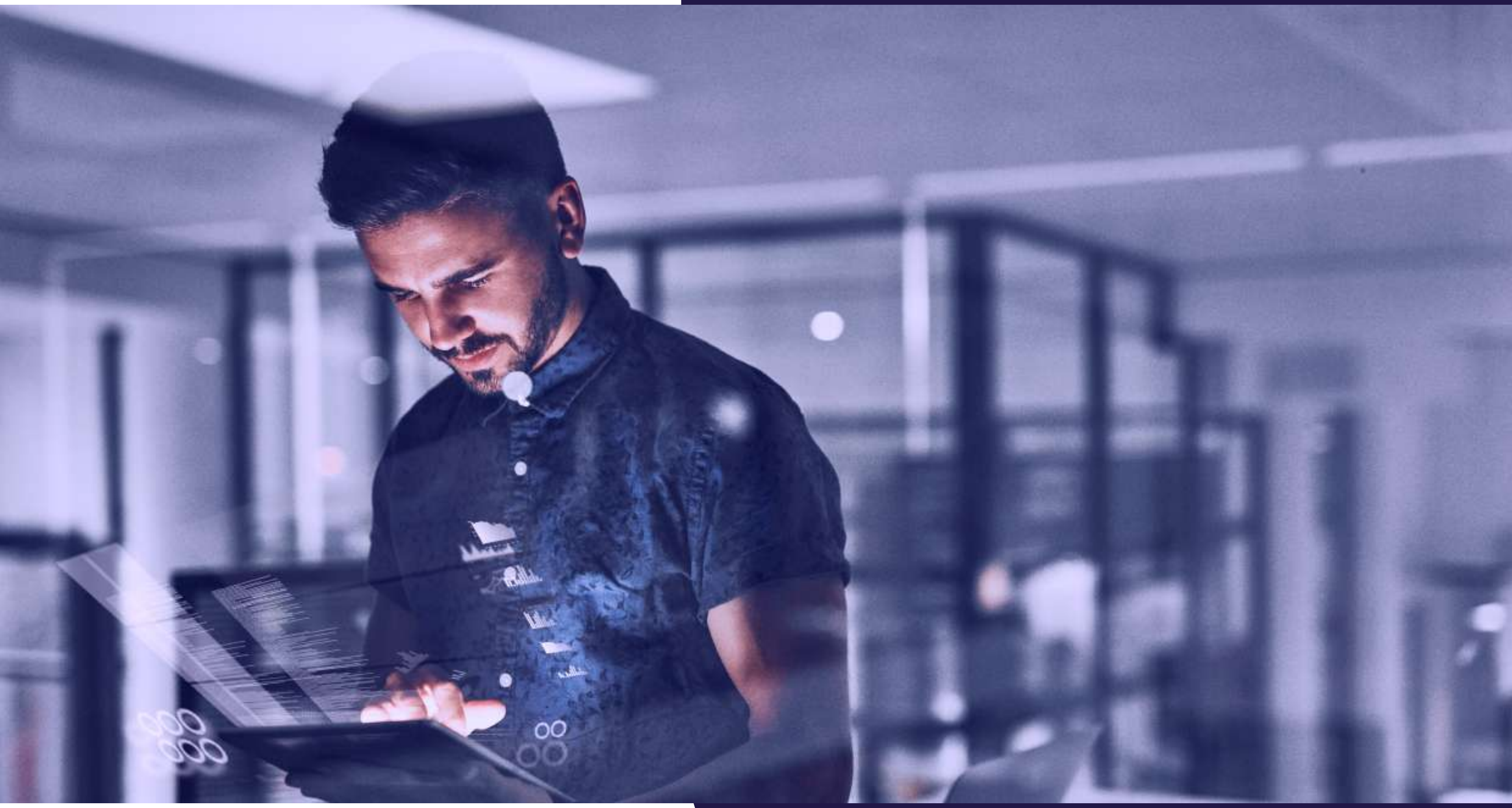


Next-Gen AI-Driven Network Automation

According to Gartner Forecasts, the Worldwide Artificial Intelligence Software Market will reach $62 Billion by the end of 2022, an increase of 21.3% from 2021. It is also said that market growth will accelerate as organizations progress in their AI maturity.

