Journal of Energy and Power Engineering 16 (2022) 24-31
doi: 10.17265/1934-8975/2022.01.005

Energy Driven by Internet of Things Analytics and Artificial Intelligence

Bahman Zohuri[1], Paul E. Bowen[2], Akansha Agarwal Dinesh Kumar[1] and Masoud Moghaddam[3]

1. Ageno School of Business, Business Analytics School, Golden Gate University, San Francisco, California 94105, USA

2. California Polytechnic State University, San Luis Obispo MBA 1996, San Luis Obispo, California 93401, USA

3. AICyberDomain.com, Chief Executive Officer, San Francisco Bay, California 94501, USA

Abstract: Developing an integrated and intelligent approach to securing the ITE (information technology environment) is an emergent and evolving concern for every organization and consumer entity during the last few decades. Major topics of concern include "SI" (security intelligence), "D-DA" (data-driven analytics), "PE" (proven expertise), and "R-TD" (real-time defense) capabilities. "DRBTs" (dynamic response behavior types) include "incident response", "endpoint management", "threat intelligence", "network security", and "fraud protection". The consumer demand for electricity as essential public access and service is indexed to population growth estimates. Consumer-driven economies continue to add electrical consumption to their grids even though improvements in lower-power consumption and higher design efficiencies are present in new electric-powered products. Dependence on the production of electrical energy has no peer replacement technology and creates a societal vulnerability to targeted public electrical grid interruptions. When access to, or production of, electrical power is interrupted, the result is a "Mass Effect" every consumer feels with equal distribution. Electric grid security falls directly into the levels of authorized, and unauthorized, access via the "IoT" (Internet of Things) concepts, and the "IoM2M" (Internet of Machine-to-Machine) integration. Electrical grid operations that include production and network management augment each other in order to support the demand for electricity every day either in peak or off-peak, thus cybersecurity plays a big role in the protection of such assets at our disposal. With help from AI (artificial intelligence) integrated into the IoT a resilient system can be built to protect the electric grid system nationwide and will be able to detect and preempt Smart Malware attacks.

Key words: Resilience system, energy flow, energy storage, energy grid business intelligence, AI, cybersecurity, decision making in real-time, ML (machine learning), DL (deep learning), BD (big data), cloud-based servers for repository and storage of data.

1. Introduction

Computer network attacks continue to evolve, so any enterprise depending on the Internet or other wireless Intranet systems for commerce must evolve cybersecurity practices that respond in advance of current and anticipated threats. The concept of the IoT (Internet of Things) draws IT (information technology) users, into an operational choice where the frequency and customer volume of the enterprise business operations demands a cybersecurity capability. Effective cybersecurity policy and practices are not improved from multiple tools. The enterprise benefits from being brilliant in the basics of cybersecurity practices. Simplicity is the better practice towards security integrity. Taking the approach of fighting new threats with more tools just adds complexity with more degree freedoms that favor higher probabilities for the cybersecurity system to fail. If the organization is not seeing that "less is more", then it is time to rethink the corporate approach to cybersecurity.

The consumer economy exists because electricity is a ubiquitous, permanent, and inevitable condition of modern living throughout the world economies. Electrical generation originated as a collection of isolated municipal responsibilities that anchor the development of further stability and economic

Corresponding author: Bahman Zohuri, PhD, adjunct professor, research fields: artificial intelligence and machine learning.

prosperity. The primacy of electrical energy generation, transmission, and management is impossible to separate from modern societal growth. Regardless of how electrical energy is created from hydro, fossil fuels, the photo-voltaic, wind, or nuclear fissile processes, the fact that it exists without any consideration for its origins or existence places networked electrical systems at the highest risks for cyberthreat-based interruptions. Cybersecurity strategies and industry best practices protect more than the continued inevitable use of electrical energy; the emotional and physical stability of society is at risk without effective cybersecurity methodologies.

