L'Internet des Objets dans l'éducation

Améliorer les expériences d'apprentissage et d'enseignement en tirant parti de l'IoT sur une infrastructure sécurisée

Résumé de la solution
IoT dans l'éducation

Alcatel·Lucent
Enterprise

L'IoT change fondamentalement l'équation commerciale dans l'éducation

L'Internet des Objets (IoT) a le potentiel de transformer l'éducation en modifiant profondément la façon dont les écoles, les collèges et les universités recueillent des données, s'interfacent avec les utilisateurs et automatisent les processus. L'IoT consiste en la mise en réseau d'objets physiques via l'utilisation de capteurs embarqués, actionneurs et autres dispositifs qui peuvent collecter et transmettre des informations sur les activités dans tout le campus en temps réel. Quand l'IoT est combiné avec des technologies telles que la mobilité des utilisateurs et l'analyse de données, il est porteur d'un nouveau paradigme dans l'éducation. L'IoT permet aux institutions de:

- Offrir aux étudiants des manières d'apprendre plus innovantes, avec des méthodes personnalisées plus dynamiques, comme les manuels numériques ou l'apprentissage basé sur le jeu.
- Changer le système des cours et la réalisation des tests des enseignants avec un équipement audio-visuel intelligent, comme des enregistreurs vidéo numériques pour la lecture et les tests en ligne.
- Simplifier les opérations pour les administrateurs de l'école par la surveillance proactive de l'infrastructure critiqueet créer des processus plus efficaces et plus rentables pour le chauffage, la ventilation, la climatisation, la gestion de l'éclairage et des équipements.
- Fournir un environnement sécurisé pour les étudiants et les enseignants avec des caméras de surveillance numériques, des serrures de porte intelligentes et des autobus scolaires connectés.

Scénarios pour l'IoT dans l'éducation

Les solutions IoT promettent de rendre les écoles et les universités plus intelligentes ainsi que plus efficaces dans leurs actions. L'IoT a le potentiel de redéfinir la façon dont les étudiants, les enseignants et les administrateurs interagissent et se connectent à la technologie et aux équipements dans l'environnement de leur salle de classe, participant ainsi à l'amélioration du processus d'apprentissage et des résultats éducatifs tout en réduisant les coûts. Des exemples de solutions IoT pour l'éducation comprennent:

- Tableaux blancs intelligents et autres médias numériques interactifs pour rassembler et analyser des données que les enseignants et les étudiants peuvent utiliser en classe - ou n'importe où et quand - optimisant le processus éducatif et ses résultats.
- Des solutions intelligentes telles que des capteurs de température et de l'équipement pour le chauffage, la ventilation et l'air conditionné pour réduire la consommation d'énergie et automatiser la gestion des opérations.
- Des cartes d'étudiant intelligentes, des dispositifs de suivi des présences, des systèmes de suivi des autobus scolaires et des capteurs de stationnement qui contrôlent les allées et venues des étudiants.
- Serrures de porte sans fil, caméras de surveillance connectées et systèmes de reconnaissance faciale qui assurent la sécurité des enseignants, des étudiants et du personnel.
- Des programmes de recherche améliorés avec des systèmes plus avancés et automatisés dans les principaux domaines d'étude, comme la médecine, l'agriculture et l'ingénierie.

Les défis du déploiement de l'IoT

L'IoT permet une gestion des flux de données sans précédent, représentant un véritable défi pour la performance, les opérations et la gestion de l'infrastructure du réseau avec une augmentation des risques de sécurité de toute origine. Pour résoudre ces problèmes, les administrateurs réseau dans les établissements scolaires doivent adapter leurs conceptions de réseau traditionnelles de façon à doter le réseau d'un niveau plus élevé d'intelligence, d'automatisation et de sécurité.

Les écoles et les universités ont besoin d'une infrastructure de réseau rentable et capable de gérer en toute sécurité et simplicité de vastes flux de données. L'infrastructure doit:

