Gursharan Singh, Rishik Kolli, and Sharmila Nimbkar

Dr. Trowbridge

Grand Challenges for Engineers

19 February 2021

Solution Development and Description

Context:

A lot of US government owned energy utilities struggle with the problem of protecting important data and ensuring that their software cannot be accessed by foreign users through the internet or poorly coordinated systems that do not ensure the safety and control of important data. The US government needs a solution that can secure site materials and data by detecting potential dangers and threats and protecting classified matter on both the state and federal levels. Securing private data is so important because the US power grid loses about $6 trillion dollars annually to cyber attacks [7]. Many services across the nation rely on the need of electricity and the impact of securing energy can be crucial to ensuring that cities, hospitals, military bases, businesses, and our economy continue to run as normal. Making sure our solution ensures that our customers have a reservoir of energy to fall back on and connecting different systems of energy will be crucial. Securing energy infrastructure does not only impact the American government and the United States Department of Energy but also the 330 million people living in America.

10 potential brainstormed ideas:

1. **Creating Analog System to prevent access from internet (also known as an "air gap"): this would entail the US energy facilities not being connected to public storage facilities like the cloud or connected to the internet**
2. **AI software that constantly keeps note of current and potential vulnerabilities (systemwide and individual): the AI software uses past analytics and data to find potential dangerous patterns or anomalies occurring with the main software of the energy plant**
3. Problems with false data injections and being able to detect false data injections with AI: using previous data and gathering and storing previous data stored by scientists in the lab, the AI can cross check the work of scientists and make sure that false data is not being imputed into the software which could be catastrophic
4. Problems with the traditional grid that relies on the delivery of electricity from generation to end-users (one direction): think of your myAsu double authentication, makes sure that before entering data that two people multiple user must verify data before being entered into software
5. To combat the previous problem have a Smart Grid which consists of a vast array of devices and systems with two-way communication and control capabilities: instead of one device inputting data into the software, multiple users have to input data that matches from multiple devices. This is helpful since threats on one device do not affect the other device.
6. Having multiple companies or energy companies working together. The AI gathers data from all sites and stores the data in a mainframe to cross-reference the data. This

mainframe that communicates with all energy plants would create a vast amount of data and a vast array of possibilities that can be used for cross reference for suspicious trends.

7. **Blockchain system that detects when suspicious data is being entered into the smart grid. Blockchain relies on confidentiality, integrity, and availability. Confidentiality relies on inscription and communication in secret from other users. Integrity would verify data with cross-referencing history. Availability allows multiple users to contain multiple copies. Can't wipe out data if there are multiple copies.**
8. Restructure existing cyber infrastructure to support existing encryption methods like AES and DES
9. Create a software that has high levels of security to prevent emails, phones, and messages from being fraudulently accessed on these networks where information sharing is prevalent.
10. Creating an organization that can spend more time and resources dedicated toward fighting cyber attacks and deafening against them one person at a time.

Solutions Considered and Decision Making

The top three solutions include creating an "air gap" to disconnect the systems from the internet, using AI software to keep track of current and potential vulnerabilities, and a blockchain that can detect when suspicious data is being entered into the smart grid.

First, disconnecting the power generation station from the internet is a foolproof method for preventing hacking through the internet. This is already a tactic that is used by nuclear power generation stations to prevent the weaponization of nuclear reactors by foriegn or nefarious hackers [1]. This method would provide strong protection but poses a slew of pragmatic challenges when trying to implement the smart grid or any kind of AI security technology or the smart grid.

The second solution is to create an AI which finds, detects, and possibly patches potential and current vulnerabilities in the network or energy producers [3]. This AI could scan and create registries of certain vulnerabilities, and as it continues to detect and fix threats, it will get better and better at doing so. However, the downside of this is that the infrastructure in the energy sector is severely lacking currently, and this solution would probably take a long time to implement effectively.

The final potential solution is to implement AI in conjunction with the Smart Grid, since a current issue that the energy sector faces is hackers introducing false data into the network to manipulate or corrupt smart grid metering systems [1, 2]. The potential solution would include an AI that can detect when suspicious behavior is occurring on the grid, flag it, and report it to someone who can investigate it. This could be accomplished using blockchain technology, which basically serves as an unalterable leger of past transactions and data transfers, allowing the AI to detect communication with suspicious parties within the Smart Grid. Since Smart Grids are an inevitable consequence of the progression of energy infrastructure and the internet of things, creating a system that can preemptively block and detect suspicious behavior is a necessity. The downsides to this is that the infrastructure in the energy system would have to be updated, and that increasing interconnectedness with the internet to implement IoT Smart Grid systems would increase vulnerabilities.

