PROJECT 2 - NEW STRATEGIC TECHNOLOGY TRENDS

MGS 602 - GLOBAL IT INFRASTRUCTURE MANAGEMENT

AKHILESH ANAND UNDRALLA
UNIVERSITY AT BUFFALO

12/04/2021

Cyber Security Mesh

Cybersecurity mesh is a recent trend that has flexible architecture providing secure integration of distributed workforce, IoT devices, and various essential business and operational services. Secure integration can be achieved through maintaining the operational technology infrastructure of the business from threat actors like denial of service, malware, phishing, remote access control, ransomware and botnet infections in a single platform using cloud services. This architecture also covers integration of Secure Access Services Edge (SASE) which is a mix of security and network connectivity technologies within a unified cloud platform that includes stand-alone products such as Extended Detection and Response (XDR), Data Loss Prevention (DLP) and Cloud Access Security Brokers (CASB). The goal of cybersecurity mesh is to have an open, interoperable security platform built with accepted digital trust standards. This architecture focuses on cloud-native applications which are based on self-contained and independently deployable microservices.

Implementing cybersecurity mesh would help enterprises in applying security policies at network level using firewalls, ports, protocols, allowing/blocking IP addresses. A cybersecurity mesh uses zero trust architecture in which all the connections are considered as untrusted unless they are verified within an enterprise network while utilising securely accessing all the data and the remote systems. This ensures protecting each device and access point outside of a secure perimeter of an enterprise network and enables supporting development (Dev) and IT operations (Ops) with flexibility, scalability that significantly reduces costs as well as boosts speed of deployment.

This trend is on the way to become a reality due to the remote work revolution. Remote work calls for employees to no longer work from just the office perimeter which makes adopting zero trust architecture a primary objective to secure an enterprise network. An example would be the infamous ‘SAP_ALL’ authorization profile that allows users to perform all the tasks in a SAP system. This is detrimental in maintaining a secure infrastructure that adopts the practice of giving full admin access to all the users unnecessarily. Cyber Security mesh redesign the network security with centralized identity level solution and promotes mandatory creation of policies that will protect enterprises resources at the individual level.

Privacy-enhancing computation

Privacy-enhancing computation is another new trend in technology that enables businesses to handle data securely. A trusted decentralized platform with systems to encrypt sensitive data and algorithms before analytics or processing. Currently, privacy enhancing applications innovation is geared towards utilizing techniques such as Differential privacy, Homomorphic encryption, Secure multi-party computation, Zero-knowledge proof, Trusted execution environments that are commercially available for deployment.

Differential privacy uses mathematical algorithms to insert noise into sensitive data while ensuring there is no significant deviation from the original. This makes it impossible for adversaries to analyse data elements whenever they gain access to sensitive data. Homomorphic encryption uses a secure form of encryption called homomorphic encryption that enables core business functions like encrypted searches and encrypted analytics like machine learning and Artificial Intelligence(AI) with built-in algorithms. Secure multiparty computation keeps individual inputs private while integrating multiple parties to operate on sensitive data i.e., to decode anything other than possible ensuring that no single party is able to decode anything other than possible business outcomes. ‘Zero knowledge proofs’ uses a cryptographic technology in which data won’t be revealed even during the process of verifying the data. Trusted execution environments is a perimeter-based security framework that enables end-to-end security while data is stored, processed and protected within connected trusted applications (TA).

Privacy enhanced computation serves the need to share data while ensuring security and privacy. This is useful in a business-to-business (B2B) environment that is looking for ways to transmit data safely. This trend addresses all of the increasing concerns over data privacy throughout the data-in-use lifecycle. Today, a wide range of new privacy-enhancing computation techniques are emerging. This paves a way for businesses to monetize huge data available and benefit from external innovation. These techniques will be beneficial when third-party service providers can add value to the business operations when organizations are not willing to share access to in-house data. Since a new trend of virtual/remote work has been a new normal, many of these techniques will provide novel frameworks that can be developed and tested specifically by large enterprises.