The energy sector is of particular concern where an attack on an operating system could cause infrastructure to shut down which triggers economic or financial disruptions or even loss of life and massive environmental damage. The potential for physical damage makes this industry a prime target for cyber-criminals, state-sanctioned cyber-attacks, terrorists, hacktivists, and others looking to make a statement.

The growing reliance on non-governmental forms of market-based valuation of specie known as cryptocurrency creates reliance on cybersecurity measures based on "2FA" (Two-Factor Authentication), and non-machine, non-virtual reliability procedures that are "brilliant in the basics" of "advising and consent" to transfer "real currency" for "cryptocurrency". The transactions enable the decentralization of traditional currency as well as its banking system; it is trading through the SWIFT (Society of Worldwide Interbank Financial Telecommunication) banking system creating the need to defend against blockchain and mining by means of digital transaction of cryptocurrency. The use of cryptocurrency makes transaction audits impossible if the attackers chose this type of currency for blackmailing the United States Treasury as means of pay-off as took place in 2021. The hackers demanded payment in cryptocurrency as the condition to remove their smart malware out of the affected pipeline distribution lines when they disrupted that sector of energy management. The ensuing disruption resulted in a hike in oil prices that remained elevated until these hackers were paid-off via cryptocurrency; the payoff transactions were not traceable and the FBI (Federal Bureau of Investigation) was never able to discover the cyber-attack perpetrators, nor were they able to track them for prosecutorial purposes [1].

The dominant trend within the energy distribution and management systems since the 1990s has been mergers into fewer management entities and an increasing reliance on the technologies supporting the IoT. The Oil and Gas Companies, as well as Electrical Utilities, are seeing the results from "Economies of Scale and Scope" that the adoption of IoT practices deliver. A corollary benefit has been the improvement of operational safety across multiple energy-management domains via SG (smart grid) interconnectivity that crosses national and international borders, especially throughout Europe. This indicates that utilization of IoT results in improved outcomes in energy management with DT (digital transformation) that allow natural communication processes distribution operators and energy producers regardless of legacy non-renewable or emerging renewable energy-producing infrastructures.

With help from the IoT, one can orchestrate a DT strategy that helps energy, oil, and gas companies leverage all the new data that IoT provides to lower the cost of production and operational expenses, streamline maintenance, and keep workers safe [2].

Smart, connected solutions are a smart move for energy companies by integrating IoT technology in place within their day-to-day operations.

IoT in energy, oil, and gas is helping companies lower the cost of utilities, improving both the end customer experience and their bottom line.

DT and IoT, as part of the next industrial revolution, combined with a comprehensive mobility strategy, are making industrial workspaces safer, more efficient, and more productive by streaming workflows within

domain real-time communications and BD (big data) among refineries, oil, and gas field production.

The overall perspective allows management and utilization of the growing amounts of data at the level of BD thresholds; one can see how oil and gas companies create a demand for DT strategies. Digital fusion terminals collect massive amounts of data that arrive from Omni-directional sources as structured or unstructured resulting in opening additional access doors or through tools that are identified as AI (artificial intelligence). Augmentation of AI with its integrated sub-systems known as ML (machine learning) and DL (deep learning) will transform legacy Business Intelligence approaches into AI [3].

When it comes to IoT and BD, cybersecurity stays in front and center of the daily operational data management volume in order to sustain and maintain operational resiliency in the event of actual attacks by Smart Malware that is further aided by actors' intent on disrupting planned daily operational processes [4].

Energy producing and utility companies are finding that investment in IoT, Data automation, and data-gathering technologies can be a double-edged sword. On one hand, digitalization opens the door to deeper business insights and more informed decision-making that enhances business performance and lowers costs. On the other hand, it generates significant risks from access points to central or distributed data processing centers.

Critical infrastructure is naturally associated with high-value targeting for cyber-attackers, and a new generation of decentralized, internet-connected sensors and other devices add complexity and increase access points to the system that magnifies cyber risk.