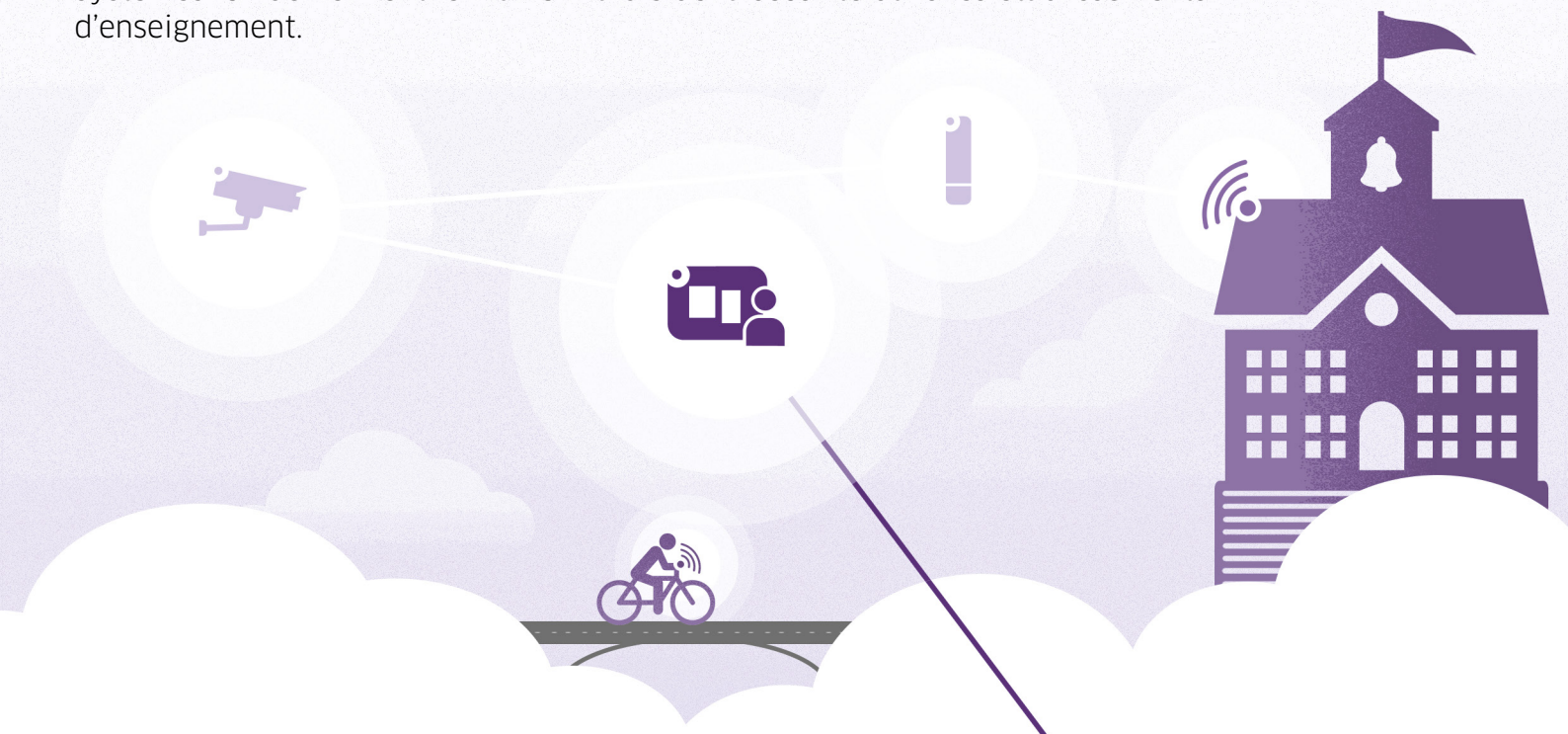
- **Fournir un processus simple et automatisé pour l'intégration de l'IoT.** Les grands systèmes IoT peuvent contenir des milliers d'équipements et de capteurs, et leur gestion manuelle est complexe et sujette à des erreurs. L'intégration automatisée permet à l'infrastructure de réseau de reconnaître dynamiquement les appareils et les affecter à des endroits appropriés dans le réseau sécurisé.
- **Fournir les ressources réseau appropriées pour que le système IoT puisse fonctionner correctement et efficacement.** Beaucoup d'équipements d'un système IoT offrent une information critique qui nécessite un niveau spécifique de qualité de service (QoS). Par exemple, des cas d'utilisation éducative nécessitent la réservation d'une bande passante appropriée dans une infrastructure de réseau à haute performance pour assurer une prestation de services fiable.
- **Créer un environnement sécurisé contre les cyberattaques et la perte de données.** En effet, les dispositifs et capteurs en réseau de l'IoT étant sensibles aux attaques, la sécurité est essentielle pour atténuer les risques de la cybercriminalité. Cette sécurité est nécessaire à plusieurs niveaux, y compris dans le confinement des réseaux IoT eux-mêmes.

Les professionnels de l'informatique planifient de dévelpper l'IoT

Les professionnels de l'informatique prévoient déjà une utilisation accrue imminente de solutions IoT dans de nombreux secteurs. Selon l'enquête de 451 Research 2017 Trends in the Internet of Things, 67% des professionnels de l'informatique ont répondu que leurs entreprises avaient déjà déployé une solution IoT, ou avaient un projet de système IoT. 21% des répondants ont déclaré que leurs entreprises prévoyaient de déployer des solutions IoT dans les 12 mois, avec 11% déclarant que l'implémentation de l'IoT dans leurs entreprises serait complétée d'ici un an.

