Securing Electrical Infrastructure in Data Centers Using Artificial Intelligence

Author - Chirag DevendraKumar Parikh, Certification Specialist, AWS

Abstract—**The speedy expansion of records centers because the backbone of virtual infrastructure has heightened the need for robust and intelligent safety answers, specially concerning their electrical systems. Electrical infrastructure—comprising energy distribution gadgets, circuit breakers, mills, and uninterruptible energy substances (UPS)—is vital for maintaining uninterrupted operations. However, those components are more and more liable to cyber-physical assaults, gadget disasters, and anomalies, probably leading to catastrophic carrier disruptions. This paper proposes a complete framework that leverages Artificial Intelligence (AI) to beautify the security and operational resilience of electrical infrastructure within facts facilities. By incorporating AI-driven predictive renovation and actual-time threat detection, this framework not simplest mitigates security risks but also optimizes electricity utilization and equipment lifespan. The study underscores the significance of intelligent automation in achieving proactive infrastructure defense and contributes to the wider imaginative and prescient of steady and resilient information center operations.**

The proposed version integrates actual-time statistics acquisition from electrical components the use of Internet of Things (IoT) sensors, observed by using preprocessing and clever analysis using gadget mastering and deep mastering algorithms. The AI-based totally device is capable of detecting peculiar patterns, ability gadget disasters, energy inefficiencies, and cyber-intrusion tries by using reading present day, voltage, temperature, and energy consumption developments. An ensemble-based risk detection mechanism combines supervised gaining knowledge of for known threats and unsupervised anomaly detection for zero-day vulnerabilities. By incorporating AI-driven predictive renovation and actual-time chance detection, this framework not most effective mitigates protection risks but also optimizes energy usage and system lifespan. The examine underscores the importance of smart automation in achieving proactive infrastructure defense and contributes to the broader vision of secure and resilient information middle operations.

Keywords— Data centers, electrical infrastructure, artificial intelligence, threat detection, anomaly detection, predictive maintenance, cyber-physical security.

Author Bio - I'm Chirag Parikh, an electrical engineer with over 13 years of experience in product safety, global market access, and regulatory compliance. At Amazon Web Services (AWS), I lead hardware compliance programs in more than 45 countries, making sure data center infrastructure, edge computing, and AI-based hardware meet global safety, EMC, and environmental standards. Earlier in my career, I worked with Intertek and SDP Engineering (a Nemko partner), where I gained hands-on expertise in EMI/EMC testing, lithium battery safety, and regulatory approvals. I hold an M.S. in Computer Engineering from California State University, Fullerton, and a B.E. from Gujarat Technological University, where I graduated as a Gold Medalist.

I. Introduction

In the digital technology, records facilities serve as the critical infrastructure powering cloud offerings, huge statistics analytics, and enterprise computing. To hold operational continuity, these facilities depend closely on complicated electric infrastructure structures, consisting of power distribution gadgets (PDUs), uninterruptible power supplies (UPS), turbines, transformers, and circuit breakers. Any disruption or anomaly in these structures can bring about extreme carrier outages, economic losses, and compromised facts integrity. Traditional tracking processes, which commonly depend upon manual tests and rule-primarily based structures, are often insufficient in addressing actual-time threats and rising cyber-bodily assaults.

As records middle environments grow to be more and more complex and interconnected, there may be a growing want for wise, adaptive, and proactive answers which can ensure the security and reliability of electrical structures. This paper presents an AI-primarily based chance detection framework that utilizes device getting to know and deep studying techniques to screen, examine, and steady the electric infrastructure of information centers. By leveraging actual-time sensor records and historic styles, the proposed device can discover anomalies, expect equipment disasters, and become aware of cyber-intrusions. This method complements response times, reduces downtime, and strengthens usual operational resilience, presenting a scalable and future-geared up answer for cutting-edge records center safety.

II. Cutting Edge Technology

The proposed gadget employs a combination of cutting-edge technology to display, examine, and stable electric infrastructure in facts centers. At the muse, Internet of Things (IoT) sensors are deployed throughout electrical components including PDUs, UPS systems, transformers, and switchgear to continuously gather actual-time data on parameters like voltage, modern, temperature, and energy consumption. This data is transmitted to a centralized AI-powered analytics engine through a steady network. The core of the system makes use of gadget mastering (ML) algorithms which includes Support Vector Machines (SVM), Random Forest, and Gradient Boosting for supervised class of recognized fault signatures.