Table 1. AI Software Market Forecast by Use Case, 2021-2022, Worldwide (Millions of U.S. Dollars)

Segment	2021 Revenue	2021 Growth (%)	2022 Revenue	2022 Growth (%)
Knowledge Management	5,466	17.6	7,189	31.5
Virtual Assistants	6,210	12.0	7,123	14.7
Autonomous Vehicals	5,703	13.7	6,849	20.1
Digital Workplace	3,593	13.7	4,309	20.0
Crowdsourced Data	3,483	13.6	4,171	19.8
Others	27,049	14.1	32,827	21.4
Total	**51,503**	**14.1**	**62,486**	**21.3**

No longer limited to providing basic phone and internet service, the telecom industry is at the epicenter of technological growth, led by mobile and 5G broadband services in the Internet of Things (IoT) era. This growth is expected to continue due to the rapid adoption of artificial intelligence (AI) in the telecom industry. Projections show that the global AI in telecommunication market size will reach $14.99B by 2027, from $11.89B in 2020, at a CAGR of 42.6% during 2021-2027.

Introduction

While it is true that we are in the middle of one of the Artificial Intelligence hypes, it is also true that the combination of unprecedented computation power and data availability, with new variations of well-seasoned Machine Learning algorithms, is dramatically changing the optimization strategies for large ICT industries. Especially, the telecommunications industry has always had to deal with complex systems, stochastic contexts, combinatorial problems, and hard-to-predict users; Machine Learning-aided optimization was just waiting there to be used by telecoms. In this paper, we introduce some basic Machine Learning concepts and discuss how they can be used in the context of telecommunications networks, particularly in wired and wireless networks.

Enterprise AI Strategy & Implementation

In Automated networking, the use of ML technology can help automate routine network operations involving visualization, analysis, and troubleshooting. It has been a constant industry effort to replace manual network management processes with various ways of automation and now through ML-based algorithms which are indeed the de facto future.

The ML technology relies on various data sources like packet-level telemetry, account log messages, KPIs, and faults data generated by network devices and then analyzed by an ML algorithm. The algorithm then learns how to recognize normal versus abnormal behavior patterns over time, predicting when the element/node might be having issues before they occur.

The goal is for networks to adjust and optimize themselves based on real-time traffic flows, congestions, port failures, high rates of packet drops, configuration changes, software updates, and more without human intervention; here are some of the most popular AI/ML implementations.

Network automation and AI/ML - It can gain insights through analytics and AI/ML that guide more trusted automation processes that lower the cost of network operations and provide users with an optimal connected experience. These technologies help IT automate:

- The deployment and management of network policies
- The integration of zero-trust security solutions to help ensure network consistency
- The identification and classification of devices on the network

Over time, AI will increasingly enable networks to continually learn, self-optimize, and even predict and rectify service degradations before they occur.

Network Optimization - 5G networks began to roll out in 2019 and are predicted to have more than 1.7 billion subscribers worldwide – 20% of global connections — by 2025. AI is essential for helping communications service providers (CSPs) build self-optimizing networks (SONs) to support this growth. These allow operators to automatically optimize network quality based on traffic information by region and time zone.

Through a network controller and management dashboard, telemetry data from the network can be ingested and processed through AI/ML engines. These AI engines in the telecom industry use advanced algorithms to look for patterns within the data, enabling telecoms to both detect and predict network anomalies. As a result of using AI in telecom, CSPs can proactively fix problems before customers are negatively impacted.

AI and machine reasoning (MR) - Machine reasoning is built from a knowledge base and reasoner (or reasoning engine) which employs logical techniques such as deduction and induction to generate conclusions. The knowledge base is fed by various data sources: learnings from previous solutions; codified telecom domain expertise; product documentation; external data sources; and importantly – insights from all the machine learning agents in the network.

The reasoner, using the knowledge base, looks at the various predictions, applies logical rules to the knowledge base, and makes sure that business intent is followed while respecting all service level agreements and recommending a path towards the goal.

