The Internet of Things in Education

Improve learning and teaching experiences by leveraging IoT on a secure foundation

Solution Brief
IoT in Education

Alcatel·Lucent Enterprise

IoT fundamentally changes the education equation

The Internet of Things (IoT) has the potential to transform education by profoundly altering how schools, colleges and universities gather data, interface with users and automate processes. IoT refers to the networking of physical objects through the use of embedded sensors, actuators and other devices that can collect and transmit information about real-time campus activity. When IoT is combined with technologies such as user mobility and data analytics, it brings a new paradigm in education. IoT enables institutions to:

- **Create new ways for students to learn** by supporting more personalized and dynamic learning experiences such as immersive digital textbooks and game-based learning.
- **Change how teachers deliver lessons and test achievement** with smart audio-visual equipment, digital video recorders for lecture capture, and online testing.
- **Simplify operations for school administrators** by proactively monitoring critical infrastructure and creating more efficient, cost-effective processes for HVAC, lighting and landscape management.
- **Provide a safer environment for students and teachers** with digital surveillance cameras, smart door locks and connected school buses.

IoT scenarios in education

IoT solutions promise to make schools and universities smarter as well as more successful at what they do. The IoT has the potential to redefine how students, teachers and administrators interact and connect to technology and devices in classroom environments, helping enhance learning experiences, improve educational outcomes and reduce costs. Examples of IoT solutions for education include:

- **Smart white boards and other interactive digital media** that can gather and analyze data for teachers and students for use in the classroom—or anywhere else, at any time—optimizing instruction and improving learning outcomes.
- **Solutions such as smart temperature sensors and smart heating, ventilation and air condition equipment** that reduce energy consumption and automate operations management.
- **Smart student ID cards, attendance-tracking devices, school bus tracking systems and parking sensors** that monitor the physical whereabouts of students.
- **Wireless door locks, connected surveillance cameras and facial recognition systems** that provide security for teachers, students and staff.
- **Research programs** enhanced with more advanced and automated systems in major areas of study, such as medicine, agriculture and engineering.

Challenges of IoT deployment

The IoT brings unprecedented flows of data, presenting performance, operational and management challenges to the network infrastructure along with increased security risks from all end-points. To address these issues, network administrators at educational institutions need to adapt traditional network designs to provide new levels of network intelligence, automation and security.

Schools and universities need a cost-effective network infrastructure that securely handles vast flows of data, but is also simple to manage and operate. The infrastructure must:

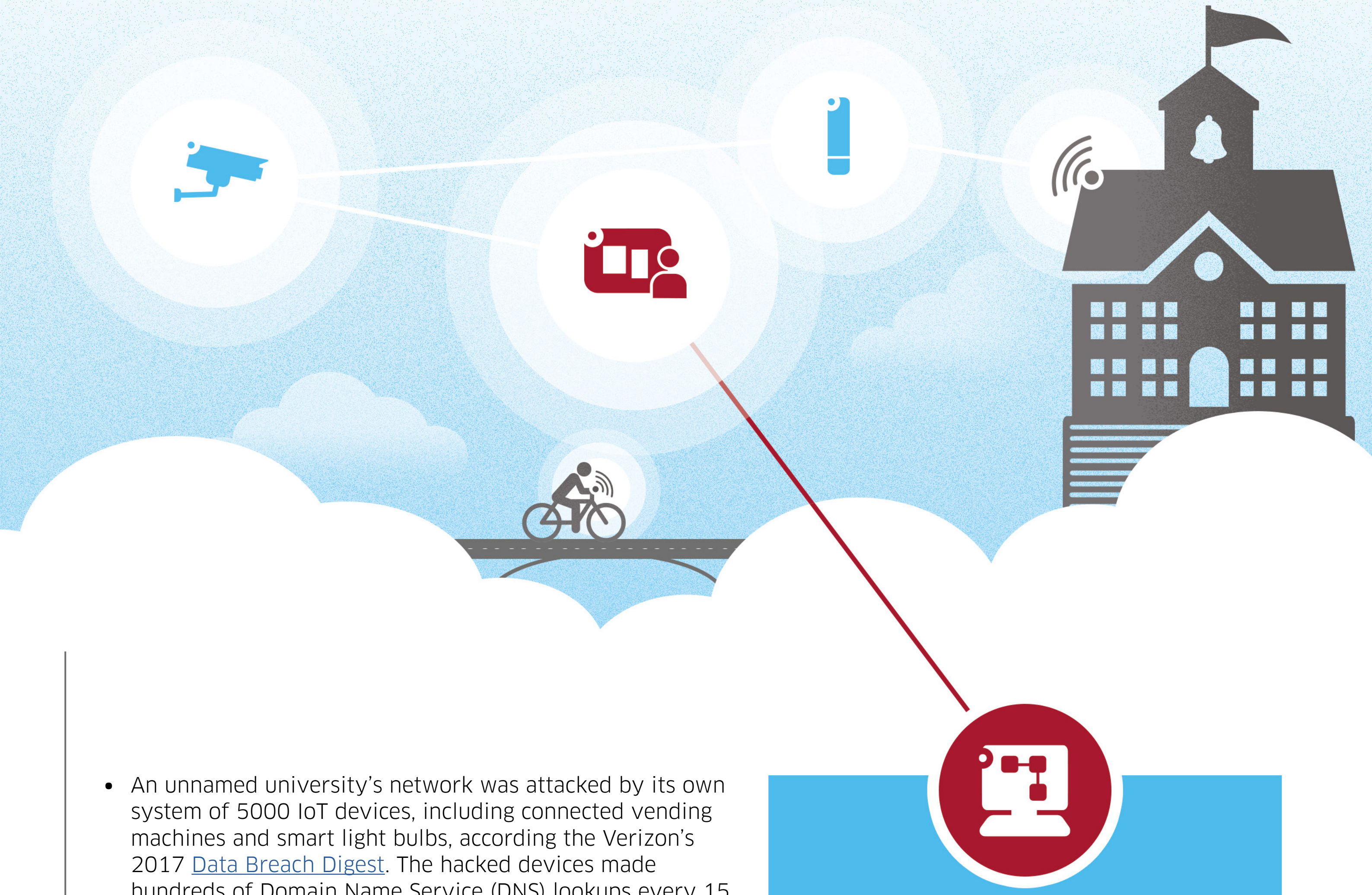
- **Provide a simple, automated process for IoT device onboarding.** Large IoT systems can contain thousands of devices or sensors, and manually provisioning and managing all of these endpoints is complex and error-prone. Automated onboarding enables the network infrastructure to dynamically recognize devices and assign them to the appropriate secured network.
- **Supply the correct network resources for the IoT system to run properly and efficiently.** Many devices in the IoT system deliver mission-critical information that requires a specific level of QoS. For example, some educational use cases require proper bandwidth reservations on a high performance network infrastructure to ensure service delivery and reliability.
- **Provide a secure environment against cyberattack and data loss.** Because the many networked devices and sensors in the IoT lead to a corresponding abundance of potential attack vectors, security is critical for mitigating risks of cybercrime. Security is necessary at multiple levels, including containment of the IoT networks themselves.

IT professionals are making plans for more IoT

IT professionals in a variety of industries are already planning for increased use of IoT solutions in the near future. According to the 451 Research survey 2017 Trends in the Internet of Things, 67 percent of responding IT professionals said their companies had either already deployed an IoT solution, or had an IoT system in pilot. Twenty-one percent of respondents said their companies planned to deploy IoT solutions within 12 months, with 11 percent claiming their companies' plans for implementing IoT were over a year away.

The IoT compounds schools' and universities' exposure to cyber crime

The growth of IoT in education also brings an explosion of cyber security threats, as the proliferation of sensors and connected devices greatly expands the network attack surface. IoT is especially susceptible because many IoT devices are manufactured without security in mind, or built by companies that don't understand current security requirements. Consequently, IoT systems are increasingly the weak link for network security in educational institutions.



- An unnamed university's network was attacked by its own system of 5000 IoT devices, including connected vending machines and smart light bulbs, according the Verizon's 2017 Data Breach Digest. The hacked devices made hundreds of Domain Name Service (DNS) lookups every 15 minutes, causing the university's network connectivity to become unbearably slow or even inaccessible.[1]
- White supremacists in 2017 hacked into networked printers and fax machines at a number of universities, including University of California, Berkeley, causing the machines to print out racist propaganda.[2]
- The Mirai botnet, which crippled internet service throughout the U.S. East Coast and a large swath of Western Europe by remotely enslaving millions of IoT devices, began as a 2016 attack on the computer network at Rutgers University. The Mirai software was designed to hijack poorly secured routers, security cameras and baby monitors.[3]

A Michigan high school student was caught in 2015 conducting a distributed denial of service attack (DDoS) that was designed to intermittently bring down the school's computing network. The botnet that caused the cyberattack targeted networked IoT devices such as surveillance cameras and routers.[4]

Building a secure IoT network infrastructure

Protecting IoT traffic and devices in school and university networks is a challenge that can't be solved by any single security technology. It requires a strategic approach that takes advantage of multiple security safeguards.

