GlobalLogic®

Infrastructure Security Considerations for Edge Computing

Authored by: Umesh Kanyal
Co-Authors: Sachin Kumar & Aditya Aggarwal

Contents

Introduction

With the rapid development in technology, new security and privacy challenges always need to be considered. Businesses should aim to build a secure infrastructure that involves several pieces of hardware because each piece either processes or transmits sensitive data. Hardware security plays an important role in ensuring confidence and integrity. Nowadays, many enterprises are adopting IoT concepts, and information security is a top concern.

IoT encourages the use of Bluetooth low energy-enabled devices (BLE), which are controlled remotely from a smartphone or tablet. Ultimately, we will see BLE infrastructure with a number of devices connected to each other using Bluetooth, wired, or wireless mediums. Security is essential for these hardware devices during data transmission.

Reader-Enabled Access Infrastructure

Reader-enabled access infrastructure connects hardware and establishes a connection between a user, hardware, services, and applications to enable computing and communication. The infrastructure we are considering here deals with hardware like a reader, gateway, or event processor that connects using Bluetooth to exchange information between devices and the cloud.

Reader-Enabled Smart Infrastructure

- Secure identity products: smart lock and smart elevator
- Equipment: reader and event processor
- Smartphone: initiates door unlock request

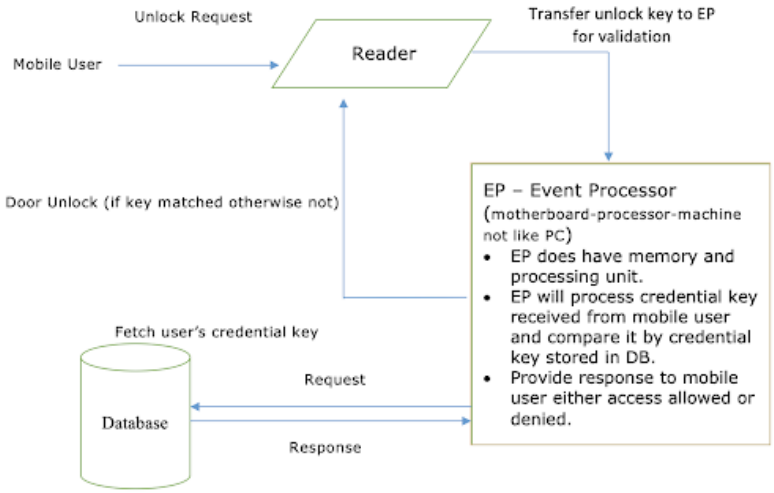
Security is vital when data transmission takes place between various BLE hardware and the cloud. Below are two important pieces of hardware that actually process the door unlock request and perform the corresponding actions.

Reader: Takes and forwards the request but doesn't have processing capabilities. It receives the door unlock request from a smartphone or access card and sends the same message to the event processor (EP) for actual processing. Based on the decision made by the EP, the reader either grants or denies access.

Event Processor: This does the actual processing by fetching the credential key from the user request (forwarded by the reader) and compares it with the credential key created from data stored in the server. If both keys match, the reader responds with access granted or denied.

The steps below describe the flow of request and response.

- The application installed on a smartphone creates a key using the login user's credentials. This key is used to identify the request.
- Makes a door unlock request using the key created in the step above. That request is received by a reader.
- A reader forwards it to the EP for processing and validation. The EP responds to the reader by processing and analyzing whether the user is valid or not and authorizes/denies access to the requested door.
- The reader receives the EP response and performs the action of unlocking the door or denying access.



Smart lock-enabled infrastructure

The Need for Hardware Security

The flowchart of door unlock requests and the role of hardware used in infrastructure is clarified in the discussion above. However, another important aspect is to secure the hardware used. The flowchart clarifies that if during any step data is tampered with, distorted, or hacked, the hardware will have a malfunction or perform unexpectedly.

