ZERO TRUST ARCHITECTURES IN THE ENERGY SECTOR: APPLICATIONS AND BENEFITS

Prof. Mag. Lars Ritter, MBA
European Polytechnical University
Bulgaria
lars.ritter@epubg.eu

Prof. Dr. Raphael Röttinger
European Polytechnical University
Bulgaria
raphael.roettinger@epubg.eu

Prof. Dr. Sebastian Wenning
European Polytechnical University
Bulgaria
sebastian.wenning@epubg.eu

ABSTRACT

The Zero Trust Architecture (ZTA) refers to a cybersecurity model that offers fundamental shifts in the traditional security paradigm by eliminating the idea of trust based on network location. ZTA provides a new way of thinking that mandates continuous verification and strict authentication of every user and device. The mandate focuses on the user or device irrespective of location, whether within or outside the specific network parameters. The energy sector relies heavily on ZTA because of the emergence of smart grids and decentralized systems. Thus, using ZTA is imperative because of the interconnectivity and critical infrastructures that influence operations. These features of smart grids also indicate their vulnerability because of potential cyber threats. Using smart grids allows for the real-time monitoring and management of the production and consumption of energy. Through smart grids, robust security measures are implemented to safeguard against cyber threats and sustain normal operations. Energy companies must rely on ZTA to enhance their security measures and facilitate the real-time detection of anomalies and potential risks. One of the features of ZTA is micro-segmentation, which deters the uncontrollable spread of risk from one segment to another. Furthermore, ZTA relies on its least privilege feature to minimize unnecessary access to information and facilitate the execution of functions, mitigating the risk of unauthorized access. The benefits of implementing ZTA include regulatory compliance, fostering a proactive security culture, and enhancing the resilience of critical infrastructures.

Keywords: Zero Trust Architecture (ZTA), cybersecurity, energy sector, smart grids, decentralized energy systems.

INTRODUCTION

Accessing and controlling confidential information and data has become a ubiquitous responsibility for most energy companies (Hussain, Pal, Jadidi, Foo, & Kanhere, 2024, p. 30). These companies rely on ZTA to achieve a transformative approach to addressing cybersecurity. Unlike traditional security models like the virtual private network (VPN), ZTA maintains that harm can occur within and outside network system parameters. Thus, ZTA advances the need for continuous verification and strict authentication of network systems to minimize damage. Some companies are merging ZTA with layered defense and global standards to create a resilient digital future in the energy sector (Muhammad, Munir, Munir, & Zafar, 2017, pp. 103-104). Through ZTA, energy companies must understand the importance of verification rather than outrightly trusting their network systems. Threats can occur for users, devices, or applications regardless of network location. Implementing smart grids in the energy sector has led to a need to implement ZTA. The implementation of ZTA underscores the essence of cybersecurity hygiene in the era of the Internet of Things (IoT) (Mughal, 2019, p. 2).

The energy sector uses the smart grid system to interconnect various systems. The interconnection of these systems creates a decentralized energy production approach that uses several power generation control systems (Panda & Das, 2021, p. 14). Energy companies rely on these networks to safeguard national security to attain economic stability. They are prime targets for cyberattacks, and energy companies focus on ZTA to bolster their defenses against potential threats and attacks. ZTA guarantees that these networks are rigorously scrutinized to identify potential cyberattack opportunities. The primary application of ZTA is within smart grids to facilitate advanced metering infrastructure (AMI), leading to real-time data on energy production and consumption (Ajiboye, Agyekum, & Frimpong, 2024, p. 1). However, energy companies must understand ZTA's numerous vulnerabilities. Implementing ZTA will force energy companies to authenticate and authorize their smart grid systems continuously. Continuous authentication and authorization checks can be expensive as these companies focus on mitigating risks of unauthorized access and potential sabotage. Here is the functional model of ZTA below.

