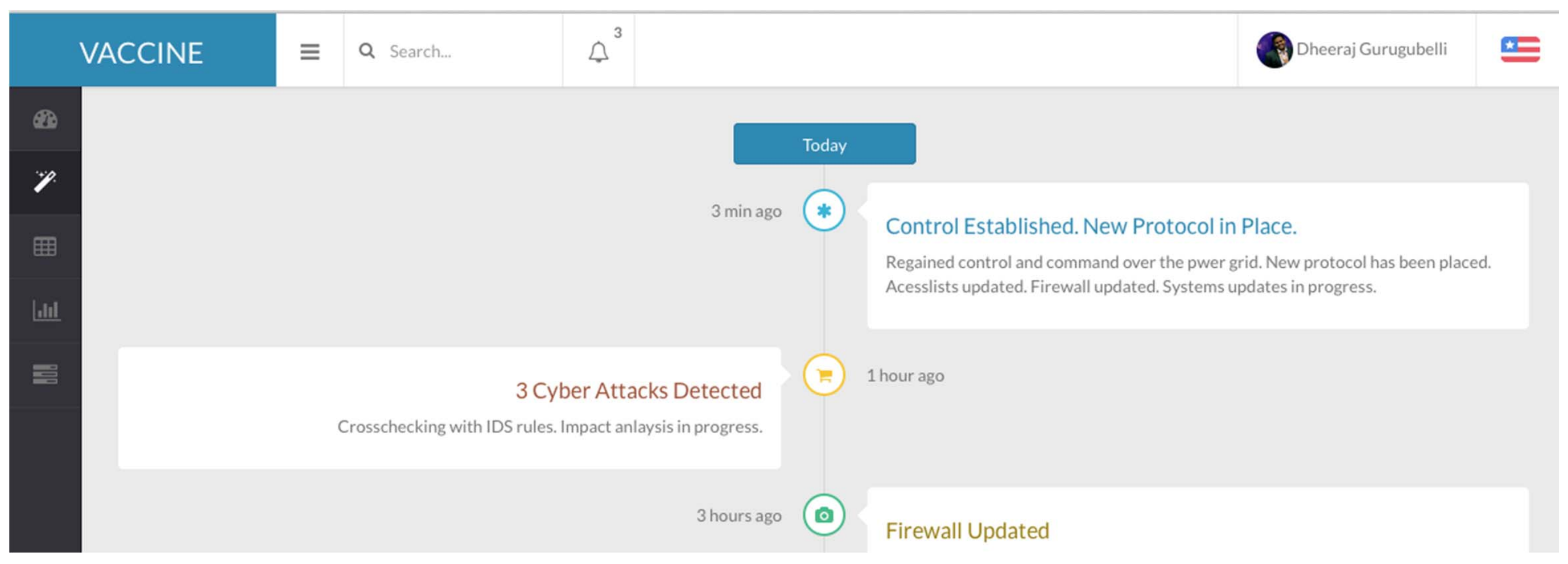
Underlying Stack

The web application built will be using the following technology stack:

- AMI Meterology Capture Layer: Apache Flume
- Data Bus: Apache Kafka
- Stream Processor: Apache Storm
- Real-Time Index and Search: Elastic Search
- Long-Term Data Store: Apache Hive
- Long-Term Packet Store: Apache Hbase
- Web Platform: Angularjs and Ruby on Rails
- Visualization Platform: Using Kibana, Jquery and D3.



Near-to-Real-time metrology data monitoring



3 min ago

Control Established. New Protocol in Place.

Regained control and command over the pwer grid. New protocol has been placed. Acesslists updated. Firewall updated. Systems updates in progress.

1 hour ago

3 Cyber Attacks Detected

Crosschecking with IDS rules. Impact anlaysis in progress.

3 hours ago

Firewall Updated

Real-time cyber critical notifications timeline

Implementation

Phase 1:	Designed the implementation framework
Phase 2:	Setup Required configuration and data capture
Phase 3:	Ingest Cleansing and Analysis
Phase 4:	Streaming Real-Time network data with Storm
Phase 5:	Visualization of real-time network data and cyber attack alerts using spatiotemporal visualization.
Phase 6:	Threat Reporting and Results

Current Work

Applying cyber attack signatures and rules to stream processing filters and network attack analytics module.

CERIAS®

PURDUE
UNIVERSITY