The security needs for every piece of hardware used in each step:

- The smartphone and each application installed need to be secure enough so any intruder or malicious code can't use login credentials to create a request key.
- The reader hardware must be secure enough so requests received can be forwarded as-is to the EP. If they are tampered with, requests may be changed for any other door, and the EP will grant access.
- Data must be secure enough in the transmission medium used between pieces of hardware.

Smart Phone <----------> Reader <----------> EP

Data can only be secured if the hardware that stores and processes data is secure. Below are a few ways to make hardware secure:

- For physical-level protection from theft and tampering, we can use Encrypting File System (EFS) to encrypt the files on the disk.
- Security threats from malicious code like viruses, worms, etc., can be tackled using software that blocks malicious code and unauthorized access.
- We can use security like biometric identification, secure key storage, and functional design specification (compression, encryption, or pattern recognition).

How Can Edge Computing Lead Hardware Security in Reader-Enabled Smart Access Infrastructure?

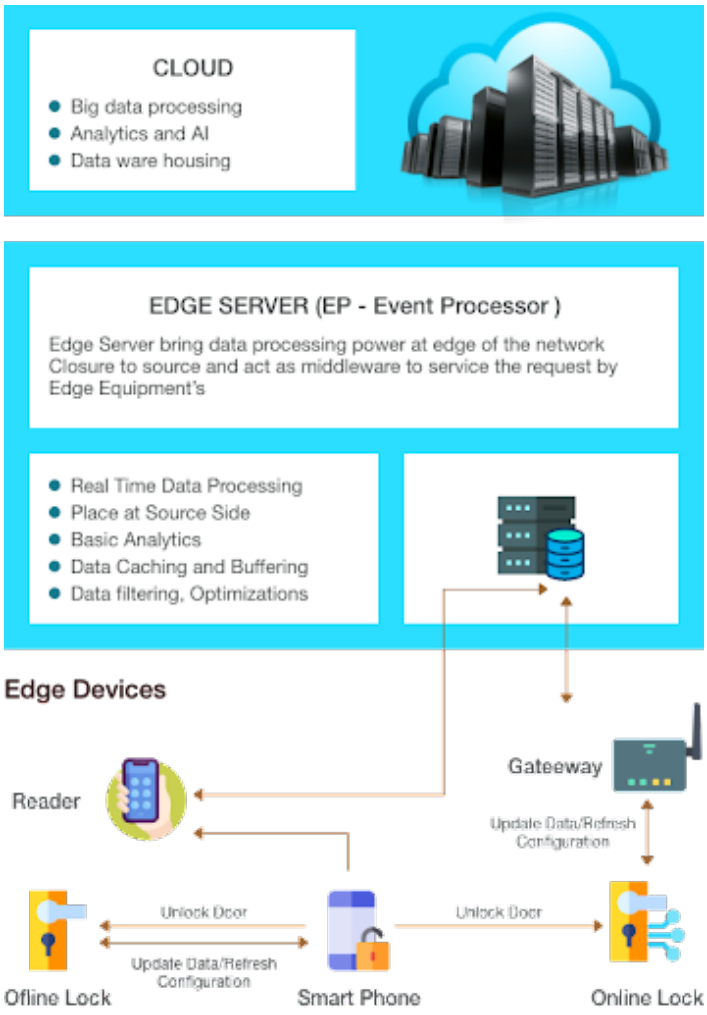
Introduction to Edge Technology

Data for any organization or firm is stored in the cloud where analytics, AI activities, and processing can be performed and data can be retrieved whenever required. In reality, all that data comes from the physical environment where we work, create data, and interact with various pieces of equipment. We perform tasks in industries like health, security, business, and education, and in locations such as factories, buildings, homes, and vehicles like trains, planes, and private cars. 5G opens up the opportunity for us to communicate on the premises where work is performed: in the factory, distribution center, warehouse, retail store, bank, hotel, etc.