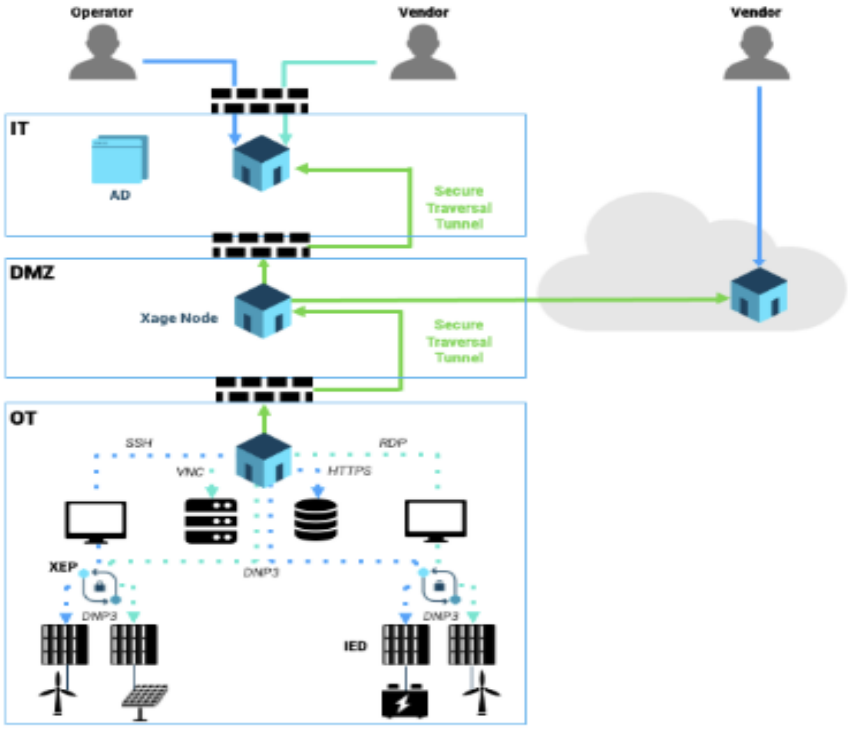

Figure 1 Zero-trust architecture protects operations and mitigates cyber attacks (Arutyunov, n.d, p. 5)

LITERATURE REVIEW

Following consistent cyber attacks, companies have resorted to ZTA security. In this model, application of all corporate resources is based on the user identity and state in which the device is regardless of the network location by the users.

Applications and Benefits of ZTA

The applications of ZTA underscores the importance of this new technology in advancing security in various industries. The technology enhances cybersecurity, indicating that users and devices should be automatically trusted regardless of network location. Technological advancements in today's environment necessitate the implementation of ZTA. These advancements have led to increasingly complex and dynamic IT environments where relying on traditional security models is inefficient (Iqbal, Abbas, Daneshmand, Rauf, & Bangash,

2020). The first area of applying ZTA is enterprise networks. In these large corporations, implementing ZTA restricts how unauthorized personal access to sensitive data. The technology is essential in instances where these enterprises promote remote work. In this case, the network perimeter of traditional security models is blurred, and the IT team cannot monitor and evaluate the actions and decisions of workers. Furthermore, the technology helps safeguard cloud environments where organizations rely on cloud services to store sensitive information (Dashti, Sajid, Jahangeer, & Zafar, 2020). A robust security framework ensures access to cloud resources to strictly control, continuously monitor, and mitigate risks that can cause adverse repercussions.

Moreover, healthcare systems also rely on ZTA to safeguard patient data within healthcare institutions. Implementing strict access controls and continuous patient data monitoring to advance healthcare providers' efficiency. Protecting sensitive data minimizes cyber threats while adhering to regulatory requirements set by HIPAA. Similarly, financial institutions rely on ZTA to improve their fraud prevention and cyberattack efficiencies. Financial institutions use this technology to rigorously verify user identities and devices to access financial systems that promote the integrity of security transactions and customer data. The energy sector also relies on this technology to protect private information involving the production and distribution of energy. Companies are using ZTA to replace their traditional security models to facilitate the protection of smart grids and prevent the disruption of normal operations. Since technology impacts various industries, it has numerous benefits. These benefits include enhanced security, minimized attack surface, improved compliance, scalability, and better user experience. For example, ZTA influences scalability because of its flexibility, making it suitable for numerous industries (Syed, et al., 2022).