Data Fabric

Another trend, Data Fabric is an architectural approach that provides full point-to-point connectivity between nodes. Data fabrics provide transformable services covering data access, integration, transformation, modeling, visualization, governance, and delivery capabilities using in-build services. Data fabric connects all these various services using connectors to data centric ecosystems. Data fabric uses Machine Learning & Artificial Intelligence that helps in improving data quality using all of the above services. Data fabric eliminates dependencies on multiple proprietary tools, resources and improves access to reliable and qualitative data. Thus, the process enables simpler data lifecycle implementation. This architecture provides efficiency by providing a unified platform to perform automated data management throughout the typical data lifecycle implementation – sourcing, cleaning, orchestrating, preparing, archiving, & analyzing.

The main objective of data fabric includes removing obstacles in cleaning the data while performing analytical functions providing extended agility and optimized tool performance while using valuable data-centric services. A process fabric which is a critical aspect of data fabric contains data operation superstructure that combines all the existing tools and orchestrates data pipelines and workflows. Process fabric connects people, processes, and technology (tools) together where data fabric sits on top of all these interconnect architecture. This setup alleviates several operational bottlenecks and resolves disconnected data management verticals.

Data Scientists at present are faced with the hassle of spending most of the time in searching, cleansing, and governing data rather than analysing. This is a hindrance while maintaining compliance with the 4V principle of big data – Volume, Velocity, Variety, Veracity, and Value. Using Data fabric challenges like higher production rates, inadequacy in managing the data, large number of sources, poor system response time. Rectifying these challenges using data fabric architecture could result in satisfied customers with quicker delivery time and inexpensive system maintenance. Data fabric is slowly rising with the recent adoption of ‘XOps’ (DataOps, MLOps, and DevOps) across organizations. This trend also reflects a remote/digital centric business model to enhance employee productivity, improve consumer and service providers touchpoints, and build innovative product experiences.

References:

Gartner_Inc. (n.d.). The Top 8 Cybersecurity Predictions for 2021-2022. Retrieved from https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022

Cybersecurity Mesh plays a significant role in businesses: Here's How. (2021, March 10). Retrieved from https://www.analyticsinsight.net/cybersecurity-mesh-plays-a-significant-role-in-businesses-heres-how/

Cybersecurity Mesh and Decentralized Identity Explained. (2021, November 30). Retrieved from https://www.esecurityplanet.com/networks/cybersecurity-mesh-decentralized-identity-emerging-security-technology/

Townsend, A. (2021, March 31). From Zero Trust to Cybersecurity Mesh. Retrieved from https://www.onelogin.com/blog/zero-trust-cybersecurity-mesh

Bernstein, C. (2020, March 10). What is a Trusted Execution Environment (TEE)? Definition from WhatIs.com. Retrieved from https://searchitoperations.techtarget.com/definition/trusted-execution-environment-TEE

Half of large companies to adopt privacy-enhancing computation by 2025. (2020, October 26). Retrieved from https://dataprotection.news/half-of-large-companies-to-adopt-privacy-enhancing-computation-by-2025/

Mallu, S. R., & 20, J. (2021, July 14). Is differential privacy the ideal privacy-enhancing computation technique for your business? Retrieved from https://www.helpnetsecurity.com/2021/07/20/differential-privacy/

Everything You Need to Know About Gartner Tech Trend Privacy-Enhancing Computation. (n.d.). Retrieved from https://stefanini.com/en/trends/news/know-about-gartner-tech-trend-privacy-enhancing-computation.

Blog - DataOps Enables Your Data Fabric. (2021, April 28). Retrieved from https://datakitchen.io/dataops-enables-your-data-fabric/

What Data Is Behind This Metric? (n.d.). Retrieved from https://www.qlik.com/blog/what-data-is-behind-this-metric

Author Details Expersight Intelligence Expersight is a leading market intelligence, & Details, A. (2021, July 06). Global Data Fabric Market Trend Analysis From 2021-25. Retrieved from https://expersight.com/global-data-fabric-market-trend-analysis/