Data encryption, authentication technology, next-gen firewalls, and physical security continue to be powerful and reliable security tools. In the discussion of cybersecurity measures protecting the energy-producing and electricity distribution systems the following practices are being adopted that are AI Centric:

- Behavioral Analytics to monitor networks for suspicious activities that deviate from a baseline of "normal actions".
- DL, ML, and AI rely on advanced algorithms to assimilate normal user and device network activity and detect anomalies.
- Threat intelligence uses information collected about existing or emerging network threats to inform decision-making by security experts.

As the IEA (International Energy Agency) points have identified in a recent "Digitalization & Energy Report" the astounding pace of ongoing technological advances, combined with falling technology costs and ubiquitous connectivity, has created unprecedented opportunities to transform traditional models of producing and consuming energy through the use of design simplification and streamlining legacy practices.

A total of 66% of oil & gas respondents say their companies have realized benefits from digitalization, with a corresponding increase of risks from cyber threats.

A total of 72% of utility professionals report that physical and cybersecurity is either "important" or "very important" over the previous emphasis to address cyberthreats.

The integration of AI is now considered in the overall systemic incorporation for IoT capability as a way of moderating risks associated with DT.

AI-powered transformation contributes measurably to increased operational efficiencies with corresponding savings in the energy-producing, electrical generation, and associated utility distribution markets according to several recent reports. The following possibilities are identified:

- Revolutionize the demand and supply-side economics. AI applications continue to be central to the processing centers that serve future SGs by continuously collecting and synthesizing data to boost awareness, efficiency, and maintenance of grid systems that support timely decisions about

allocation—and optimization—of energy resources and improve the customer experience. Advanced neural network design, natural language processing, and machine intelligence technologies can all be overlaid on existing physical and virtual assets to monitor supply and demand changes in real-time, actively manage the grid, prevent real-time disruptions, and efficiently balance the utilization of fossil fuel and renewable energy sources.

- Optimize energy exploration investment. DL and ML as sub-systems of AI can improve planning and forecasting while reducing resource extraction risks. AI can assess a host of key variables ranging from well integrity, extraction equipment condition, geological stability metrics, and thermal gradients in order to directly aid in operational decision-making and operational safety [5, 6].
- Maximize reservoir production. AI systems provide the foundation for digital oil field extraction concepts and "Best Practices" implementation; AI is essential for modeling extraction operations, field surveillance, and reservoir characterization to optimize production costs and increase recovery.

Despite industry trends to integrate AI capabilities, there remains to inherit organizational and cultural resistance. Obstacles include aversion to using new operational concepts that remove legacy operations personnel from traditional job tasks, reliance on legacy technologies unable to incorporate AI, and concerns about whether new technologies will deliver as promised without effective modeling demonstrations and experimentation.

2. AI-Driven IoT

With current demand and a need for a proper IoT innovative technology augmenting with a proper AI in place, electricity production owners and organizations can deliver the cutting-edge IoT/AI solutions to their consumers and customers for energy in the way that works best for their business, which includes:

- Advanced predictive modeling. Make better predictions of energy demand with more accurate forecasting models based on more data from more sources, including smart meters and weather stations. Automatically track model accuracy, and easily update models to reflect changes.
- Smart meter analytics. Optimize smart meter deployment and manage timely customer communications to get the most value from your investments in smart meters and advanced metering infrastructure.
- Comprehensive asset data. Integrate structured and unstructured data from all sources to get an enterprise view of asset performance and drive improved grid reliability.
- Advanced early-warning analytics. Identify potential issues early, even before they occur, so you can proactively take corrective action to improve outcomes.
- Automated monitoring and predictive alerts. Reduce downtimes, avoid major defects, address potential performance issues before they escalate, and use built-in workflows and case management capabilities for faster problem resolution.