AI/ML and predictive analytics - AI-driven predictive analytics are helping telecoms provide better services by utilizing data, sophisticated algorithms, and machine learning techniques to predict future results based on historical data. This means operators can use data-driven insights to monitor the state of equipment and anticipate failure based on patterns. Implementing AI in telecoms also allows CSPs to proactively fix problems with communications hardware. In the short term, network automation and intelligence will enable better root cause analysis and prediction of issues. Long term, these technologies will underpin more strategic goals, such as creating new customer experiences and dealing efficiently with emerging business needs.

Use Cases for Network

Common Enterprise Network Issues	Monitoring Services	Security Services	Network Optimization & Maintenance Services
● **Wi-FI Authentication** – Incorrect username and password – Disabled authentication or authorization policy – Unavailability in database ● **LAN Network Fault** – Presence of duplicate IP or MAC addresses – Unintented shutdown of port by admin – VIAN misconfiguration – Failed DOT1x authentication ● **BGP Flapping** – Excessive update messages are sent for network reachability in case of an unstable routing peer	● **Network Traffic SLA Monitoring** – Network SLAs are monitored through continuous assessment of packet latency, jitters, RTT and packets dropped leveraging ICMP, TCP, UDP, RTP and HTTP protocols ● **Network Interface Bandwidth Utilization** – Excess bandwidth utiliution of network interface leads to dropped packets and link congestion ● **Monitoring Dropped Packets** ● **CPU Monitoring** – High CPU utilizatlon in network devices often leads to dropped packets and low network throughput ● **Remote Network Monitoring**	● **Network Anomaly & Security Detection** – Detect unusual outbound network traffic flow – Detect unusual communication with a server – Detect unusual outbound email activity – Detect port scanning activity on a specific host or several hosts – Detect suspicious login activities through compromised user credentials or hijack attempts – Block access to questionable webites and files hosted online – Block bandwidth hogging websites (e.g.,streaming or gaming sites)	● **Device Performance Optimization** – Management of device performance degradation ● **Predicting Preventive Maintenance Service** – Identify any lags in performance, connectivity timings

With real AI, the network becomes easier to operate. You can quickly configure, troubleshoot, and protect your network while minimizing errors and resolving network issues. And when you can fix problems before they impact users, you are delivering a next-level experience.

AI/ML helps us in detecting network access failures, such as authentication and authorization failures, in LAN and Wi-Fi systems to determine and remediate the root causes of network access failures. If authentication fails, it may be necessary to check all Syslog data from each network element and then utilize this Syslog data to identify the exact root cause of this error. Of course, this process can be time-consuming and may require a great deal of human effort.

Once a root cause is identified, remediation actions can be taken to fix the authentication issue, which again can require much time and effort by an individual.

Similarly, during the festive seasons like Christmas or the Sales seasons like Thanksgiving, there is always a spike in traffic that's much higher than in previous weeks which causes slowness on the Internet due to Bandwidth Utilization. Hence, AI/ML driven Enterprise strategy helps us in network bandwidth utilization monitoring as it is essential in finding the root cause of a slow network. It offers a network utilization monitor for providing comprehensive network traffic and bandwidth analysis based on SNMP monitoring and the flow of data. Streamlined network bandwidth utilization monitoring allows us to detect, diagnose, and resolve network performance issues with ease.

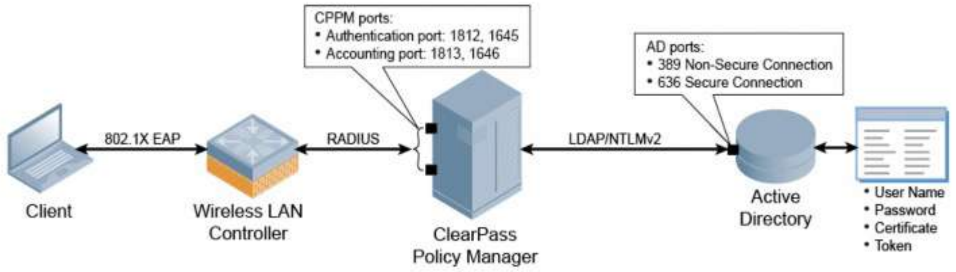
It also offers real-time alerts for bandwidth logs, so we can get notified when a device starts to use too much bandwidth. With customizable notification thresholds, it allows us to set simple or complex conditions to trigger alerts based on simple bandwidth utilization or nested conditions based on the network topology. Custom alerting also reduces unwanted alerts to the inbox, focusing on important or critical network issues only.