To help educational institutions take advantage of the benefits and mitigate the risks of IoT deployment, Alcatel-Lucent Enterprise (ALE) provides a multi-level security strategy. ALE's strategy delivers protection at every layer of the infrastructure, from the individual user and device out to the network layer itself. It also provides an IoT containment strategy to simplify and secure device onboarding and deliver the right network resources to run the system properly and efficiently, all in a secure environment to safeguard organizations from cyberattack.

IoT containment

To enable IoT containment, all users, devices and applications within the ALE network are assigned profiles. These profiles, which define roles, access authorizations, QoS levels and other policy information, are relayed to all switches and access points in the network.

- Devices are placed in "virtual containers," using network virtualization techniques that allow multiple devices and networks to use the same physical infrastructure, while remaining isolated from the rest of the network.
- In these virtual containers, QoS and security rules are applied.
- By segregating the network with virtual containers, if a breach does occur in one part of the virtual network, it does not affect other devices or applications in other virtual networks.
- When a new IoT device is connected, the network automatically recognizes its profile and assigns the device to the appropriate virtual environment.
- Communication is limited to the devices within that virtual environment and to the application in the data center that controls these devices.
- Because all users also have profiles within the ALE network, access to the IoT virtual containers can be limited to authorized individuals and groups.

In-depth security

In addition to IoT containment, ALE networking technologies provide layered security across multiple levels of the network.

- At the user level, profiles ensure users are authenticated and authorized with the appropriate access rights.
- At the device level, the network ensures that devices are authenticated and compliant with established security rules.
- At the application level, the network can establish rules regarding each application or group of applications, including blocking, limiting bandwidth and controlling who can access which application.
- At the network level, ALE switches benefit from CodeGuardian™. It protects networks from intrinsic vulnerabilities, code exploits, embedded malware and potential back doors that could compromise switches, routers and other mission-critical hardware.
- ALE smart analytics use deep packet inspection and other technologies to detect the type of data and applications moving through the network, making it possible to identify unusual network traffic patterns and unauthorized activity.

IoT devices pose risks to assets across the entire network. By establishing containers via virtual network segmentation, IoT devices and the applications that control them are isolated, thereby reducing threats without the cost or complexity of separate networks.

End-to-end operational and network management

ALE network solutions for education also provide significant operational and management advantages.

- **ALE enables multiple separate virtual networks to operate on a single infrastructure,** saving CAPEX investment in multiple physical networks.
- **The ALE Unified Access solution allows wired and wireless technologies to work together** as a single, robust network, with a common set of network services, a policy framework, a common authentication scheme and a single authentication database.
- **ALE networking solutions also have a single management system for all elements of the infrastructure,** including unified management of both wired LAN and wireless WLAN networks. The Alcatel-Lucent OmniVista® 2500 management suite provides a single pane of glass to manage virtual environments, switches, access points and all other components of the network.

A high performance network portfolio

ALE switches, access points and controllers support the latest generation of high bandwidth and low latency capabilities and can manage large numbers of devices in high-density environments. ALE networking products and solutions are able to address the networking needs for educational institutions of all sizes. ALE also provides a selection of ruggedized switches, access points and routers for network deployments outdoors or in harsh environments.

Secure IoT networks and strategies for education are here today

ALE products and solutions build a secure network foundation to help schools and universities deploy IoT systems that can create new ways for students to learn and improve how teachers deliver lessons and test achievement. Secure IoT solutions also help simplify operations for school administrators and provide a safer environment for students and teachers. ALE's IoT containment and layered security strategies reduce the risks and simplify the setup of IoT networks by easing device onboarding, providing more efficient operations and greatly increasing security. ALE helps organizations unlock the full potential benefits of IoT by providing enhanced levels of network intelligence, automation and security.

Want to learn more?

For more information about ALE's IoT solutions, go to ALE IoT Security.

Connected Education

Where Education connects with technology that works. For your school, college or university. With global reach and local focus, we deliver purpose built networking and communications for the education environment that enable secure, reliable collaboration between your faculty and students.

ALE | Where Everything Connects

[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