With all the above privileges utilizing IoT and AI as combined innovative technology of D2M (Device-to-Machine) and M2M (Machine-to-Machine), they harness the sensor data to boost uptime, performance, and productivity while lowering maintenance costs and reducing your risk of revenue loss.

3. Resiliency Driven IoT

As part of the infrastructure of today's organization and enterprise, an operation is linked to the rest of the world and takes place based on their involvement in the world of IoT, which comes of it the risk and risk management once these entities are on Internet and networks around both Internally and Externally. With this basic rule in mind comes with it is the resiliency and integrity of entities' hardware and software within their environment and that comes under the umbrella

of ITE (information technology environment).

ITE is the policies and procedures that the entity implements and the IT (Information Technology) infrastructure (hardware, operating systems, etc.) and application software that it uses to support business operations and achieve business strategies and they need to be totally secure and resilient as well and as we stated ITE is an emergent and evolving concern for every organization and consuming entity involve with IoT.

ITE arises when an entity as part of its IoT network is involved with DT and comes with it the necessary risk and thus has a BRS (business resilient system) in place [7].

For any entity operating in today's technological world of computer software and hardware, one needs a modernized IT to encounter and resolve all the related security and safety issues involved with this hardware and software that are in the loop of IoT networks.

DT is changing industries and is providing organizations with unprecedented benefits. This shift is impacting the boundary cross-government at local and federal and public sectors and ignoring DT is not an option. So how can government and public sector agencies make the shift?

Fueled by new technologies and paradigms, DT is changing industries and is enabling organizations to reap unprecedented benefits, including improved efficiencies, happy customers, and the ability to expand their reach. But unfortunately, organizations that do not embrace DT are being left behind. They lose their competitive advantage and often cease to exist.

Naturally, for us to be able to handle our DT, we need to be on IoT, and with that comes IT and its environment components as we stated are a combination of hardware and software and all its related components, holistically are listed here as follows:

- Computing Platforms.
- Applications/Apps.
- Connectivity (Networking).
  - Wireless (WiFi, 3G/4G data as well as 5G data services in recent years, and Bluetooth).
  - Personal (i.e., Bluetooth)
  - Local (i.e., Ethernet)
  - Distance (Wide-Area Network, i.e., DSLA)

The above is among the components that are dealing with the IoT and they all need to be not only secure but to be resilient as well.

Associated with these components as part of the network and their resiliency should be the ability to some ways to measure the sizes that are required by ITE dimensions and are listed as below:

- ✓ Geography
- ✓ A number of computing platforms
- ✓ Variety of technology
- ✓ Footprint
- ✓ The heat produced and power consumed
- ✓ Rules that influence use and operations

All the above summarizes the basic infrastructure that needs to be in place as part of ITE requirements going forward with IoT and associated resiliency along with it in order to enhance the security of such environments.

In nutshell, the modernization of IT among private enterprises sectors and government organization falls into Four Pillars that can be presented as [8]:

(1) How a lack of visibility impacts the public sector's ability to adopt cloud, DevOps, and DCOI (Data Center Optimization Initiative) initiatives and part of their interoperability. This DCOI has a cost-saving measure, as well as a call for agencies to think more strategically about they use resources to achieve goals like cloud migration and sharing both information and services as well as knowledge transfers.

(2) Migrate any workload to the cloud and maximize the use of cloud computing, where BD can be stored and restored that are coming from Omni-Direction in terms of structure and unstructured format.

(3) Datacenter repository consolidation imitative as part of DCOI aims to push agencies among the government to both consolidate data centers and optimize their operation through better server utilization and automated monitoring of key metrics as part of their KPI (key performance indicator), while AI along with its components such as ML and DL could be augmented as part of IT modernization steps toward futuristic technology [9].