Edge computing places workloads in computation and data storage as close to the edge devices where the data is being created or needed and actions are being performed. It improves the way businesses collect and analyze their data by processing information near to the source as opposed to in the cloud. It provides real-time information, which allows companies to make data-driven decisions.

The event processor acts like an edge server, and devices like the reader and gateway act as edge devices in smart lock infrastructure. Edge computing will be beneficial if data is created and processed locally, so the infrastructure we are considering here also deals with a user's data at a particular company. That data will be created and manipulated locally, so placing an edge server (EP) with frequently used and sensitive data can play a crucial role if placed in between the company and the cloud.

Infrastructure Using Edge Computing

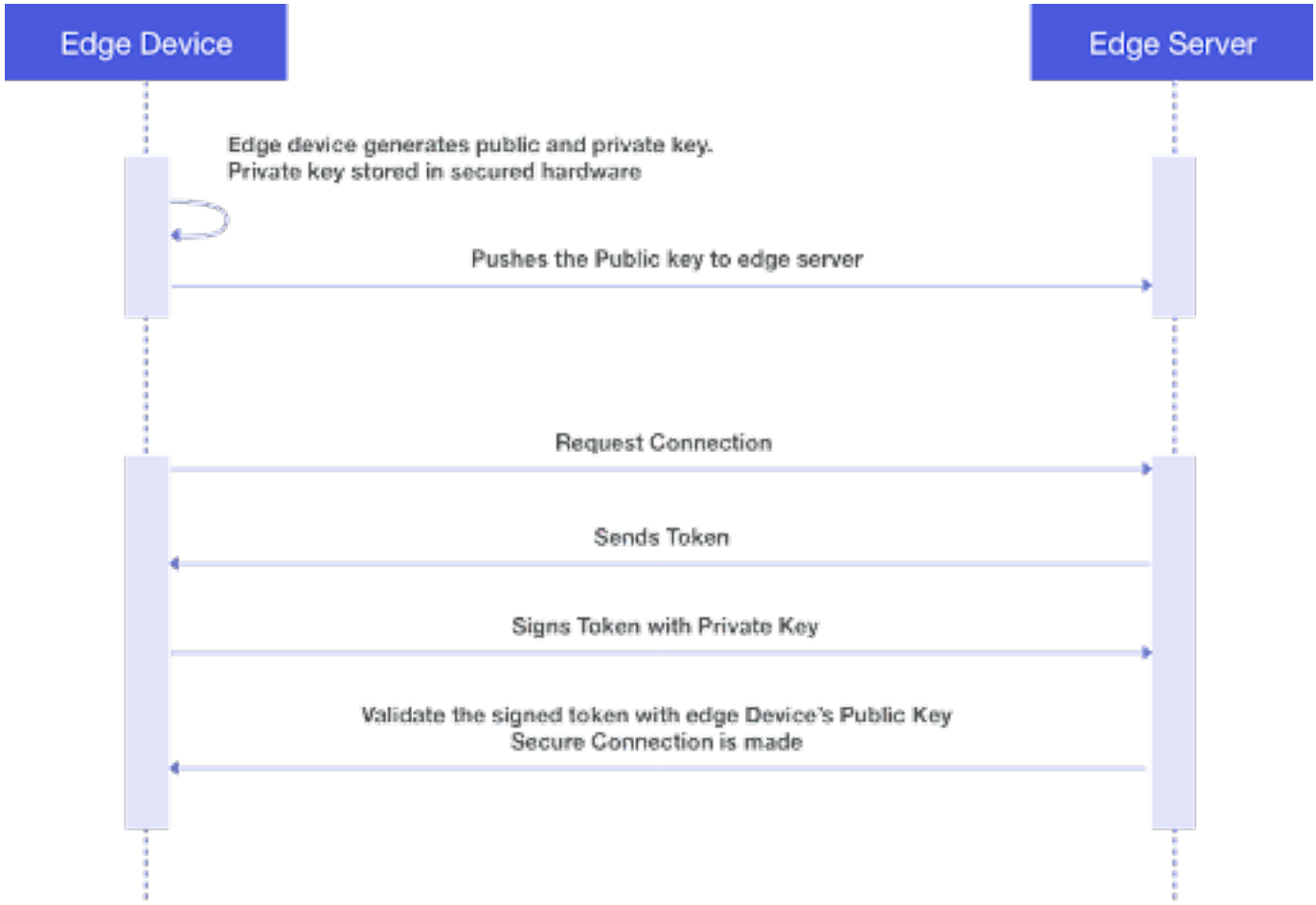


Proposed Solutions for Edge Computing Security

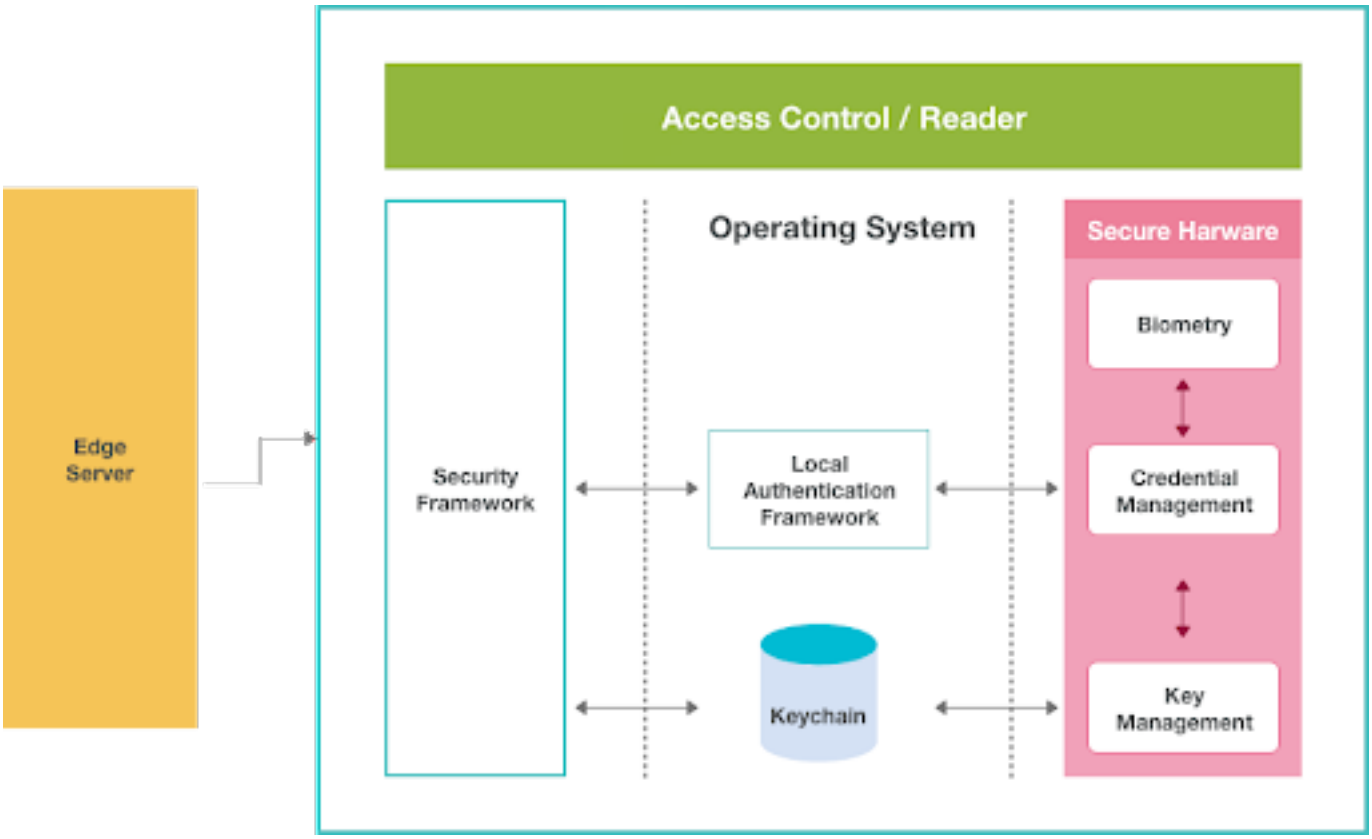
Device capabilities: Edge computing aims to improve the capabilities of edge devices by involving processing, security, and intelligence. Existing infrastructure can be enhanced by making the reader capable of processing the user's door unlock request itself and not dependent on the event processor.