Methodology

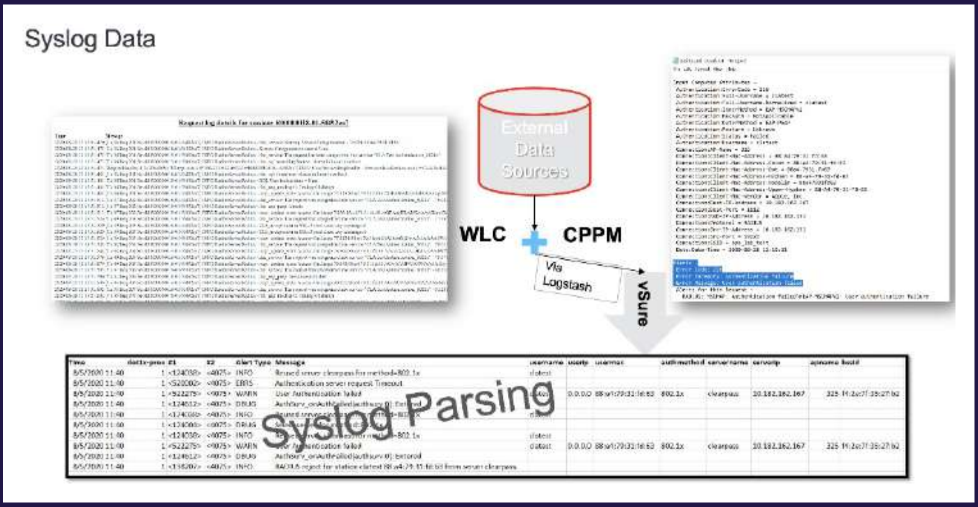
The four-step mechanism is configured to determine the relevant diagnostics given a set of symptoms and can be configured for automating the process of root cause analysis in a way that can generalize well to accommodate new types of problems.

1. Data Collection: Collect relevant data from the network and stream the data to a message bus. The network may be configured to handle a mixture of raw text and quantitative features obtained from network devices (e.g., L2 switches, wireless controllers, routers, firewalls, authentication servers, and authorization servers). As such, the network may introduce an ML pipeline that combines Natural Language Processing (NLP) techniques to extract relevant quantitative metrics, together with supervised learning models. The first step in this respect may be to rebalance a dataset to properly handle the relative rarity of the authentication and authorization failures.

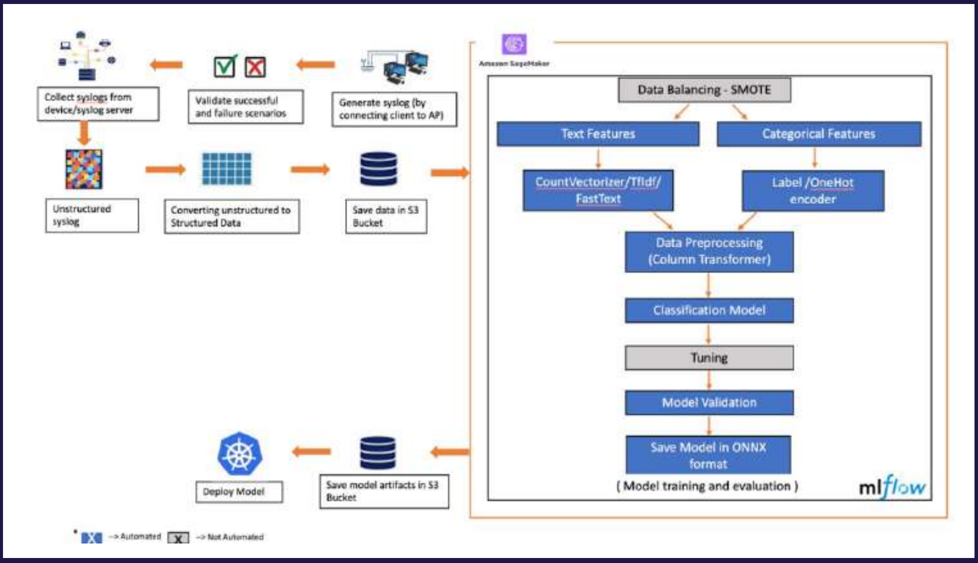
Targeted UseCase (WiFi Authentication Failure)