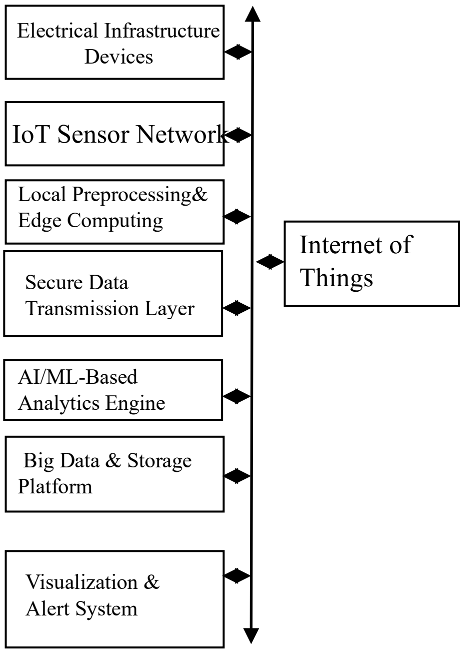
Electrical Infrastructure Devices
IoT Sensor Network
Local Preprocessing& Edge Computing
Secure Data Transmission Layer
AI/ML-Based Analytics Engine
Big Data & Storage Platform
Visualization & Alert System
Internet of Things

Fig. 1. Block diagram

The proposed system employs a aggregate of modern-day technologies to reveal, examine, and secure electric infrastructure in statistics facilities. At the muse, Internet of Things (IoT) sensors are deployed across electrical components along with PDUs, UPS systems, transformers, and switchgear to constantly collect actual-time data on parameters like voltage, current, temperature, and strength consumption. This facts is transmitted to a centralized AI-powered analytics engine via a steady community. The middle of the machine uses machine studying (ML) algorithms which includes Support Vector Machines (SVM), Random Forest, and Gradient Boosting for supervised category of known fault signatures. Additionally, unsupervised mastering strategies, together with K-Means clustering and Isolation Forests, are used for anomaly detection and zero-day hazard identification. For temporal sample popularity and prediction, Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) models are employed. The framework also integrates a cloud-primarily based dashboard that visualizes threats and anomalies in actual-time at the same time as issuing computerized indicators via email or mobile applications. Edge computing competencies are used for nearby statistics pre-processing to reduce latency and ensure rapid hazard detection. The machine is designed with cybersecurity protocols for facts integrity, authentication, and stable transmission. To ensure scalability and resilience, the platform leverages containerized microservices (using Docker and Kubernetes) for deploying ML models and managing workloads successfully throughout distributed computing environments. Big records frameworks which include Apache Kafka and Apache Spark are hired to address high-throughput statistics ingestion and real-time analytics from heaps of IoT endpoints. Additionally, unsupervised gaining knowledge of strategies, such as K-Means clustering and Isolation Forests, are used for anomaly detection and 0-day hazard identity. For temporal sample popularity and prediction, Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) fashions are employed. The framework additionally integrates a cloud-based totally dashboard that visualizes threats and anomalies in actual-time even as issuing automatic signals through e mail or mobile programs. Edge computing abilties are used for local information pre-processing to reduce latency and ensure fast hazard detection. The gadget is designed with cybersecurity protocols for facts integrity, authentication, and steady transmission.