(4) Shared services enable the government agencies to overcome not only constraints in budgets among each other but resources and skills gaps between government and public organizations as well. Modernization inherently involves innovation, and a lack of training or expertise cannot always be the barrier to adoption. With shared services, agencies or departments pay only for what they use and do not have to invest, manage and maintain individual systems and applications. This frees valuable funds for other initiatives, and it also reduces the time spent on IT maintenance and management [8]. A common service delivery model also ensures consistency across recipients of shared services, promoting a healthy and uniform cybersecurity posture.

Again, at the end the ITE, are the policies and procedures, where the entities can implement along with IT infrastructure such as hardware and software, where they can support business operations and resiliency could be achieved as part of business strategies as a paradigm in particular in the energy sector, where government and industry need to team up as a very close partner as PE (proven expertise).

4. Data-Drive Analytics (D-DA)

As massive shear of data is growing to the level of BD volume and size is continuously rising, we need to access them freely among organizations and enterprises both public and government that benefit from them by increasing their information and knowledge and consequently the power of acting and reacting decision making.

Data get pulled from everywhere and direction as well as integrating everything, connect everyone through the IoT, both structured and instructed format as we have stated before. Faster analysis of these data as real-time as possible is a driving factor behind any resiliency requirement behind our action, reaction, and counter-action as fast as possible, since these data travel within Omni-direction at the speed of electrons through IoT.

When it comes to dealing with the energy sector a valuable DA (data analytics) and DP (data predictive) methodology in a cost-effective manner is in demand and becomes very vital, when this source of necessity comes under attack by Smart Malware and Cybersecurity attacks, where we need a quick and if not real-time but near real-time in the real world.

When a company employs a "data-driven" approach, it means it makes strategic decisions based on data analysis and interpretation. A data-driven approach enables companies to examine and organize their data with the goal of better serving their customers and consumers [5, 6].

5. IoT Vulnerability and Security Driven by R-DT (Real-Time Defense)

IoT risks are expanding as more and more, as well as varied devices are connected to each other via web and Internet. As part of DoD (Department of Defense) policy recommendations for the IoT is expressing how we can improve our readiness and build in BRS (business resilience system) in place, knowing the real-time status of material within weapon system and in particular nuclear weapons type and when it comes to energy sector beside flow of energy within network grid, but we need to be worried about NPP (nuclear power plant) in line as a means nonrenewable (or renewable depending on one's point of view) source of energy. This allows utility owners of these power plants to be more responsive to emergent threats [10, 11].

An enhanced R-TD technology puts us ahead of any cyber attack via IoT ahead of any incoming threat

to our energy system vulnerability by eliminating the blind spots within the system and detecting them faster and faster by preventing any breach of security [12].

This way we can turn the IoT security from a defense position to an offence one and AI can provide and offer us such a line defense and offense boundary [13].

Bear in mind that, the IoT economic impact is estimated at $6.2 trillion annually by 2025 and thus coming with it is its security which is an inevitable scenario.

In nutshell, we understand IoT security requires a different mindset, one where security is tied to your data, protecting data through keyless signatures wherever the data move, change or are accessed, creating digital footprints to monitor and report any malicious or suspicious activities, irrespective of where the data resides, in the cloud, your car, at home, or on your smartphone.

The social, economic, and political impacts of IoT are just starting to be understood and debated. The effects on quality of life, health, environment, productivity, agriculture will unleash the next wave of innovation as we transition from the consumer internet to the industrial internet, and based on General Electric report, the industrial Internet will have a $270 billion impact on the business of this company. This is what we know today as the IoT and based on the report from General Electric.

6. Conclusion

According to Steve Martin, Chief Digital Officer, GE Energy Connections, the incorporation of AI-assisted decision-making offers up a 200 billion dollar annual cost avoidance for participating industries.

The direct contribution of AI-assisted operations is 50 billion dollars in additional profits within oil and gas supply chains.

The adoption of the IoT as an inevitable consequence of DT within energy-producing industries as either renewable or nonrenewable electrical generation entities, a corresponding threat from potential cyberattacks is created unless cybersecurity practices are equally considered in the overall system practices. Fewer tool choices and stringent cybersecurity human factors create lower probabilities of cybersecurity system failure.