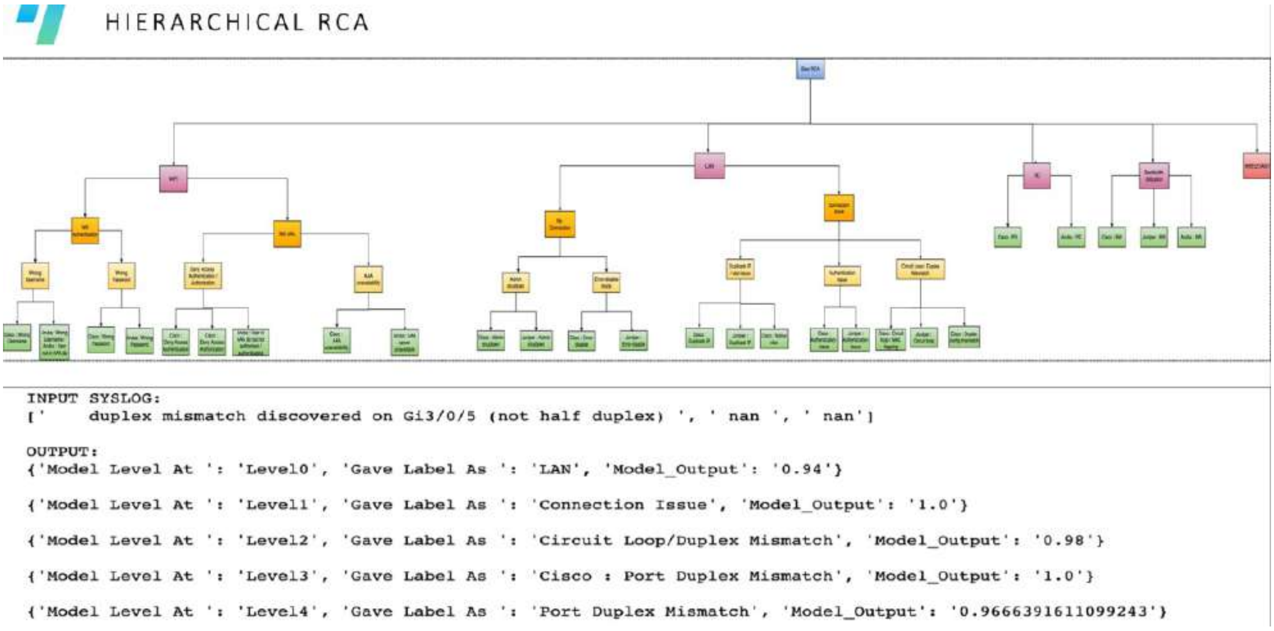
2. Data Cleaning & Pre-Processing: Syslog messages and datasets, obtained by the data collection module, may typically be in a complex, unstructured, and noisy format. To get high accuracy and precision, therefore, a tailored pre-processing step may be used in the present disclosure to make this textual data more insightful and suitable for model training.



For example, this may be achieved through a combination of techniques or strategies, such as stemming & lemmatization, OneHot Encoding, CountVectorizer, TF-IDF, Column Transformer, and FastText, which allows the root-cause analytics systems of the present disclosure to represent unstructured Syslog messages as fixed-size vectors, which are more suitable for ML algorithms.