III. Electrical Infrastructure Devices

Electrical infrastructure paperwork the backbone of facts center operations, ensuring continuous and dependable energy transport to servers, storage systems, networking devices, and cooling devices. A traditional data center's electrical surroundings accommodates a couple of interconnected components, which include energy distribution gadgets (PDUs), uninterruptible strength components (UPS), transformers, computerized transfer switches (ATS), backup mills, and circuit breakers. These components work collectively to offer strong voltage degrees, manipulate strength redundancy, and save you downtime during application energy disasters. The UPS structures provide quick-time period strength at some point of outages, permitting time for backup generators to activate, whilst PDUs distribute power correctly across IT masses. Transformers alter voltage as required, and ATS guarantees automatic switching between strength resources. Grounding systems and surge protectors also are crucial for defensive touchy device from electrical spikes or faults. Given the vital role of electrical infrastructure, any failure can cause operational disruptions, statistics loss, or system harm. Therefore, its tracking and protection are paramount. With growing electricity densities and complexity, guide oversight is inadequate. Integrating AI-primarily based tracking and predictive analytics gives real-time insights, enabling proactive preservation, anomaly detection, and improved safety against cyber-bodily threats. This shift ensures excessive availability, power performance, and operational resilience for modern-day statistics centers.

IV. IOT Sensor Network

An IoT Sensor Network plays a pivotal role in modernizing the tracking and control of electrical infrastructure in records facilities. These networks include interconnected sensors embedded within important electric additives including PDUs, UPS systems, circuit breakers, transformers, and turbines. The sensors continuously acquire real-time information on diverse parameters including voltage, contemporary, temperature, humidity, vibration, and electricity consumption. Each sensor node is equipped with a microcontroller, a communication module, and energy-green sensing factors. These nodes transmit data to a centralized facet tool or cloud platform via a secure network. The gathered facts serves as the muse for AI-pushed analytics, permitting real-time monitoring, predictive preservation, fault analysis, and anomaly detection. IoT sensor networks enhance visibility into the operational fitness of electrical structures, reduce the want for guide inspections, and improve responsiveness to rising threats. By allowing non-stop far off monitoring, additionally they assist power optimization and compliance with operational standards. In the context of AI integration, sensor information becomes the input that trains and refines machine getting to know fashions, permitting systems to detect subtle deviations from ordinary behavior and trigger preventive moves. This synergy enhances the reliability, safety, and resilience of records middle infrastructure.

V. Big Data & Storage Platform

The Big Data and Storage Platform is a critical thing that manages the massive extent, pace, and form of data generated through IoT sensor networks and monitoring systems. This platform is liable for gathering, processing, storing, and analyzing real-time and historical records from numerous electric components inclusive of PDUs, UPS systems, transformers, and circuit breakers. To deal with excessive-throughput facts streams from hundreds of sensors, technology like Apache Kafka are applied for real-time facts ingestion. Kafka acts as a allotted messaging device that ensures scalable, fault-tolerant transmission of time-stamped statistics to downstream processing layers. For real-time and batch analytics, Apache Spark is employed to perform complicated computations, stumble on anomalies, and assist machine studying workflows across huge datasets.

For lengthy-time period garage and retrieval of time-series facts, databases such as InfluxDB or TimescaleDB are used. These systems are optimized for correctly storing information indexed by way of time, allowing short querying of trends, historical comparisons, and overall performance metrics. Additionally, NoSQL databases like MongoDB or cloud-based item garage (e.G., Amazon S3, Azure Blob) are regularly incorporated for unstructured information storage including logs, images, and model outputs. This platform additionally helps data preprocessing, normalization, and feature extraction, which are important for feeding extraordinary inputs into AI/ML models. Data governance features consisting of encryption, access manipulate, and compliance logging are constructed in to ensure safety and regulatory adherence. By combining allotted computing, scalable garage, and actual-time analytics, the Big Data and Storage Platform permits the predictive and prescriptive intelligence. By combining disbursed computing, scalable storage, and actual-time analytics, the Big Data and Storage Platform enables the predictive and prescriptive intelligence necessary for proactive security. It ensures that information center operations can reply dynamically to threats, optimize infrastructure utilization, and keep high availability with minimal manual intervention. Furthermore, these structures may be containerized and orchestrated the use of equipment like Docker and Kubernetes, taking into account efficient aid management and deployment flexibility. This structure supports elastic scaling based totally on load, and its modularity makes it easier to integrate with 0.33-birthday party tools and APIs for visualization, alerting, and choice guide systems. To deal with excessive-throughput facts streams from thousands of sensors, technology like Apache Kafka are utilized for actual-time facts ingestion. Kafka acts as a distributed messaging system that guarantees scalable, fault-tolerant transmission of time-stamped records to downstream processing layers. For real-time and batch analytics, Apache Spark is employed to carry out complicated computations, stumble on anomalies, and help machine studying workflows across huge datasets. For lengthy-time period garage and retrieval of time-collection information, databases along with InfluxDB or TimescaleDB are used. These systems are optimized for efficaciously storing facts indexed with the aid of time, permitting short querying of trends, historical comparisons, and performance metrics. Additionally, NoSQL databases like MongoDB or cloud-based totally object storage (e.G., Amazon S3, Azure Blob) are frequently integrated for unstructured facts storage together with logs, photographs, and version outputs.