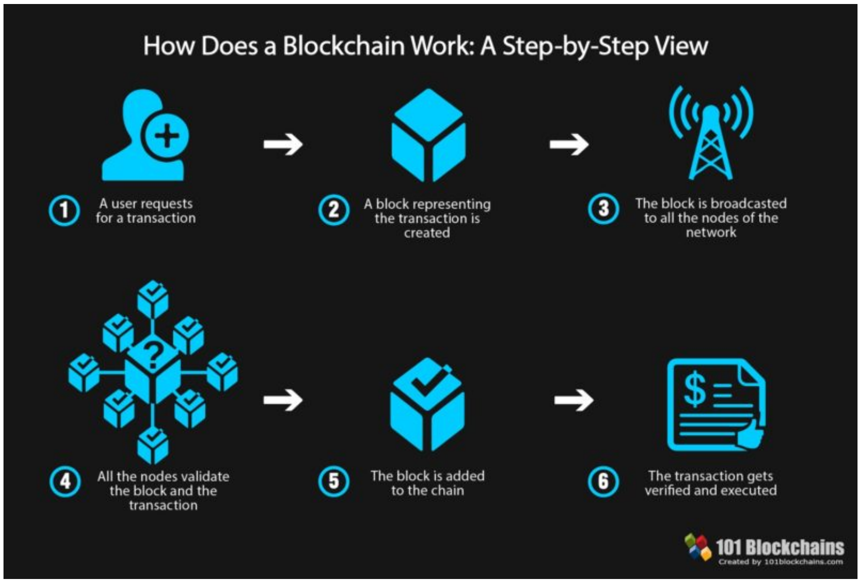
Ultimately, the best solution is an AI system combined with blockchain technology that flags, detects, and patches vulnerabilities within both the network in general and the metering system in particular. This technology would have the least downsides while providing the most benefits. It would have to be implemented quickly and correctly, but wouldn't require a new inertial shift in the industry or government since smart grids are a system that are being implemented on most grids anyway. The downside is that implementing smart grids would increase vulnerabilities in the current system, but this solution will hopefully diminish these dangers and help smart grids be used effectively and safely [4].

Solution Description and Function:

The solution to securing the US grid from cyber attacks is transformation of it into a type of blockchain. Blockchain has the triad of attributes of confidentiality, Integrity and Availability. These attributes prevent potential vulnerabilities from occurring due to high encryption levels in blockchain. Blockchain preserves confidentiality by maintaining anonymity for all transactions and data transfers.

Additionally, blockchain provides integrity because its decentralized system in which all nodes in the network have access to the data, it has a map of authentication that allows it to confer with all other member systems of the network before any change is authenticated or data is recorded. Thus, blockchain is incredibly secure and difficult to alter, meaning it provides protection against external threats from other governments or hackers who seek to access and alter the data for nefarious purposes [6]. Since data in the blockchain is shared by the entire network and exists separately, attempting to alter information recorded on the blockchain is analogous to trying to change the DNA of an entire species one individual at a time; too many copies of the correct data exist within the system and would override the alterations.