Application in the Energy Sector

ZTA in the energy sector is primarily associated with smart grids and decentralized energy systems (Alagappan, Venkatachary, & Andrews, 2022). Due to the complexities of these systems, there is an increasing demand for a robust cybersecurity approach that enhances the protection of confidential information. The energy sector is highly interconnected because of its various infrastructures. The cybersecurity model operates on the principle of "never trust, always verify," and it offers security for enterprise assets such as devices, data, users, and other components (Syed, et al., 2022, p. 57143). The new model provides better security features than traditional models. Traditional security models have a predetermined trust concept that forces organizations to trust their IT systems unquestioningly without taking initial precautionary measures. Every access to the network location request is extensively authenticated, authorized, and encrypted, irrespective of origins (Fernandez & Brazhuk, 2024, p. 4). Therefore, this model offers the least privileged access and continuous monitoring approach to ensure the network does not involve additional resources.

Applying ZTA in smart grids integrates AMI, distributed energy resources (DERs), and other essential automation technologies. These components exemplify these grids' essence and must be safeguarded to increase efficiency, sustainability, and reliability. Nonetheless, these grids have various interconnected components that expose them to numerous entry points for threats (Krause, Ernst, Klaer, Hacker, & Henze, 2021, p. 5). The interlinked components include sensors, control systems, and communication networks, and they present a plethora of challenges because of diverse entry points for potential cybersecurity threats. Implementing ZTA allows interconnected components, devices, and users to gain access after authentication, impeding potential threat entry points. ZTA blocks its blanked spread to other network sections if a single entry point is compromised. Therefore, the company will offer continuous

monitoring and real-time analysis of the grids to detect anomalies and expunge unauthorized access attempts.

ZTA is essential in securing decentralized energy systems to facilitate the transition to sustainable energy. Decentralized energy systems also encompass renewable energy sources that influence the push for transition to sustainability. Decentralized energy systems have diverse and distributed systems, increasing their vulnerability to cyberattacks. Through ZTA, energy companies can implement strict access controls that protect data integrity. For example, ZTA offers the option of encrypting devices to achieve confidentiality and privacy. This outcome will facilitate and sustain resilience and reliability in energy supplies.

Smart Grids and ZTA

An example of smart grids that rely heavily on ZTA is 5G (Alipour, Ghasemshirazi, & Shirvani, 2022, p. 2). These grids are crucial in facilitating the gathering and analysis of information from power lines, distribution power stations and end users. For efficiency, these grids must possess fast and dependable connections to support real-time monitoring of service delivery. Thus, energy companies rely on 5G smart grids to catalyze upgrading existing energy provision endeavors. Reliable smart grids guarantee a high quality of living, ensuring there is fulfilling potential in transportation, market support, and appropriate use of available resources. Despite the efficiency of these systems, there are potential risks associated with cyberattacks. In 2015, Ukraine's smart grid system was attacked by an unauthorized party, consequently leading to an outage in the SCADA distribution system (Alipour, Ghasemshirazi, & Shirvani, 2022, p. 2). These grids might also experience replay attacks, MITM attacks, Dos attacks, and false data injection attacks. In most cases, energy companies are experiencing impracticality when seeking to implement ZTA into their smart grid systems. This challenge arises from curated communication rates and other unforeseen bottlenecks. Currently, the advent of 5G helps enhance the implementation of ZTA into smart grids to enhance how they address potential risks associated with the production and distribution of power to end users.