VI. Enhancing Service Quality Within Big DATA

Enhancing provider pleasant in the Big Data platform is critical to make sure dependable, efficient, and secure operations, especially in venture-essential environments such as information centers. With the exponential increase of information from IoT gadgets, tracking tools, and infrastructure logs, maintaining high provider best calls for strong facts management, wise analytics, and actual-time responsiveness. One of the important thing components of enhancing service excellent is data accuracy and consistency. Implementing automatic facts validation, cleaning, and normalization approaches allows make sure that the statistics entering the analytics pipeline is clean, dependable, and suitable for gadget mastering and selection-making obligations. Real-time processing abilities, the usage of frameworks which includes Apache Kafka and Apache Spark, play a vital position in detecting and responding to anomalies, equipment disasters, or security threats right away. This immediate feedback loop enhances system responsiveness and reduces downtime. Scalability and fault tolerance are also critical. Distributed architectures and containerized microservices (e.G., the usage of Docker and Kubernetes) permit the system to handle fluctuating masses with out degrading overall performance. This guarantees consistent provider shipping even under high site visitors or failure situations. Security and compliance similarly contribute to service first-class. Encrypting data in transit and at rest, imposing access controls, and retaining audit trails assist defend touchy records and meet regulatory necessities.

VII. High-Performance System For Electrical Infrastructure In Data Centers

A high-performance system for electrical infrastructure in data facilities is critical to make sure uninterrupted strength transport, most useful electricity performance, and speedy fault reaction. As facts facilities develop in complexity and demand, the reliability in their electrical subsystems together with PDUs, UPS gadgets, switchgear, transformers, and backup mills turns into a essential element of average machine overall performance. A high-overall performance system integrates advanced sensor networks, real-time tracking, and AI-pushed analytics to proactively come across anomalies, expect disasters, and optimize strength consumption. These structures are able to managing tremendous streams of real-time records the usage of side computing and high-pace records buses, which decrease latency and permit rapid nearby choice-making. Automation and manipulate systems are embedded within the electrical infrastructure to support clever load balancing, voltage law, and redundancy switching, which prevent outages and reduce system stress. Machine gaining knowledge of algorithms continuously analyze ancient and actual-time information to forecast thing degradation and optimize renovation schedules. To make certain fault tolerance and scalability, the system structure includes redundant electricity paths, modular additives, and self-restoration abilities, which permit isolated faults to be corrected with out impacting the wider data center operation.

VIII. Applications Predictive Maintenance and Anomaly and Fault Detection

AI permits predictive upkeep with the aid of analyzing real-time records from sensors connected to electric components inclusive of UPS systems, circuit breakers, and PDUs. Using device studying algorithms, the gadget identifies symptoms of wear, overall performance degradation, or unusual pastime before disasters occur. This prevents unplanned outages, reduces repair fees, and extends the lifespan of gadget. Maintenance can be scheduled based on actual situations instead of fixed durations, growing efficiency and reliability.