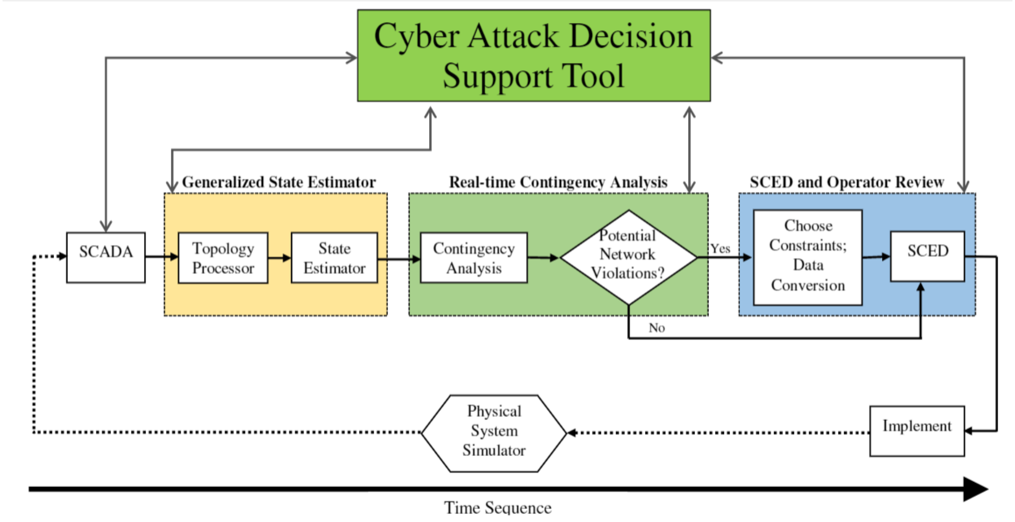
The availability of blockchain is provided by the fact that it had a self authentication system embedded inside. It gets rid of any middle man who has to be in control of managing any contact occurring between parties of the network. This self authentication mechanism creates a faster system that can be highly trusted by both parties and not having to fear any intrusion from occurring within. This also gets rid of any potential human error to occur during the management of important data and communications if there was no blockchain in place.


How Does a Blockchain Work: A Step-by-Step View
1 A user requests for a transaction
2 A block representing the transaction is created
3 The block is broadcasted to all the nodes of the network
4 All the nodes validate the block and the transaction
5 The block is added to the chain
6 The transaction gets verified and executed
101 Blockchains
Created by 101blockchains.com

[5]

Implementation or Form of Solution:

The implementation of blockchain technology will be more than enough in securing the grid, but to add more security measures in place to create a way to detect imminent threats and persistent attacks we will also have incorporation of AI. AI comes handy after all the encryption and authentication that is already in place to observe and detect continuous threats that are out of the norm. This way if there is a consistent threat of unknown communication between devices or entities that should not be occurring it can be located and dealt with. In all US owned government facilities, we need an AI predicting software machine that uses blockchain principles. The AI software keeps track and makes sure that there is no data that seems abnormal or anomalous by looking through previous data. The AI software needs to have access to the history of data that has been used in the energy plant. We need storage components for the AI software which could be massive and take up to 56,900 square feet which is the average of primary storage facilities in the United States. We need a motherboard that contains the main components of a computer and is an essential part for any deep learning device. We need a processor that executes the program that the software or computer program runs. Another essential piece of our program is a GPU (Graphical Processing Unit) which can rapidly manipulate and alter data to give accurate models of what correct data looks like in the power plant and what inaccurate or suspicious data looks like. It analyzes past data and gives strong and accurate models. However, thanks to blockchain, a central processing unit is not actually required, since the cloud allows us to harvest processing power from all the devices (phones, oncputers, servers, laptops) that already exist within the network [8].


Cyber Attack Decision Support Tool
Generalized State Estimator
Real-time Contingency Analysis
SCED and Operator Review
SCADA
Topology Processor
State Estimator
Contingency Analysis
Potential Network Violations?
Yes
No
Choose Constraints; Data Conversion
SCED
Implement
Physical System Simulator
Time Sequence

[8]

1. Kristy Hartman. “Protecting the Nation’s Energy Infrastructure: States Address Energy Security”, National Conference of State Legislatures, 2013. <https://www.ncsl.org/documents/energy/EnergySecurityFinal-10-13.pdf>
2. https://csrc.nist.gov/CSRC/media/Presentations/False-Data-Injection-Attacks-in-Smart-Grid-Challe/images-media/presentation-10_yu.pdf
3. Idaho National Laboratory. “Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector”.US Department of Energy, August 2016. <https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf>
4. https://www.technologyreview.com/2010/08/02/262366/hacking-the-smart-grid-2/
5. https://inlea.com/but-how-does-blockchain-really-works/
6. CompTIA, “How Blockchain and Cybersecurity Work Together | CompTIA”, *Youtube*, Nov 5, 2019
7. Cybercrime Magazine, “Cybercrime Damages $6 Trillion By 2021”, Oct. 16, 2017.
8. Gokkulnath T S, “Choosing Components for Personal Deep Learning Machine”, Nov 21, 2017. <Choosing Components for Personal Deep Learning Machine | by Gokkulnath T S | ML Review | Medium>