As indicated in the application of ZTA in the energy sector section, energy companies rely on features like AMI, GERs, and other automation devices to safeguard the sanctity of smart grids. Additionally, these companies rely on the efficiency of ZTA to impede attacks within or outside the network and protect operations. The least privilege also provides solid operational efficiency. Nonetheless, ZTA offers other essential impactful options that improve the uniqueness and effectiveness of smart grids. These include dynamic policy, trust evaluation, and integrity monitoring (Alipour, Ghasemshirazi, & Shirvani, 2022, p. 5). A dynamic policy determines the decisions that must be executed to determine whether to give or deny access to specific network assets of the smart grid. Trust evaluation and integrity monitoring support thorough analysis of requests to access smart grids from diverse sources. The introduction of 5G technology in the smart grid system has enhanced their operations, halting unnecessary power disruptions or loss of confidential information. This technology has refined the power consumption of buildings, enhanced dependability by supporting a connection with mobile devices, reduced communication overhead by streamlining the type of information being shared, and enabled the processing of diverse and massive amounts of data. ZTA offers the protection needed to ensure these grids operate as initially intended.

Decentralized Energy Systems and ZTA

In decentralized energy systems, there is inefficiency because of complex trust relationships between various components (Ossietzky, 2022, p. 4). Complexity arises due to the nature of these relationships constantly changing without warning. What are decentralized systems? Decentralized systems refer to one or more units that enhance how energy is generated at a

location where it is consumed nearby (ibid.). Notably, these systems rely on distributed energy systems (DES) to enhance how consumers access energy. The multiple units of the decentralized energy system are connected through various components and resources. Furthermore, end users must be associated with these energy systems to advance consistency and reliability. In today's society, energy demands are very high, and companies must ensure essential and adequate provision of energy to address the unique needs of end users. Therefore, the integrity of these decentralized systems is crucial to avoid the disruption of power supply. ZTA plays a crucial role in sustaining the integrity of these systems. However, attaining full accountability and efficiency is still challenging because of the complex relationships of diverse components within these systems. ZTA provides several tenets that address the uniqueness of this cybersecurity approach. Thus, energy companies should rely on these tenets to emphasize the essence of verification by allowing access to their decentralized systems. Since these systems are not foul-proof due to complex relationships between components, insisting on verification and authentication will minimize access to private or confidential information. Moreover, relying on ZTA will facilitate continuous improvement to strengthen the safety of these systems and prevent potential cybersecurity attacks. Ultimately, disruptions to power provisions will be significantly avoided.

Despite the successes of ZTA in the energy sector, it is essential to acknowledge various challenges. These challenges impair the technology's success and promise to disrupt daily operations. These challenges include legal considerations, high costs, and a lack of specialized expertise. These challenges prevent the successful implementation of ZTA, impeding the sustainability of cyberattack mitigations. Potential solutions for addressing these challenges include implementing sophisticated infrastructure, training programs to enhance specialized expertise, and collaborating with industry players to offer new implementation perspectives. Overall, energy companies must plan their ZTA implementation processes to align them with their infrastructures to avoid other unnecessary outcomes (Kujo, 2023, p. 42). Initial costs can be expensive, and these companies must minimize unnecessary expenses.

METHODOLOGY

The methodology approach used in this paper is a systematic review of scholarly sources and case studies discussing the implementation of ZTA, its benefits, and its application in the energy sectors. The literature materials accessed were submitted, accepted, and published between 2017 and 2024. Working with these articles led to the development of current information regarding using ZTA in the energy sector. The articles were selected based on the keywords and offered vital information on using ZTA to prevent cyberattacks in smart grids and decentralized power systems. The keywords acted as an inclusion criterion in the study. Once selected, the articles were screened for relevance to identify their importance in this study. The accepted articles were relevant because they offered essential information on the need and benefits of implementing ZTA in the energy sector. Finally, data extraction was conducted to develop common themes and patterns from the selected sources. The common themes were primarily associated with the implementation and benefits of ZTA, especially in the energy sector. Ultimately, these themes were synthesized to develop findings regarding the topic under investigation.

Implementing ZTA within the energy sectors goes through different phases. They include, identifying crucial assets, progressive monitoring and authentication of the requests and applying micro-segmentation to separate network segments. In addition, secure communication protocols and endpoint security measures are determined to ensure integrity of all devices and data transmission.

