NORTHROP GRUMMAN
ENGINEERING & SCIENCE STUDENT DESIGN SHOWCASE
FLORIDA TECH

Project Thor: Creating Randomness Using Lightning

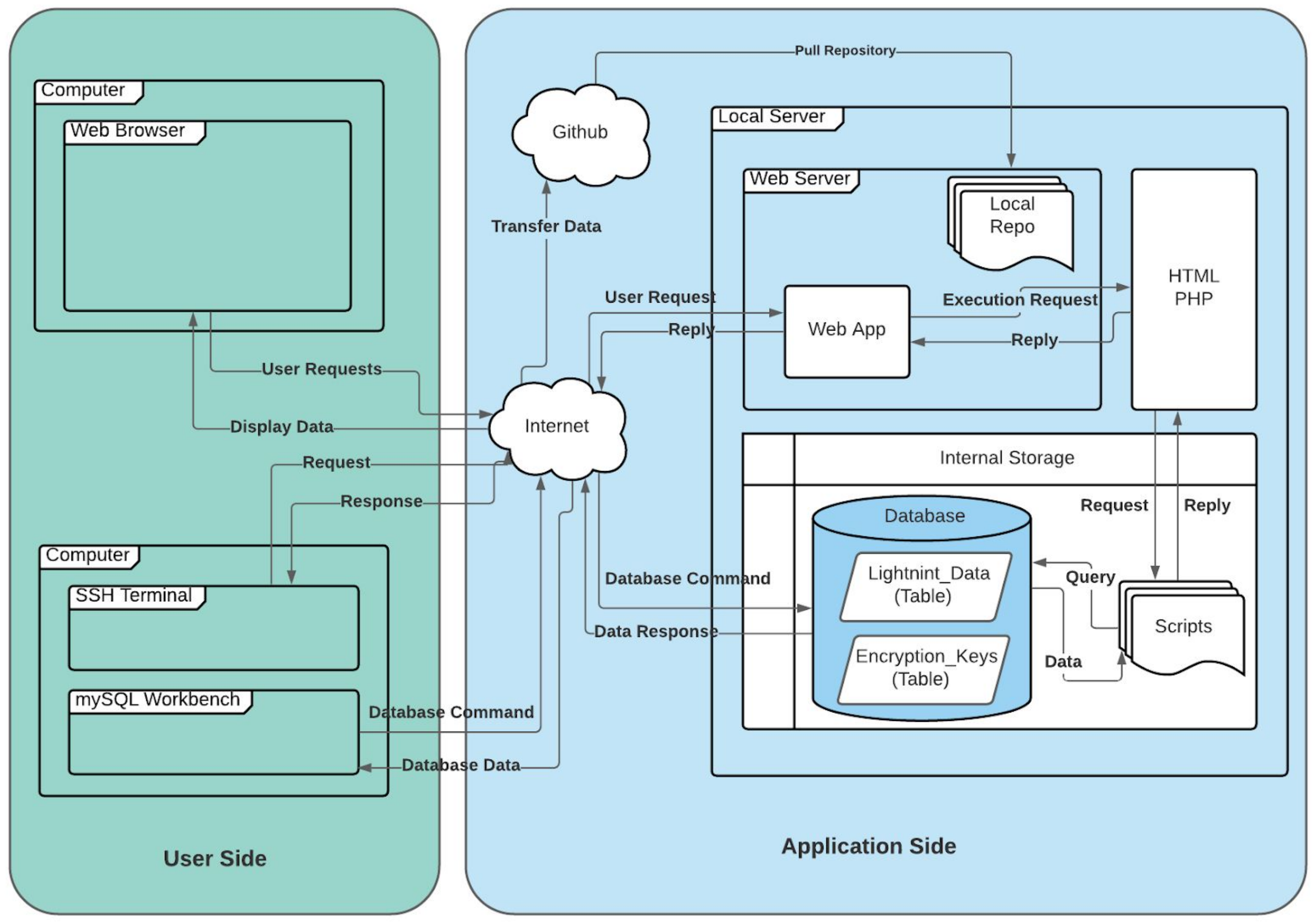
Josh Temel, Adonay Pichardo, Jared Blanco, Luke Bonenberger
Faculty Advisor: Dr. Siddhartha Bhattacharyya, Dept. of Computer Engineering & Sciences, Florida Institute of Technology
Sponsor: Dr. Amitabh Nag, Dep of Physical & Space Sciences, Florida Institute of Technology

