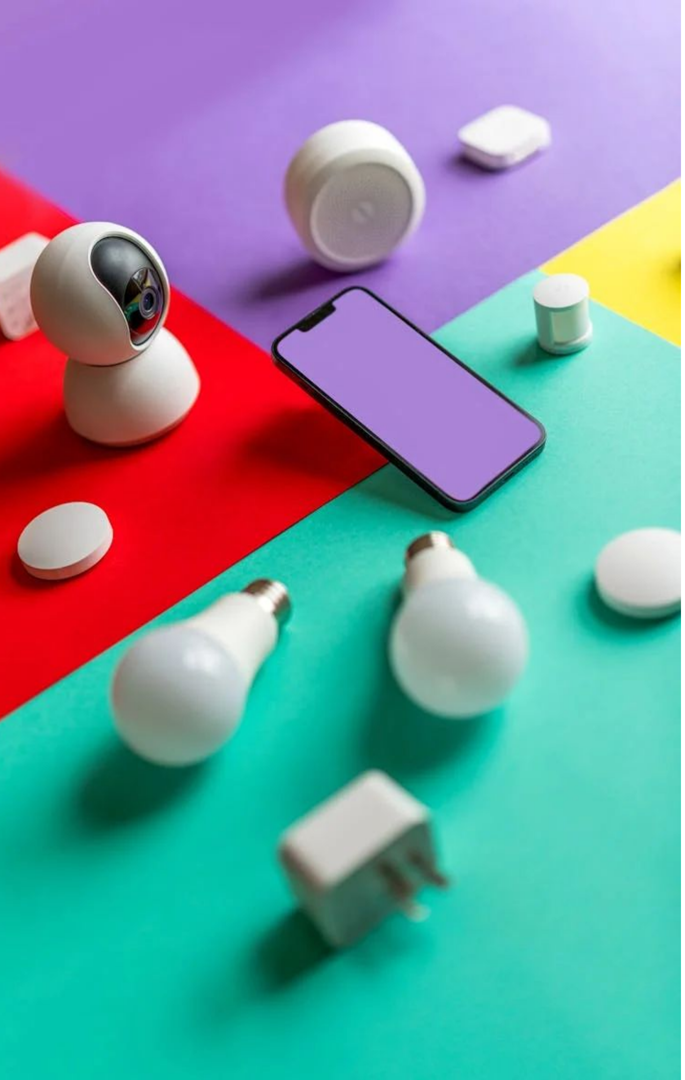


Sustainable Smart Home

Sustainable Smart Homes: Leveraging AWS and Azure for IoT device automations

Karimah Ayinde-Usman

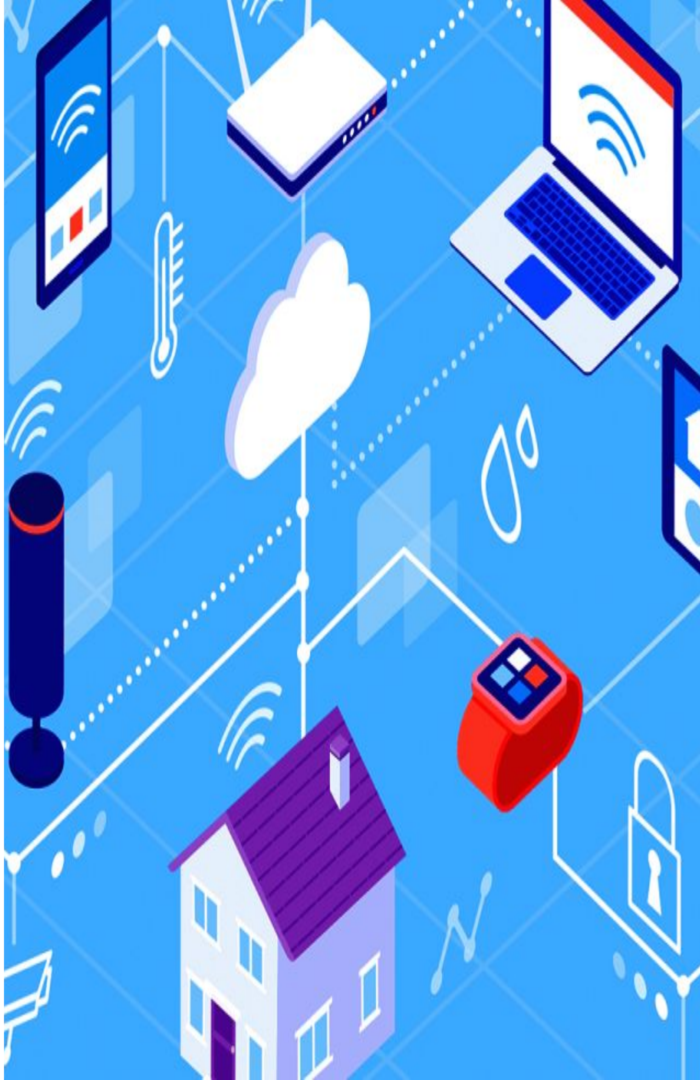
BRIEF

Design a smart home system that optimises energy usage and integrates seamlessly with your lifestyle.

Utilise different cloud platforms (e.g., AWS for data storage, Azure for machine learning for energy prediction) to achieve specific functionalities.

Focus on scalability as you add more smart devices.

Implement features like automated lighting control based on occupancy or solar power availability



MY INTERPRETATION OF THE BRIEF

The solution will be:

1. For controlling internet-enabled devices from anywhere (via an app) - devices include light switches, appliances, thermostats, doorbells, door locks, plugs
2. Multi-cloud so requires connectivity between at least 2 cloud providers
3. Must be scalable, enabling the addition of more smart devices in the future
4. Optimised using a machine learning solution
5. Scalable and cost optimised to prevent overspending in the cloud
6. Monitored for opportunities to: improve performance, reduce costs, improve security posture

Whilst this is not a corporate solution, we must still address security. A key security risk that needs to mitigated is **availability**, ensuring users are always able access the devices that they use in day to day life. For example, using the smart locks attached to doors. Similarly, ensuring that all users are authenticated and authorised to perform actions to prevent unauthorised access.

THREAT MODEL

Before designing I conducted a threat model to identify threats to mitigate, using STRIDE since it is a relatively simple cloud solution.

Spoofing (S)

- Threat: An unauthorised device impersonating a genuine smart home device to control the smart home components
- Mitigation: using IoT Core to authenticate devices since it uses mutual authentication, IAM policies and device certificates

Tampering (T)

- Threat: An attacker making changes to the data sent from the smart devices, leading to incorrect data being analysed by the machine learning model
- Mitigation: sending data using secure comms protocols to prevent man in the middle attacks and ensuring that data is encrypted at rest

Repudiation (R)

- Threat: A user being able to deny taking a specific action within the smart home cloud solution, impacting device control
- Mitigation: Ensuring that robust logging and monitoring capabilities are in place for monitoring user activity, that are tamper proof and centralised

Information Disclosure (I)

- Threat: An unauthorised user gaining access to the energy consumption patterns or details about the devices
- Mitigation: make use of IAM policies/access controls to implement RBAC, restricting access to data in line with roles