Several sources highlighted the need to identify critical assets within the energy sector. For example, the need for a robust inventory of every asset, like digital assets and physical infrastructure to understand the possible attack vectors and vulnerabilities. They recommended a detailed risk assessment for evaluating the possibility and effect of different cyber-attacks.
Other sources highlight the importance of determining critical assets within the energy sector. according to (Zhang, Seppanen, & Torkki, 2018, n.p.). There is need for a comprehensive inventory of crucial and digital assets in understanding the possible attack vectors and vulnerabilities. The authors recommend a detailed risk assessment to determine the possibility and effect of different cyber threats.

Lastly, Training and awareness programs among employees are important to maintain a safe environment. According to another research, there is need to train and educate employees on cyber-security and possible threats. The article also recommends consistent simulation exercises like penetration testing, to check the efficiency of security measures and determine areas to improve

Case Study 1: Financial Services Firms Implementing ZTA
Top seven financial firms are facing increased cyber-security threats, like phishing attacks and threats (Chaudhry & Hydros, 2023, p. 98). The VPN-based access control protocol failed to offer sufficient mitigation to this risk which prompted the banks to stop their operations. In such a case, customers may not lose their money but the loss will affect the banks and the country's economy. Cyber security then turned out to be the major concern for the whole organization and hence measure to adopt different policies were reached. The firms then opted to use the ZTA model, which incorporates a multi-factor authentication (MFA) and tight access principles. Through verification of one's identity of every user, and device, one is granted access to the data and application as shown in the figure below.