Motivation

- Random numbers are the backbone of security and encryption algorithms. Therefore, if an attacker can predict the random numbers used to generate your encryption keys, then they can overcome your security. Our team hopes to address the problems with sources in currently used random number generates being predictable, infiltrators being able to observe the sources of randomness, and being infiltrators being able to manipulate sources of random number generators.
- We hope to improve todays used encryption methods by exploring other techniques for creating random numbers.

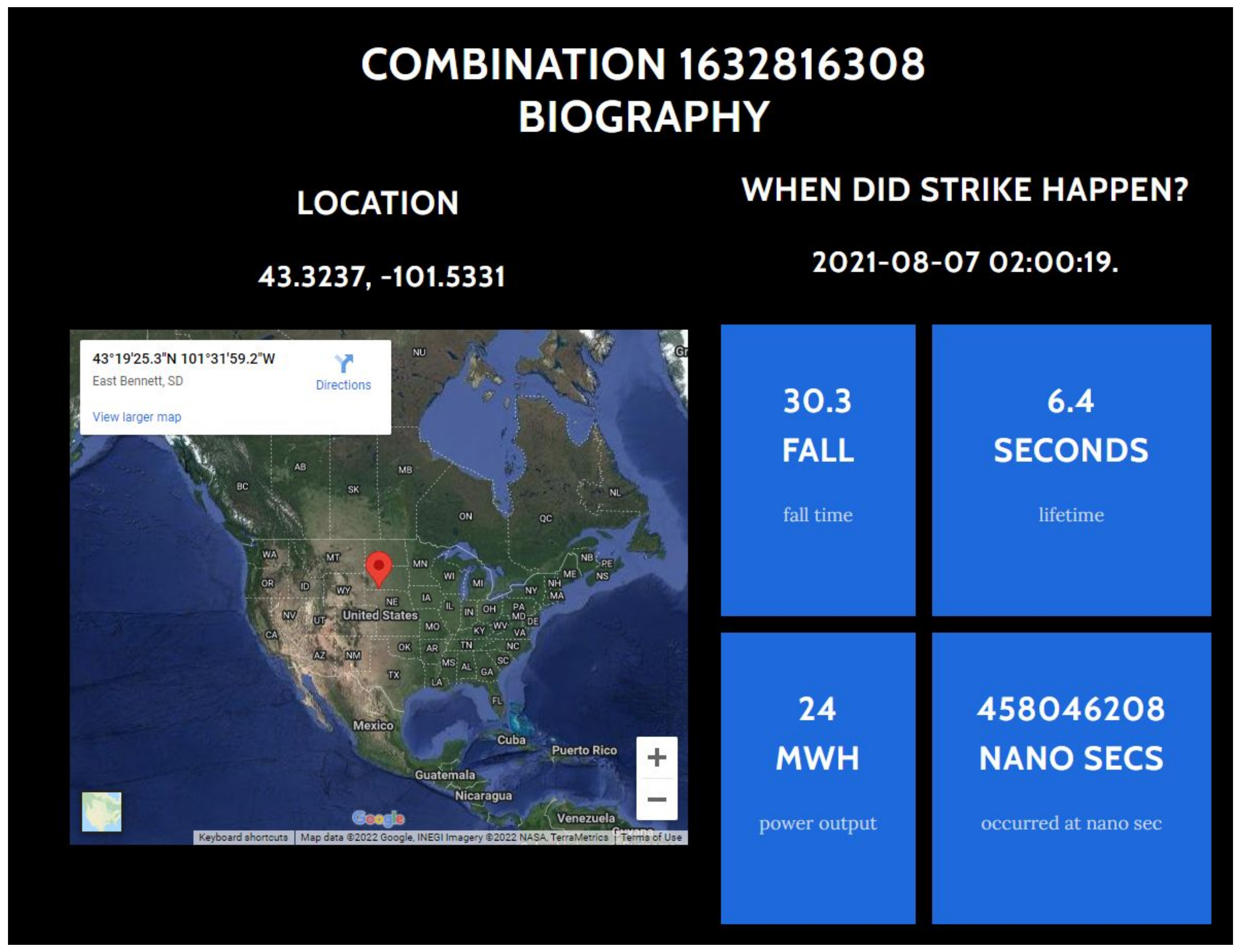
Project Goal

- The Project Thor team hopes to use natural phenomenon data in order to provide less predictable seed values for later encryption.
- For our project specially, we have selected lighting to be our source of natural phenomenon data.
- Our team will be taking in data provided by the clients numerous lightening detectors located across the country and use that data to produce a naturally fueled encryption key.
- This key generation process is intended to be supported by a web application and database.



Features

- **Key Generation Using Natural Phenomena Data**
  - Our program is utilizing lighting data as our source of natural phenome data. This lighting data is collected and provided to us from Florida Tech's physics department that uses nodes around the country for collection.
  - The key is than generated by equally weighing the selected fields from the lighting strike and combining them. This can be done either by combining all fields from one lighting strike to provide the user a key that is specific to that strike or utilizing multiple lighting strikes to generate the key.
- **Data base for key storage**
  - The Database has several tables/relations to store data as it is taken from a simple ASCII file, is parsed into our specific format, and then stored into separate tables after it has been mutated to our useful random numbers.
- **Web application for key access**
  - Generate keys and encrypt files using lightning data with AES encryption.