L'IoT augmente l'exposition des écoles et des universités à la cybercriminalité

La croissance de l'IoT dans les transports entraîne une explosion des menaces à la cybersécurité car la prolifération des capteurs et des équipements connectés élargit considérablement la surface d'attaque sur un réseau. L'IoT y est particulièrement sensible car la fabrication de beaucoup d'appareils IoT ne prend pas en compte leur sécurité, ou leur production est réalisée par des entreprises qui ne comprennent pas les exigences de sécurité actuelles. Par conséquent, les systèmes IoT deviennent le maillon faible de la sécurité dans les établissements d'enseignement.



- Le réseau d'une université dont le nom n'a pas été divulgué a été attaqué par son propre système de 5000 appareils IoT, comprenant des distributeurs connectés et des ampoules intelligentes, selon le rapport 2017 Data Breach Digestde Verizon. Les équipements piratés ont fait des centaines de recherches DNS (Domain Name Service) toutes les 15 minutes, rendant la connectivité au réseau de l'université insupportablement lente, voire inaccessible.[1]
- En 2017, des suprémacistes blancs ont piraté les imprimantes et télécopieurs en réseaux dans un certain nombre d'universités, y compris l'University of California, Berkeley, amenant les machines à imprimer de la propagande raciste.[2]
- Le botnet Mirai, qui a paralysé le service Internet à travers la côte Est des États-Unis et une grande partie de l'Europe de l'Ouest en asservissant à distance des millions de dispositifs IoT, a réalisé une attaque en 2016 sur le réseau informatique de la Rutgers University. Le logiciel Mirai a été conçu pour pirater des routeurs mal sécurisés, des caméras de sécurité et des dispositifs de surveillance des bébés.[3]

Un lycéen du Michigan a été pris en 2015 pendant qu'il perpétrait une attaque par déni de service distribuée (Distributed Denial of Service attack, DdoS) conçue pour saturer par intermittence le réseau informatique de son école. Le botnet à l'origine de la cyberattaque était constitué de dispositifs IoT en réseau ciblés tels que des caméras de surveillance et des routeurs.[4]

Construire une infrastructure de réseau IoT sécurisé

Protéger le trafic et les d'équipements IoT au sein des réseaux des écoles et universités est un défi qui ne peut être résolu par aucune technologie classique de sécurité. Cela nécessite une approche stratégique qui tire parti de multiples mesures de sécurité.

Pour aider les établissements scolaires à tirer parti des avantages et à atténuer les risques du déploiement de l'Internet des Objets, Alcatel-Lucent Enterprise (ALE) propose une stratégie de sécurité à plusieurs niveaux. Cette stratégie fournit une protection pour chaque couche de l'infrastructure, de l'utilisateur ou périphérique individuel à la couche réseau elle-même. ALE fournit également une stratégie de confinement de l'IoT pour simplifier et sécuriser l'intégration des appareils et offrir les bonnes ressources réseau pour faire fonctionner le système correctement et efficacement, le tout dans un environnement sécurisé pour protéger les organisations des cyberattaques.

Confinement de l'IoT

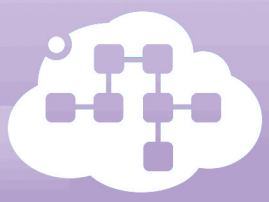
Pour permettre le confinement de l'IoT, tous les utilisateurs, équipements et applications au sein du réseau ALE reçoivent des profils. Ces derniers, qui définissent les rôles, les autorisations d'accès, les niveaux de qualité de service et autres informations sur les règles de sécurité sont relayés à tous les commutateurs et points d'accès dans le réseau.

- Les équipements sont placés dans des "conteneurs virtuels", en utilisant des techniques de virtualisation de réseau qui permettent à plusieurs appareils et réseaux d'utiliser la même infrastructure physique, tout en restant isolés du reste du réseau.
- Dans ces conteneurs virtuels, des règles de qualité de service et de sécurité sont appliquées.
- En séparant le réseau avec des conteneurs virtuels, si une violation se produit dans une partie du réseau virtuel, elle n'affecte pas les autres équipements ou applications dans d'autres réseaux virtuels.
- Lorsqu'un nouvel équipement IoT est connecté, le réseau reconnaît automatiquement son profil et affecte le périphérique à l'environnement virtuel approprié.
- La communication est limitée aux équipements du même environnement virtuel et à l'application au centre de données qui les contrôle.
- Comme tous les utilisateurs ont aussi des profils au sein du réseau ALE, l'accès aux conteneurs virtuels IoT peut être limité aux individus et groupes autorisés.

Sécurité approfondie

En plus du confinement IoT, les technologies de réseau d' ALE fournissent une sécurité multicouches sur plusieurs niveaux du réseau.