To mitigate network attacks via the IoT now in the future innovative technology is required to protect IoT infrastructures by providing a 360 ° view of the data that are coming in Omni-direction at any time either real-time or at least near-real-time, anywhere and on any device, static or dynamically as part of DRBTs (dynamic response behavior types) including incident responses.

The DOE (Department of Energy) urges the adoption of IoT as operational norms in order to homogenize and harmonize diverse energy extraction, electrical generation, and utility distribution networks to facilitate Smart-Grid Technologies as Nationwide, and international networks continue to aggregate and evolve.

References

[1] Zohuri, B., Nguyen, H. T., and Moghaddam, M. 2022. "What is Cryptocurrency? Is It a Threat to Our National Security, Domestically and Globally?" *International Journal of Theoretical & Computation Physics* 3 (1): 1-14.

[2] Zohuri, B., Kumar, A. A. D., and Masoud, M. "Cost-Effective Detecting, Preventing and Mitigating Cyber Threats to Nuclear Energy Systems." (in publish)

[3] Zohuri, B., and Moghaddam, M. 2020. "From Business Intelligence to Artificial Intelligence." *Modern Approaches on Material Science* 2 (3): 231-9.

[4] Zohuri, B., and Rahmani, M. 2019. "Artificial Intelligence Drive Resiliency with Machine Learning and Deep Learning Components." *International Journal of Nanotechnology & Nanomedicine* 4 (2): 1-18.

[5] Zohuri, B., and Rahmani, M. 2020. "Machine Learning Driving Forecasting Paradigm." *ACTA Scientific Computer Science* 2 (4).

[6] Zohuri, B., Mossavar-Rahmani, F., and Behgounia, F. 2022. *Knowledge Is Power in Four Dimensions: Models to Forecast Future Paradigm: With Artificial Intelligence Integration in Energy and Other Use Cases* (1st ed.). London, United Kingdom: Academic Press Publishing

Company.

[7] Zohuri, B., and Moghaddam, M. 2017. *Business Resilience System (BRS): Driven through Boolean, Fuzzy Logics and Cloud Computation: Real and Near Real Time Analysis and Decision Making System* (1st Ed.). New York: Springer Publishing Company.

[8] Splunk. 2022. "The Four Pillars of Government IT Modernization." https://www.splunk.com/en_us/form/four-pillars-of-government-it-modernization.html?utm_campaign=bing_amer_usa_en_search_generic_pubsec&utm_source=bing&utm_medium=cpc&utm_term=government%20it%20modernization&utm_content=Four_Pillars_Of_Govt_WP_EN&_bt=71605787835887&msclkid=93239e25107919052807fc0e95723d45.

[9] Zohuri, B., and Zadeh, S. 2020. *Artificial Intelligence Driven by Machine Learning and Deep Learning* (1st ed.). New York, NY: NOVA Science Publishers, Inc.

[10] Zohuri, B., and Mossavar-Rahmani, F. 2019. "Our Daily Lifer Dependency Driven by Renewable and Nonrenewable Source of Energy.*" Journal of Energy and Power Engineering* 13: 67-73.

[11] Zohuri, B., Rahmani, M., and Moghaddam, M. 2022. "Renewable and Nonrenewable Energy Flow Resiliency for Day-to-Day Production and Consumption." *Journal of Energy and Power Engineering* 16: 13-8.

[12] Zohuri, B., and Mossavar-Rahmani, F. 2020. "Energy Source Driven Electricity Production: A Global Tactical and Strategical Paradigm." *Journal of Energy and Power Engineering* 14: 26-32.

[13] Zohuri, B., Moghaddam, M., and Rahmani, M. 2022. "Business Resilience System Integrated Artificial Intelligence." *International Journal of Theoretical & Computational Physics* 3 (1): 1-7.