Collect syslogs from device/syslog server
Validate successful and failure scenarios
Generate syslog (by connecting client to AP)
Unstructured syslog
Converting unstructured to Structured Data
Save data in S3 Bucket
Amazon SageMaker
Data Balancing - SMOTE
Text Features
Categorical Features
CountVectorizer/TfIdf/ FastText
Label /OneHot encoder
Data Preprocessing (Column Transformer)
Classification Model
Tuning
Model Validation
Save Model in ONNX format
(Model training and evaluation)
mlflow
Deploy Model
Save model artifacts in S3 Bucket
--> Automated
--> Not Automated

3. Model Training & Apply pre-trained ML models: To compute the distance of given symptoms (new data) to known diagnostics and diagnostic families from the hierarchical knowledge base. The hierarchical model may combine the regression output of all ML sub-models to predict the most likely root causes. For example, starting with the prediction of the root sub-model, the models may recursively traverse the hierarchical model to compute the regression output of each sub-model. By construction, each sub-model may be increasingly specific. If the accuracy of a sub-model (e.g., internal point or node in the tree) is below a threshold, the corresponding subtree may be discarded to optimize computational requirements. If the accuracy of a specific root cause is below another threshold, the system may automatically predict increasingly generic root causes until the accuracy is sufficient.



```
INPUT SYSLOG:
['    duplex mismatch discovered on Gi3/0/5 (not half duplex) ', ' nan ', ' nan']

OUTPUT:
{'Model Level At ': 'Level0', 'Gave Label As ': 'LAN', 'Model_Output': '0.94'}

{'Model Level At ': 'Level1', 'Gave Label As ': 'Connection Issue', 'Model_Output': '1.0'}

{'Model Level At ': 'Level2', 'Gave Label As ': 'Circuit Loop/Duplex Mismatch', 'Model_Output': '0.98'}

{'Model Level At ': 'Level3', 'Gave Label As ': 'Cisco : Port Duplex Mismatch', 'Model_Output': '1.0'}

{'Model Level At ': 'Level4', 'Gave Label As ': 'Port Duplex Mismatch', 'Model_Output': '0.9666391611099243'}
```

4. Filter and rank the diagnostics: Hierarchical models may combine the outcome of heuristic or statistical (non-ML) models. Each node in the hierarchical model is mapped to network automation workflows and can be triggered for Remediation if the distance calculated by the inference engine is within a certain trigger threshold.

AI/ML is beneficial in the following:

ML and AI help make enterprise networks more efficient by using data-driven algorithms to identify patterns within the enterprise infrastructure. For example, ML can be used through anomaly detection—or looking at changes within your environment over time and determining whether they fit within a normal pattern or not. Here are eight roles that AI and ML play in network management:

Log analysis - The role of AI and ML in log analysis is simple: it detects, collects, and analyses logs from all parts of an enterprise environment (e.g., routers, switches, and WAN optimization devices). It then provides real-time insights into network performance, so you can pinpoint problems faster than ever before.

Logs can be seen as textual data, which means that NLP techniques like Longest Common Substring (LCS), Bert, or GPT-3 language model can be applied to gather and summarize the same logs in an organized manner, making it possible to search for specific types of logs.

Advanced analytics - Advanced analytics methods based on machine learning modeling, can make the computing process smart through intelligent decision-making in a business process. A general structure of a machine learning-based predictive has a wide range of methods such as regression and classification analysis, association rule analysis, time-series analysis, behavioral analysis, log analysis, and so on.

One of the most common applications is Anomaly detection which uses time series over Long Short-Term Memory (LSTM) modeling which is a neural network model. The neural network model is utilized to model a system log as a natural language sequence. This enables studying log patterns and detecting anomalies when there is a deviation from the trained model. In addition, workflows are also constructed under the underlying system log so that developers can analyze the anomaly and perform the necessary RCA for it.

Performance monitoring - Nowadays, with software-defined networking (SDN) becoming increasingly popular, monitoring performance has become steadily more important.

SDN is often used to help automate network tasks and free network administrators from mundane tasks, like troubleshooting SNMP (simple network management protocol) issues. Now, automated tools can help monitor traffic flows across an SDN-enabled network.