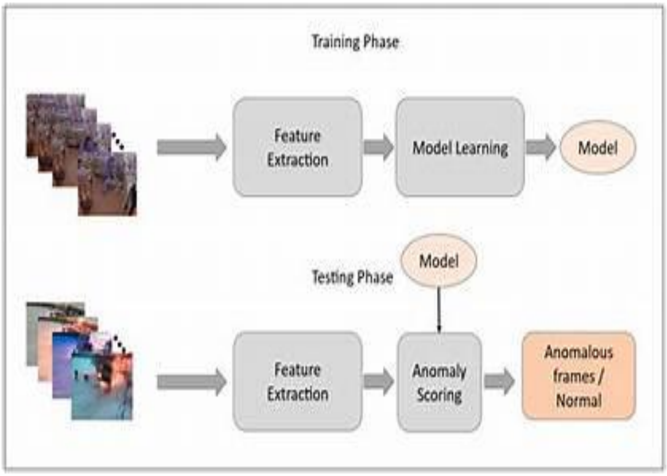

Fig. 2. Real time anomaly detection

The diagram affords a -phase procedure for video-based totally anomaly detection: the training segment and the testing phase. In the training section, a fixed of video frames commonly containing most effective everyday behavior is used as enter. These frames undergo feature extraction, wherein applicable characteristics inclusive of motion patterns, item appearances, or spatial-temporal capabilities are derived using techniques like Convolutional Neural Networks (CNNs). The extracted features are then fed right into a model mastering factor, which includes training a device learning or deep mastering version to apprehend and represent normal conduct. The resulting version captures the normal styles determined in the enter statistics and is saved to be used during the trying out section. In the testing segment, a new set of video frames probably containing both normal and anomalous occasions is brought. Just like inside the education phase, functions are extracted from each frame the use of the identical method. These features are then evaluated through the paradox scoring module, which makes use of the previously skilled model to decide how a whole lot every frame deviates from the learned regular styles. Based on the anomaly ratings, frames are classified into classes: anomalous or regular. Frames that extensively differ from the educated model’s expectations are categorized as anomalous. This entire system is essential in surveillance structures, industrial protection, or intelligent shipping programs, where detecting deviations from normal behavior is critical. The first-class of detection relies closely at the accuracy of feature extraction and the robustness of the getting to know model in taking pictures regular patterns all through education.

Fig. 3. Predictive Maintainance in Data Centers

The photo represents a conceptual visualization of predictive upkeep in information facilities, illustrated in a stylized, digital way. Predictive protection is a proactive technique that leverages records analytics, tool studying, and sensor generation to count on disasters earlier than they occur, thereby minimizing downtime and optimizing machine lifespan. In the diagram, the data center surroundings is depicted with a couple of rows of server racks, cooling gadgets, power distribution units, and network devices. Several technicians or engineers are proven interacting with device, in all likelihood appearing routine inspections or responding to signals generated through the predictive device. The presence of sensors and manage gadgets embedded in equipment shows the continuous collection of operational statistics together with temperature, vibration, humidity, strength intake, and fan pace. This actual-time information is important for identifying deviations from regular working situations. The records amassed by those sensors is transmitted to centralized tracking systems or cloud-based totally analytics systems wherein it is processed and analyzed using AI and machine studying algorithms. These algorithms pick out patterns, hit upon anomalies, and predict potential equipment failures. Once an issue is expected such as an overheating server or a failing power supply alerts are sent to records center workforce via dashboards or mobile notifications, enabling well timed preservation earlier than breakdowns arise. By implementing predictive renovation, facts centers can achieve higher operational performance, lessen unscheduled downtime, decrease repair charges, and expand the lifecycle of critical equipment.