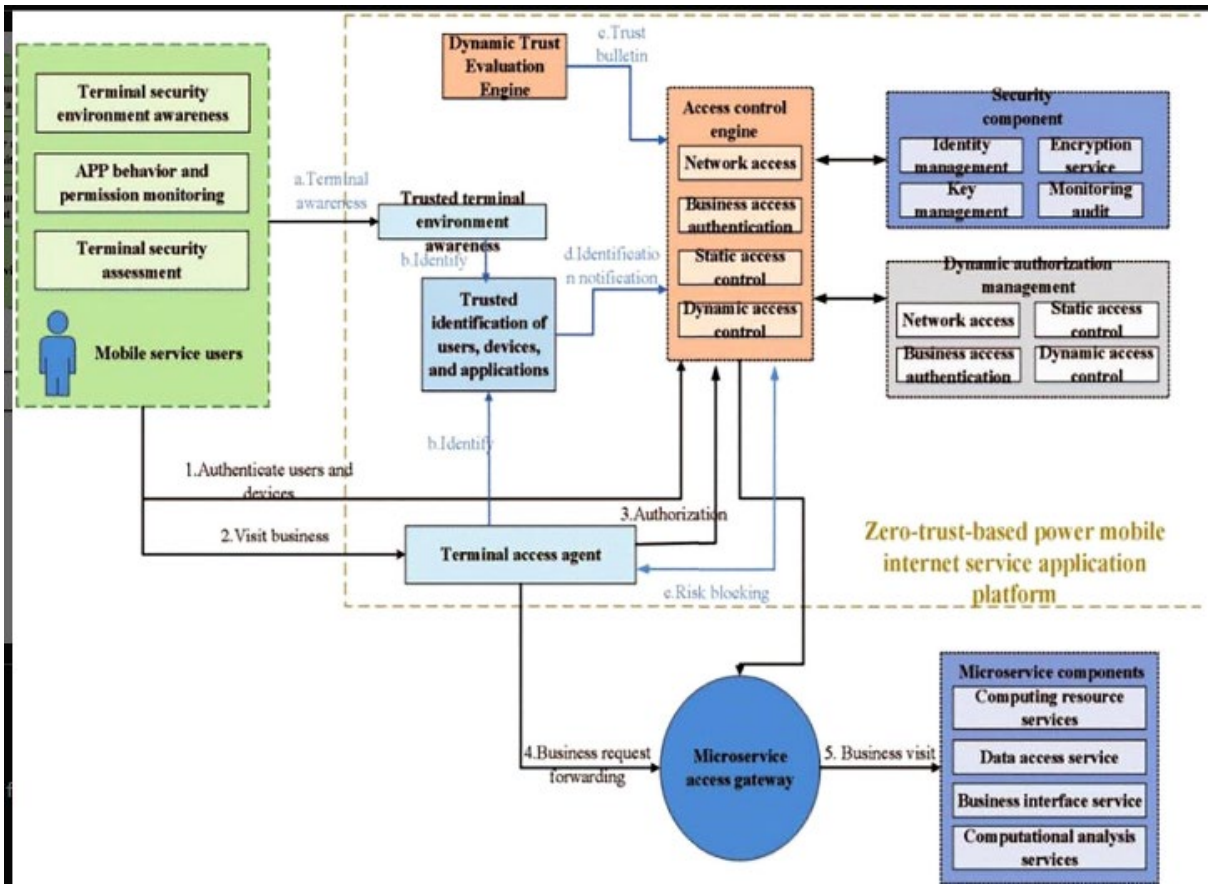

Figure 2 Zero-trust framework for power mobile internet business (Chaudhry & Hydros, 2023, p. 102)

Through this methodology, energy firms can efficiently implement the ZTA to improve their cybersecurity position, ensure resilient operations against cyber threats and protect crucial infrastructure. The systematic review of scholarly sources offers important insights into best practices for implementing ZTA within the energy sector. This enhanced the security of the firm. After implementation, the financial sector experienced a drastic reduction in successful unauthorized access and phishing attacks attempts. The ZTA also promoted a secure remote work for the organization.

Case Study 2: Healthcare firms implementing ZTA

Another case involves health care firms like the case of Scripps that was struggling with securing patients data using the outdated systems and devices, aggravated by the desire to support remote healthcare service (Burky, 2023, n.p.). It experienced a serious ransomware attack which affected the hospitals operations, leading to temporal shutdown of systems and diverting patients. The attack involved data encryption and a demand for ransom affecting the operations of the hospital. The organization implemented the ZTA, focusing on securing different endpoints, data encryption both at rest and in transit and employed identity and access management (IAM) solutions to ensure that only authorized people can have access to the sensitive data of the patient. Adopting the ZTA led to improved data protection of the patients data, which complies with regulations from the health care and also improved trust of the patients to the facility. The firm also attained great visibility into its network traffic, making it possible to detect threats and responses on time.

- Steps taken in these two cases:
- Security audit and incidence analysis
- Network segmentation

- Multi-factor authentication (MFA)
- Continuous monitoring and response
- Data protection and encryption

RESULTS

The implementation of Zero Trust Architecture (ZTA) in the energy sector encompasses smart grids and decentralized systems. Key technological components involved include Advanced Metering Infrastructure (AMI), Distributed Energy Resources (DERs), and automation devices. Energy companies must continuously verify their systems to sustain micro-segmentation and least privilege access. The benefits of implementing ZTA are manifold, including enhanced security, regulatory compliance, prompt detection of anomalies, and increased resilience against cyber threats. However, the sector faces challenges such as high costs, lack of specialized expertise, and legal considerations. Potential solutions involve implementing sophisticated infrastructure, developing training programs to enhance specialized expertise, and collaborating with industry players to gain new perspectives on implementation.

In the healthcare sector, ZTA enhances the protection of patient data and ensures regulatory compliance. The finance sector benefits from ZTA through improved fraud prevention by focusing on rigorous verification processes (Chaudhry & Hydros, 2023, p. 102). For enterprises, ZTA promotes the security of remote work by controlling access to sensitive data. In cloud services, ZTA supports continuous monitoring to facilitate risk mitigation. Each sector leverages ZTA to address specific security concerns and operational challenges, demonstrating its broad applicability and effectiveness across different industries.

These case studies and articles portray the transformation to ZTA and how it is benefiting firms. This shows how different organizations can efficiently improve their cybersecurity stance by adopting the ZTA comprehensive model. While cyber threats keep evolving, the ZTA offers robust and flexible foundations for protection of crucial assets like data, placing emphasis on the need for a continuous verification and least privilege I the current digital space. The path towards ZTA requires careful planning, collaboration, and commitment to progressive evaluations and changes. Nevertheless, as demonstrated in these case studies, shifting towards ZTA for security, compliance and operational efficiency explains how much efficient it is, making it an important tool for any organization to safeguard its digital space.