Security alerts - Automated networking requires an automated security system, which is why many companies are investing in AI and ML. As a result, organizations can now use these emerging technologies to automate network security tasks such as malware detection, vulnerability scanning, intrusion prevention systems (IPS), advanced threat protection (ATP), DDoS mitigation, and more.

With these technologies, enterprises can achieve better uptime while decreasing human error by leveraging automated networking to create more efficient networks for all users and devices.
Systems can incorporate an assess-centered methodology called STRIDE-AI, an AI/ML component, that helps in the identification and analysis of threats, Malware prediction, Spoofing, Tampering, DDoS, etc.

Traffic management - Automated tools help manage traffic to optimize performance. With these tools, information about Internet Protocol (IP) addresses is automatically gathered for analysis. The data is then integrated with other business or engineering intelligence systems to automate network management tasks.

Intelligent programmable automation controller (IPAC) - A key component to automating networks with AI is programmable automation controllers (PACs). These devices allow network administrators to automate tasks using software instead of doing everything manually.

It can be constructed with the help of a Predictive maintenance procedure using AI as follows:

- A learning model including a threshold value is generated from current machine data.
- The machine is monitored based on the learning model. If the machine status exceeds the threshold value, a notification is issued.
- The machine status is checked. If no error is found, a new threshold value is set.
- An error occurs while threshold value setting and monitoring are repeated. Components are replaced.
- A new learning model, including the threshold value, is generated based on the previous error level after components are replaced. Repeating these steps makes status-based maintenance more reliable.

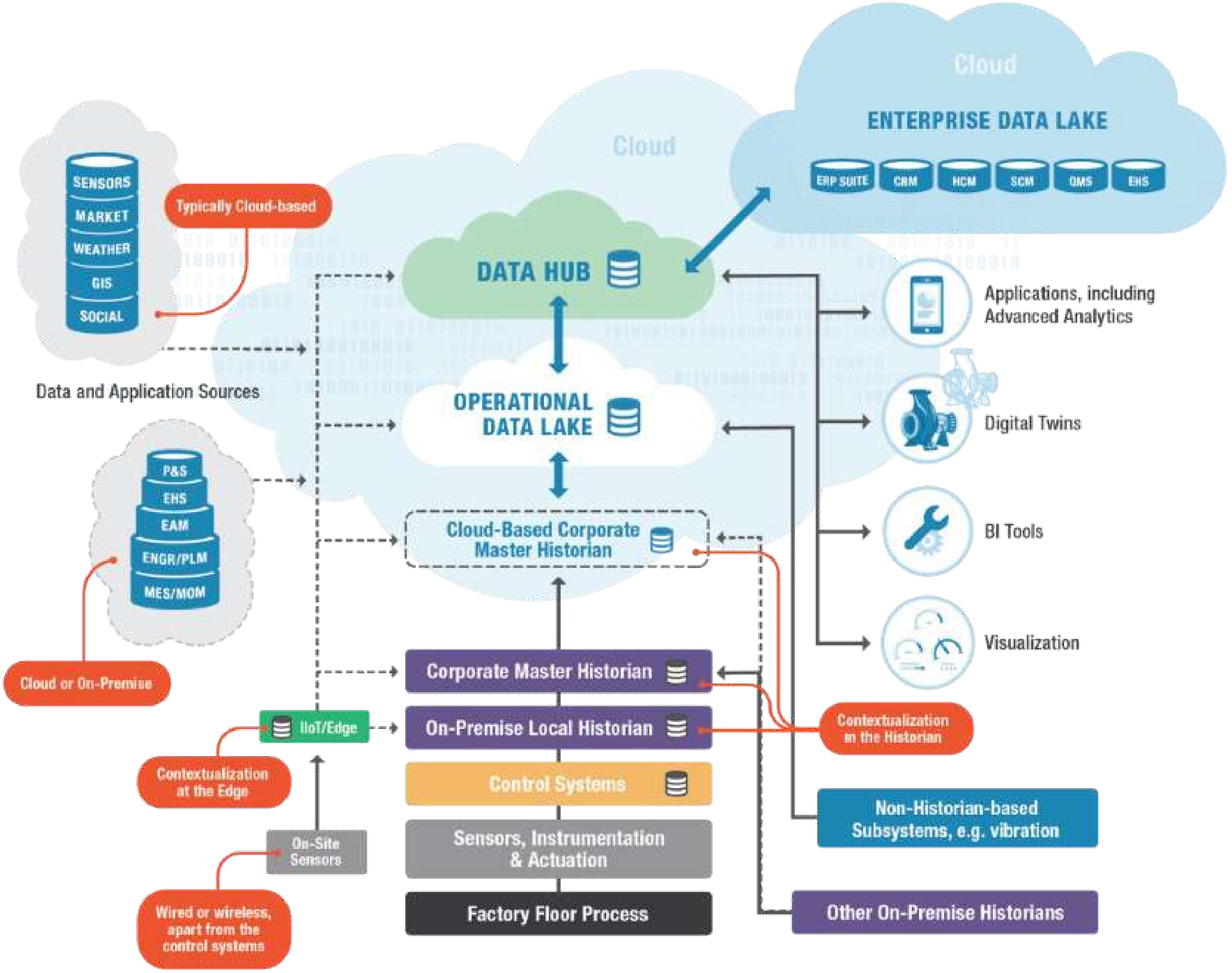
Autonomous scanning and patching - Modern switches employ AI to automate certain tasks, such as maintenance. These automated tools allow network administrators to shift their focus from a reactive state to one that is more proactive, allowing them to monitor and identify issues before they become problems. Some vendors even provide self-healing networks using AI techniques like ML. The goal is to reduce or eliminate outages by automatically remediating faults as soon as they occur.