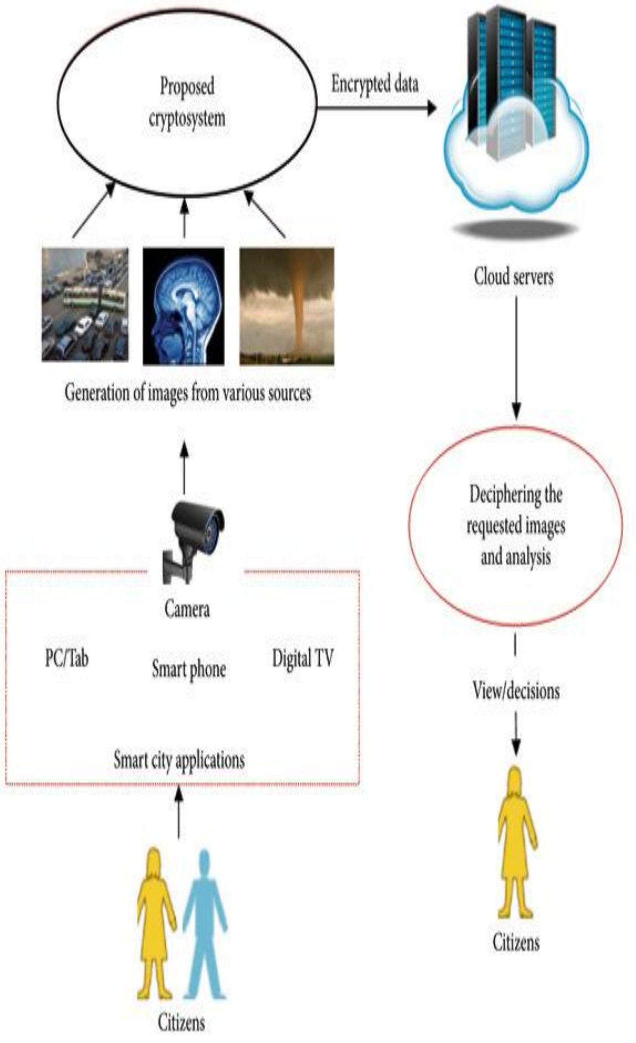

Fig. 4. Secure Data Transmission Layer

The diagram illustrates the workflow of a proposed cryptosystem for smart town image processing and analysis, that specialize in stable records transmission and choice-making for residents. It showcases how photos from various resources are securely amassed, encrypted, transmitted, and analyzed for public use. The procedure starts with the technology of pix from various sources, consisting of surveillance cameras, smartphones, clinical imaging gadgets (e.G., mind scans), and environmental tracking systems (e.G., weather-related occasions like tornadoes). These sources are normally part of smart metropolis programs, which include gadgets like PCs, tablets, smartphones, and digital TVs used by residents in urban environments. Once the pictures are captured, they may be fed into a proposed cryptosystem. This machine is answerable for encrypting the picture data to make sure records security and privateness for the duration of transmission. The encrypted image information is then sent to cloud servers, which act as a secure garage and processing platform. In the cloud servers, a committed module is chargeable for decoding the encrypted pix and reading the asked information. This step may additionally involve going for walks photo recognition algorithms, anomaly detection, or contextual analysis based totally on smart metropolis necessities (e.G., detecting visitors congestion, scientific emergencies, or weather warnings). After the analysis is whole, the processed records or decisions together with alerts, recommendations, or visible outputs are transmitted again to the stop-customers. These customers are the citizens, who view the effects and make choices accordingly thru their related devices. This system is designed to facilitate actual-time selection-making, decorate urban residing, and make certain stable information handling in clever town infrastructures.

IX. IOT Networks Security

IoT Networks Security refers to the practices, protocols, and technology used to protect Internet of Things (IoT) devices and the networks they operate on from cyber threats and unauthorized get admission to. With the rapid growth of IoT gadgets including smart domestic appliances, scientific sensors, commercial machines, and smart metropolis infrastructure the assault floor has extensively extended, making IoT protection a important concern. IoT devices usually have restricted processing energy, reminiscence, and storage, which makes it challenging to put in force conventional safety features. Moreover, many IoT devices are deployed in far flung or uncontrolled environments, making them vulnerable to bodily tampering and network-primarily based assaults.

Common protection threats consist of records breaches, malware infections, device hijacking, denial-of-carrier (DoS) attacks, and guy-in-the-center (MitM) attacks. To stable IoT networks, numerous layers of safety are essential. Device-level security consists of robust authentication mechanisms, secure boot techniques, and firmware integrity checks. Network-level security involves encryption protocols (inclusive of TLS/SSL), firewalls, and intrusion detection structures (IDS) to prevent unauthorized conversation and statistics leaks. Cloud and facts safety ensure that the information gathered and transmitted via IoT devices is encrypted, anonymized, and saved securely. A key component of IoT protection is everyday software program updates and patch management to restoration vulnerabilities. Additionally, implementing get entry to control policies and tool identification management allows in ensuring handiest legal customers and structures can interact with IoT devices.