  - See where the lightning strike occurred, its duration, power output, and other attributes which corresponds to generated key or encrypted file.



COMBINATION 1632816308
BIOGRAPHY

LOCATION

43.3237, -101.5331

WHEN DID STRIKE HAPPEN?

2021-08-07 02:00:19.

30.3 FALL fall time	6.4 SECONDS lifetime
24 MWH power output	458046208 NANO SECS occurred at nano sec

43°19'25.3"N 101°31'59.2"W
East Bennett, SD
Directions
View larger map
United States
Mexico
Cuba
Puerto Rico
Guatemala
Nicaragua
Venezuela
Keyboard shortcuts | Map data ©2022 Google, INEGI Imagery ©2022 NASA, TerraMetrics | Terms of Use

Future Improvements

- Provide our random number generators via a python library instead of a web application. This would allow for easier implementation and use of our generated seed values.
- Include a dropdown list of encryption algorithms to be utilized from our web application that would be seeded by our weighted lightning data.
- Implanting a rolling data base of constantly updating lightning strikes.
- Implementing a rest API for our web application for easier pulling of keys.
- Optimizing key generation process through more in-depth hashing algorithms through the data base as well as implementing a more efficient duplicate key prevention system.

Security Risk

- If the data base would become compromised, any infiltrator would currently have access to all utilized fields and past generated fields
- Lighting data could become more predictable with scientific advances
- Keys generated by a single lighting strike still can be reversed engineers if the strike time is known

Other Application for Data

- Modern best practices rely on pseudo random
- Keys are currently being utilized in the context of cyber security but there are additional ways to utilize these keys such as game theory, computer simulations, statistical samples, and password generation are all areas this data could be used.

Acknowledgments

- Dr. Siddhartha Bhattacharyya and Dr. Chan for their continued guidance
- Dr. Amitabh Nag for providing the lighting data
- All classmates for amazing project feedback