Putting in place measure like the ZTA may lead to a high security system that will benefit organizations including their effort in protecting data of their clients. External parties with good reputations in developing security systems could gain from using the ZTA, together with financial savings in the audits of security systems. On the internal side of the company, there is high feasibility and time is used efficiently in monitoring security systems. Internally, the firm gets high feasibility and effective time use in monitoring security systems with high visibility, decreasing the complexity of developing security systems. Since the ZTA naturally aligns with security concepts and needs of major secret units, crucial confidential units need to design and deploy suitable solutions faster.

DISCUSSION

The study's findings indicate the importance of ZTA in the energy sector. Implementing ZTA in the energy sector offers numerous benefits companies can leverage to enhance security. ZTA's implementation enhances security and facilitates how companies adhere to regulatory compliance. Continuously verifying and authenticating attempts to access confidential

information secures the integrity of the network systems. Users, devices, and applications linked to the systems that attempt to execute unauthorized access are promptly thwarted. Canceling unauthorized access to these systems prevents the potential risks of cyberattacks. ZTA's micro-segmentation and least privilege features facilitate how this outcome occurs. Moreover, implementing ZTA offers real-time anomaly detection. Energy companies rely on this to mitigate unauthorized access to smart grids and decentralized energy systems. Thus, they sustain operational ability and ensure that the sanctity of national grids is protected. ZTA's AMI, GERs, and other automation devices facilitate how it sustains continuous surveillance and offers rapid response to achieve resilience.

Furthermore, ZTA guarantees scalability and flexibility. The energy sector is dynamic because of the diversity of technological components. These technological components offer complex informational environments that are prone to cyberattacks (Feng & Hu, 2023, pp. 75-90). Relying on traditional security models in this sector can lead to damaging results because they provide predetermined security measures. They do not safeguard against unforeseen attacks from users, devices, and applications and can lead to faster and broader attacks on the whole network system. Thus, ZTA limits the spread of attacks from single users, devices, and applications. Nonetheless, the findings also indicate pitfalls associated with ZTA. These pitfalls must be addressed to ensure that future operations run seamlessly and uninterrupted. These pitfalls include legality issues, high costs of development and sustenance, and a lack of adequate skilled expertise. Thus, to address them, energy companies should leverage support through collaboration, implementing sophisticated infrastructure, and implementing training programs to enhance specialized expertise.

CONCLUSIONS

In conclusion, the energy sector must implement ZTA because of its digitized cyber protection features and qualities. Safeguarding smart grids and decentralized energy systems sustains normal operations by mitigating cyberattack disruptions. ZTA mitigates cyberattacks by ensuring that attacks on specific segments do not interfere with other network components to cause paralysis. Through its benefits, ZTA indicates future success for energy companies globally. However, there are challenges that these companies must capture to limit unintended disruptions in the production and distribution of energy in the future. Future researchers should work on identifying critical additional parameters that can address barriers to the widespread adoption and implementation of ZTA.

The energy industry has undergone revolution over the years which needs digital analytics, collaboration, data driven automation and physical assets. The future for a smart power grid involves electric substations managed by industrial IoT devices which can communicate with the customer, administrators and different energy sources blend to utilize the generation and distribution of energy. Fixing security issues due to merging new and legacy equipment calls for a very sophisticated security solution. Today’s approaches are complex to manage, and limit growth of digital transformations.

Additionally, the data shows that security is not all about defensive tactics. It requires a clear understanding as the basis for moving towards smart infrastructure. To unlock the importance of digital transformations in the energy sector, firms need to adopt the ZTA to security which controls all the relations between machines, people and applications across IT systems anywhere in the world. The persistent basic would protect each asset, and interactions enabling energy industries to control, and protect themselves and customers from cyber-attacks.