Encryption technique: In edge computing, a user request transmits to the edge server via the reader. This data transmission can be vulnerable because the information is exposed, and attackers or intruders can manipulate the instructions by tampering with the data. To make data transmission secure, data can be sent in the form of ciphertext by applying cryptography techniques.

Secure Hardware: To make existing hardware more secure, additional hardware can be introduced for storage or computation. Nowadays, hardware like Secure Enclave for iOS-specific OS and KeyStore for Android OS are available. This secure hardware also uses encryption techniques to store data in encrypted form, which makes it secure. Even if the device is cloned, the keys stored in this new hardware cannot be cloned or tampered with, which makes it more secure.



Connection establishment between reader and edge



Reader architecture incorporating additional security hardware

Challenges to Proposed Solutions for Edge Computing Security

Building a reader capable of processing user requests for unlocking doors is expensive. Likewise, pushing intelligence, processing power, communication capabilities, and artificial intelligence to edge devices will definitely have cost implications. The cost of micros has continued to fall while their capabilities have significantly increased. They are still more expensive than cheaper microcontrollers, making low-end micros more desirable for mass-produced devices.

Introducing additional hardware for secure storage or computing will increase the cost and coordination with existing hardware. Because communication with existing hardware is a requirement and needs a bridge, firmware can act like a bridge here, but implementation would be challenging.

Conclusion

Edge computing in conjunction with infrastructure security is a great help. Edge devices cannot make direct connection to the cloud every time for their operational activities due to many reasons: latency, internet connectivity, etc.

Edge devices like access readers need to respond in milliseconds. They require processing near the device and do not rely on the internet, which is made possible with edge computing. Since edge devices are not directly connected to the internet, they are secure. Edge servers can update themselves when required and facilitate edge devices as per their offline needs.

About the Authors

Umesh Kanyal

Over 16+ years of experience in Microsoft Technologies that includes Windows, Web and Mobile Platforms. Has hands-on and led various projects on all the platforms. Currently working on security domain and mobile platform that mainly targets IoT using Edge Computing.

Aditya Aggarwal

Detailed-oriented, accountable, and committed engineer with around 10 years of experience in designing and building applications for iOS platform.Strong understanding of the patterns and practices ensuring the performance, quality and responsiveness of applications.

Sachin Kumar

Software professional with 7+ years of hands-on experience in software development, design, project management and change management. Proficient with Microsoft technologies like ASP.NET/C# .NET, Web API, Xamarin, WPF and Well versed with software development life cycle and agile methodology.

GlobalLogic®

GlobalLogic, a Hitachi Group Company, is a leader in digital product engineering. We help our clients design and build innovative products, platforms, and digital experiences for the modern world. By integrating our strategic design, complex engineering, and vertical industry expertise with Hitachi's Operating Technology and Information Technology capabilities, we help our clients imagine what's possible and accelerate their transition into tomorrow's digital businesses. Headquartered in Silicon Valley, GlobalLogic operates design studios and engineering centers around the world, extending our deep expertise to customers in the automotive, communications, financial services, healthcare & life sciences, media and entertainment, manufacturing, semiconductor, and technology industries.



www.globallogic.com