X. Result

Securing electric infrastructure in records centers the usage of Artificial Intelligence (AI) results in better reliability, decreased downtime, and proactive fault prevention. AI algorithms examine real-time data from sensors to locate anomalies, expect equipment screw ups, and optimize electricity utilization. This effects in stepped forward operational efficiency, early identification of electrical dangers, and automated responses to capability threats. AI-pushed systems allow non-stop tracking and intelligent choice-making, making sure the safety and resilience of strength structures. Ultimately, AI integration minimizes human error, lowers upkeep fees, and strengthens the general protection posture of the facts middle's electric infrastructure, ensuring uninterrupted provider transport and gadget toughness.

TABLE I. IOT NETWORK SERVICES

IOT Network Assignment		
SL.No	***Effectiveness of IOT Network services***	***IOT Network Services secure***
1	The effectiveness of IoT community services lies of their potential to enable seamless verbal exchange, automation, and real-time decision-making throughout a huge variety of linked gadgets. These offerings facilitate records collection, transmission, and analysis from sensors and actuators embedded in various environments which include houses, industries, healthcare, and smart cities..	Securing IoT community offerings is crucial because of the substantial range of connected gadgets and the touchy records they manage. These networks are often susceptible to cyber threats including data breaches, unauthorized get right of entry to, and denial-of-carrier assaults. To make certain protection, IoT community services put into effect multiple layers of safety together with sturdy encryption protocols (like TLS), stable device authentication, and community segmentation to isolate essential structures.
2	Technologies like LPWAN, 5G, and part computing enhance the velocity and responsiveness of IoT networks, whilst protocols which include MQTT and CoAP make certain lightweight and secure data change. Additionally, IoT platforms integrate cloud services to control huge volumes of records and observe AI-driven analytics for actionable insights. Overall, the effectiveness of IoT network services is pondered of their capacity to reduce operational fees, increase safety, and enhance the nice of existence by using allowing smarter and greater responsive systems.	Firewalls, intrusion detection structures (IDS), and continuous monitoring tools help detect and respond to malicious pastime in real time. Additionally, everyday firmware updates and patch control cope with vulnerabilities as they are discovered. Secure conversation protocols like MQTT with TLS and CoAP with DTLS are used to prevent eavesdropping and tampering throughout statistics transmission.

XI. Conclusion

In conclusion, IoT community offerings are remodeling the way devices talk, manner records, and have interaction with their environments across a huge range of industries, which include healthcare, manufacturing, transportation, and clever towns. These services permit actual-time tracking, automation, and facts-pushed selection-making, notably enhancing operational performance, reducing fees, and improving user studies. However, because the adoption of IoT keeps to grow, so does the complexity and scale of the networks concerned, bringing new challenges associated with overall performance, scalability, and, most critically, protection.

Security stays a cornerstone for the successful implementation and operation of IoT networks. Without robust protection mechanisms, those networks are at risk of cyber threats along with statistics interception, unauthorized device get right of entry to, and disbursed denial-of-carrier (DDoS) assaults. Therefore, a comprehensive safety framework is essential, incorporating encryption, secure verbal exchange protocols, access control, tool authentication, and continuous tracking. Employing a "protection by design" technique guarantees that safety is embedded from the floor up, no longer brought as an afterthought. Furthermore, leveraging advanced technology which includes synthetic intelligence (AI) and system learning (ML) complements the effectiveness of IoT networks by using enabling predictive protection, anomaly detection, and adaptive protection mechanisms. These technologies allow networks to examine from statistics patterns and reply to ability threats in actual time, thereby growing reliability and consider.

References

[1] J. C. Haass, "Cyber threat intelligence and machine learning," IEEE Xplore, vol. 2, no. 1, pp. 156–159, Sep. 2022.

[2] N. Gupta, I. Traoré, and P. M. F. D. Quinan, "Automated event prioritization for security operation center using deep learning," IEEE Xplore, vol. 2, no. 1, pp. 5864–5872, Dec. 2019.

[3] S. Rass, S. König, J. Wachter, V. Mayoral-Vilches, and E. Panaousis, "Game-theoretic APT defense: An experimental study on robotics," Comput. Secur., vol. 132, Sep. 2023, Art. no. 103328.

[4] Z. T. Sworna, C. Islam, and M. A. Babar, "APIRO: A framework for automated security tools API recommendation," ACM Trans. Softw. Eng. Methodol., vol. 32, no. 1, pp. 1–42, Jan. 2023.