The lack of granular ZTA strategy explains why incidences like the Colonial Pipeline ransomware hack easily took place forcing all operations to shut down (Srinivasan & Ni, 2023, pp. 1-3). This also explains why there are several cyber -attacks shut-down from firms globally. The ZTA is meant to protect everything from those with old passwords to encryption options to IoT devices that have digital identities within to make operators feel the importance of digital transformation. They will be able to have easy and remote access, efficient data sharing and convenience in their collaborations across the different partners, customers and suppliers.

REFERENCES

Ajiboye, P. O., Agyekum, K. O.-B., & Frimpong, E. A. (2024). Privacy and security of advanced metering infrastructure (AMI) data and network: A comprehensive review. *Journal of Engineering and Applied Science*, 1-30.

Alagappan, A., Venkatachary, S. K., & Andrews, B. J. (2022). Augmenting Zero Trust network architecture to enhance security in virtual power plants. *Energy Reports*, 1309-1320.

Alipour, M. A., Ghasemshirazi, S., & Shirvani, G. (2022). *Enabling a Zero Trust Architecture in a 5G-enabled smart grid.*

Arutyunov, R. (n.d). *Cybersecurity Fabric: Pervasive and Zero-Trust.* Retrieved from https://www.energy.gov/sites/default/files/2021-06/Roman%20Arutyunov-A1.pdf

Burky, A. (2023). *Scripps ransomware post-mortem reveals significant ripple effects for nearby hospitals*. Retrieved from Fierce healthcare: https://www.fiercehealthcare.com/health-tech/scripps-ransomware-post-mortem-shows-cybersecurity-regional-problem

Chaudhry, U. B., & Hydros, A. K. (2023). *Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm.* IET blockchain.

Dashti, W., Sajid, A., Jahangeer, A., & Zafar, A. (2020). Security challenges over cloud environment from service provider perspective. *Cloud Computing and Data Science*, 12-20.

Feng, X., & Hu, S. (2023). Zero Trust Architecture for cyber-physical power system security based on machine learning. In C. I. Wang, *AI Embedded Assurance for Cyber Systems.* Springer, Cham.

Fernandez, E. B., & Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards and Interfaces*, 103832.

Hussain, M., Pal, S., Jadidi, Z., Foo, E., & Kanhere, S. (2024). Federated Zero Trust Architecture using artificial intelligence. *IEEE Wireless Communications*, 30-35.

Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., & Bangash, Y. A. (2020). An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. *IEEE Internet of Things Journal*, 10250-10276.

Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in power grids: Challenges and opportunities. *Sensors*, 6225.

Kujo, J. (2023). *Implementing Zero Trust Architecture for Identities and Endpoints with Microsoft tools.* Jyväskylä: Jamk University of Applied Sciences.

Mughal, A. A. (2019). Cybersecurity hygiene in the era of Internet of Things (IoT): best practices and challenges. *Applied Research in Artificial Intelligence and Cloud Computing*, 1-31.

Muhammad, T., Munir, M. T., Munir, M. Z., & Zafar, M. W. (2017). Integrative cybersecurity: Merging Zero Trust, layered defense, and global standards for a resilient digital future. . *International Journal of Computer Science and Technology*, 99-135.

Ossietzky, C. V. (2022). *Development Paths for Decentralized Energy Systems in the Context of the Energy Transition – Identification of Interdependencies and Technology Lock-Ins.* Oldenburg: Universitat Oldenburg.

Panda, D. K., & Das, S. (2021). Smart grid architecture model for control, optimization and data analytics of future power networks with more renewable energy. *Journal of Cleaner Production*, 126877.

Srinivasan, S., & Ni, L.-K. (2023). *Ransomware Attack at Colonial Pipeline Company.* Harvard Business School Case 123-069.

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access*, 57143-57179.

Zhang, Z., Seppanen, H., & Torkki, P. (2018). Critical infrastructure vulnerability—A method for identifying the infrastructure service failure interdependencies. *International Journal of Critical Infrastructure*.

TABLE OF FIGURES