- Au niveau de l'utilisateur, les profils garantissent leur authentification, ainsi que l'accès avec les droits appropriés.
- Au niveau de l'équipement le réseau assure l'authentification des dispositifs et leur conformité aux règles de sécurité établies.
- Au niveau de l'application, le réseau peut établir des règles concernant chaque application ou groupe d'applications, comme bloquer, limiter la bande passante et contrôler qui peut accéder à quelle application.
- Au niveau du réseau, les commutateurs ALE bénéficient d'un code diversifié sécurisé. Ce logiciel protège les réseaux contre les vulnérabilités intrinsèques, les codes subvertis, les logiciels intégrés malveillants et les moyen d'accès détournés potentiels qui pourraient compromettre des commutateurs, des routeurs et autres composants de mission critique.
- Le système d'analyse intelligente d' ALE utilise l'inspection approfondie des paquets et d'autres technologies pour détecter le type des données et des applications se déplaçant à travers le réseau, ce qui permet d'identifier des modèles de trafic réseau inhabituels et les activités non autorisées.



Les équipements IoT présentent des risques pour les données transitant sur l'ensemble du réseau. En établissant des conteneurs via une segmentation de réseaux virtuels, les appareils IoT et les applications qui les contrôlent sont isolés, réduisant ainsi les menaces sans avoir le coût et la complexité de réseaux séparés.

Gestion intégrale de l'exploitation et du réseau

Les solutions réseau pour l'éducation d' ALE procurent également d'importants avantages opérationnels et de gestion.

- ALE permet à plusieurs réseaux virtuels distincts d'opérer comme une infrastructure unique commune, évitant les dépenses d'investissement (CAPEX) dans plusieurs infrastructures physiques.
- La solution ALE Unified Access permet à des technologies filaires et sans fil de cohabiter dans un réseau unique et robuste, à travers le partage des services réseau, du cadre réglementaire, du mode d'authentification; et l'unicité de la base de données pour l'authentification.
- Les solutions réseau d' ALE ont également un système de gestion unique pour tous les éléments de l'infrastructure, y compris la gestion unifiée à la fois du réseau LAN câblé et réseau WLAN sans fil. La suite de gestion d'Alcatel-Lucent OmniVista® 2500 fournit une fenêtre unique pour gérer les environnements virtuels, les commutateurs, les points d'accès et tous les autres composants du réseau.

Un portefeuille réseau à haute performance

Les commutateurs, points d'accès et les contrôleurs d' ALE supportent la dernière génération d'exigences en termes de bande passante élevée et de faible latence et gérent un grand nombre d'équipements dans des environnements à haute densité. Les produits et solutions réseau de ALE sont en mesure de répondre aux besoins en matière de réseau pour des organisations de toutes tailles. ALE propose également une sélection d' commutateurs robustes, points d'accès et routeurs pour les déploiements réseau en extérieur ou dans des environnements difficiles.

Les réseaux IoT sécurisés et les stratégies pour l'éducation sont disponibles aujourd'hui

Les produits et solutions d' ALE constituent une base sécurisée de réseau pour aider les écoles et les universités qui déploient des systèmes IoT à créer de nouvelles façons d'apprentissage pour les étudiants et de réalisation de cours et tests pour les enseignants. Les solutions IoT sécurisées aident également les administrateurs scolaires à simplifier les opérations et à fournir un environnement plus sûr aux étudiants et aux enseignants. Le confinement de l'IoT d' ALE et les stratégies de sécurité en couches réduisent les risques et simplifient la configuration des réseaux IoT en facilitant l'intégration des appareils, en fournissant un service opérationnel plus efficace et en augmentant considérablement la sécurité. ALE aide les organisations à profiter des avantages potentiels de l'IoT en fournissant des niveaux supérieurs d'intelligence de réseau, d'automatisation et de sécurité.

Voulez-vous en savoir plus?

Pour plus d'informations sur les solutions IoT d'ALE, rendez vous dans .ALE IoT Security.

Éducation connectée

Un environnement dans lequel l'éducation est connectée à l'aide de technologies efficaces. Pour votre école, établissement d'enseignement supérieur ou université. Grâce à notre envergure mondiale et à nos implantations locales , nous fournissons des solutions de réseau et de communication spécifiques pour les environnements de l'éducation qui permettent une collaboration sûre et fiable entre le corps enseignant et les étudiants.

1 University attacked by its own vending machines, smart light bulbs & 5,000 IoT devices
2 More Anti-Semitic Fliers Printed at Universities
3 Ex-Rutgers student pleads to cyberattacks, creating IoT botnet that brought down Internet
4 Michigan High School Student Facing Charges After launching DDoS attack on School Network