[5] J. Kinyua and L. Awuah, "AI/ML in security orchestration, automation and response: Future research directions," Intell. Autom. Soft Comput., vol. 28, no. 2, pp. 527–545, 2021.

[6] C. H. Chi, S. Y. Ooi, E. H. Binti, Y. H. Pang, M. K. B. A. Yan, and K. I. B. Sidin, "Intelligent-based SIEM security email alert," in Proc. 11th Int. Conf. Inf. Commun. Technol. (ICoICT), Aug. 2023, pp. 481–486.

[7] H. V. Vo, H. P. Du, and H. N. Nguyen, "AI-powered intrusion detection in large-scale traffic networks based on flow sensing strategy and parallel deep analysis," J. Netw. Comput. Appl., vol. 220, Nov. 2023, Art. no. 103735.

[8] G. González-Granadillo, M. Faiella, I. Medeiros, R. Azevedo, and S. González-Zarzosa, "ETIP: An enriched threat intelligence platform for improving OSINT correlation, analysis, visualization and sharing capabilities," J. Inf. Secur. Appl., vol. 58, May 2021, Art. no. 102715.

[9] A. Sridharan and V. Kanchana, "SIEM integration with SOAR," in Proc. Int. Conf. Futuristic Technol. (INCOFT), Nov. 2022, pp. 1–6.

[10] K. Hughes, K. McLaughlin, and S. Sezer, "A model-free approach to intrusion response systems," J. Inf. Secur. Appl., vol. 66, May 2022, Art. no. 103150.

[11] T. Ahmed, A. Shah, M. Kolla, and R. Yellasiri, "Reduction of alert fatigue using extended isolation forest," in Proc. Int. Conf. Forensics, Analytics, Big Data, Secur. (FABS), Dec. 2021, pp. 1–5.

[12] K. Prabu and P. Sudhakar, "An automated intrusion detection and prevention model for enhanced network security and threat assessment," Int. J. Comput. Netw. Appl., vol. 10, no. 4, p. 621, Aug. 2023.

[13] X. Wang, X. Yang, X. Liang, X. Zhang, W. Zhang, and X. Gong, “Combating alert fatigue with AlertPro: Context-aware alert prioritization using reinforcement learning for multi-step attack detection,” Comput. Secur., vol. 137, Feb. 2024, Art. no. 103583.

[14] J. M. Spring and P. Illari, “Review of human decision-making during computer security incident analysis,” Digit. Threats, Res. Pract., vol. 2, no. 2, pp. 1–47, Jun. 2021.

[15] J. R. Goodall, E. D. Ragan, C. A. Steed, J. W. Reed, G. D. Richardson, K. M. T. Huffer, R. A. Bridges, and J. A. Laska, “Situ: Identifying and explaining suspicious behavior in networks,” IEEE Trans. Vis. Comput. Graphics, vol. 25, no. 1, pp. 204–214, Jan. 2019.

[16] H. J. Ofte and S. Katsikas, “Understanding situation awareness in SOCs, a systematic literature review,” Comput. Secur., vol. 126, Mar. 2023, Art. no. 103069.

[17] O. Akinrolabu, I. Agrafiotis, and A. Erola, “The challenge of detecting sophisticated attacks,” in Proc. 13th Int. Conf. Availability, Rel. Secur., Aug. 2018, pp. 1–9.

[18] H. Bennouri, A. Abdi, I. Hossain, and A. Pujol, “The role of SOC in ensuring the security of IoT devices: A review of current challenges and future directions,” in Proc. 12th Medit. Conf. Embedded Comput. (MECO), Jun. 2023, pp. 1–8.

[19] Z. T. Sworna, Z. Mousavi, and M. A. Babar, “NLP methods in host-based intrusion detection systems: A systematic review and future directions,” J. Netw. Comput. Appl., vol. 220, Nov. 2023, Art. no. 103761.

[20] S. Neupane, J. Ables, W. Anderson, S. Mittal, S. Rahimi, I. Banicescu, and M. Seale, “Explainable intrusion detection systems (X-IDS): A survey of current methods, challenges, and opportunities,” IEEE Access, vol. 10, pp. 112392–112415, 2022.