Automated provisioning - With automated provisioning, you can automate all aspects of network deployment, from initial configuration to ongoing maintenance. In addition, automated networking complements continuous service monitoring by measuring performance against SLAs, triggering specific actions based on threshold breaches or other changes, and proactively alerting administrators. The result is an automated network that's always ready for use, even under heavy loads.

The Future of AI in the Telecom Industry

AI in the telecom market is increasingly helping CSPs manage, optimize, and maintain infrastructure and customer support operations. As tools and applications become more available and sophisticated, the future of AI/ML in the telecom industry will continue to develop. Employing AI, telecoms can expect to continue accelerating growth in this highly competitive space.

The below architecture gives us a glimpse of Telecom Data Hub, which provides Network optimization, predictive maintenance, virtual assistants, RPA, fraud prevention, and new revenue streams are all examples of telecom AI/ML use cases where the technology has helped deliver added value-for enterprises.


Cloud
ENTERPRISE DATA LAKE
ERP SUITE
CRM
HCM
SCM
QMS
EHS
Cloud
SENSORS
MARKET
WEATHER
GIS
SOCIAL
Typically Cloud-based
Data and Application Sources
DATA HUB
OPERATIONAL DATA LAKE
Cloud-Based Corporate Master Historian
P&S
EHS
EAM
ENGR/PLM
MES/MOM
Cloud or On-Premise
Applications, including Advanced Analytics
Digital Twins
BI Tools
Visualization
Corporate Master Historian
IIoT/Edge
On-Premise Local Historian
Contextualization in the Historian
Contextualization at the Edge
Control Systems
Non-Historian-based Subsystems, e.g. vibration
On-Site Sensors
Sensors, Instrumentation & Actuation
Wired or wireless, apart from the control systems
Factory Floor Process
Other On-Premise Historians

©LNS Research. All Rights Reserved.

ABOUT BRILLIO

At Brillio, our customers are at the heart of everything we do. We were founded on the philosophy that to be great at something, you need to be unreasonably focused. That's why we are relentless about delivering the technology-enabled solutions our customers need to thrive in today's digital economy. Simply put, we help our customers accelerate what matters to their business by leveraging our expertise in agile engineering to bring human-centric products to market at warp speed. Born in the digital age, we embrace the four superpowers of technology, enabling our customers to not only improve their current performance but to rethink their business in entirely new ways. Headquartered in Silicon Valley, Brillio has exceptional employees worldwide and is trusted by hundreds of Fortune 2000 organizations across the globe.

https://www.brillio.com/
Contact Us: info@brillio.com