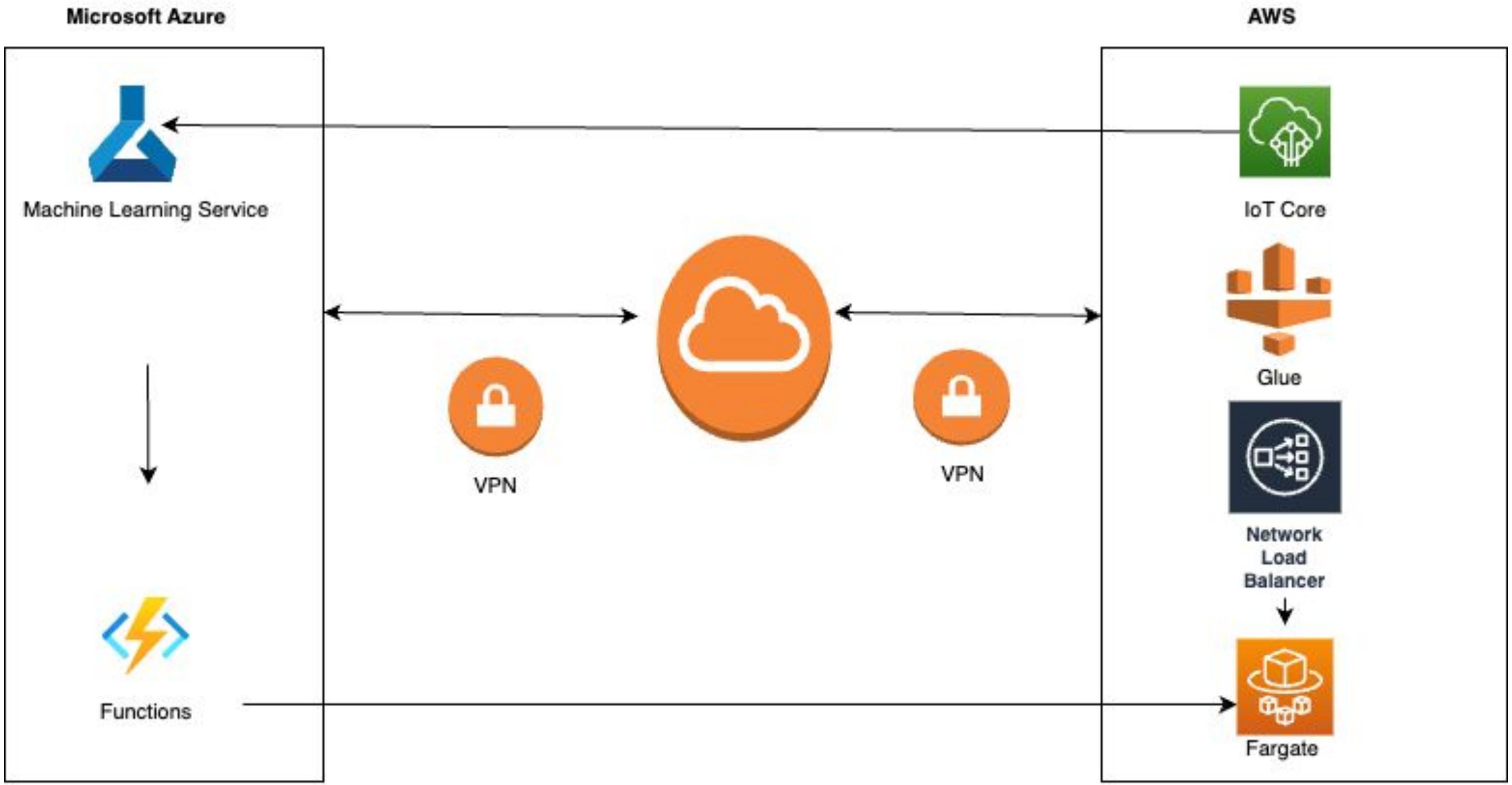
Denial of Service (D)

- Threat: An attack that causes the smart home solution to be unavailable to genuine users
- Mitigation: implementing IDS/IPS systems to block suspicious traffic

Elevation of Privilege (E)

- Threat: An attacker gaining access to the smart solution and elevating their access, subsequently gaining unauthorised access to data.
- Mitigation: use identity and access management mechanisms within AWS and Azure to enforce granular access control. Avoiding root accounts for day-to-day use and account hardening.

HIGH LEVEL DESIGN



DESIGN EXPLANATION

The brief specified that multiple cloud vendors were in use, so I chose Microsoft Azure and AWS.When designing this solution, I opted for serverless/managed solutions to reduce the overhead required for managing the solution.

DESIGN CHOICES

AWS IoT Core: smart devices will be securely onboarded and maintained through IoT Core. Receiving control commands from Fargate and sending such commands to the registered devices.

AWS Glue: Sensor data will need to be transformed before being placed in the machine learning model (Azure), to save on data transfer costs, this will be completed via AWS Glue.

Azure Machine Learning (AML): The chosen solution for creating the machine learning model that will control lighting by receiving real-time sensor data from AWS IoT core deployed as a web service (AWS). Predictions of whether the light should be on/off can be made based on occupancy (binary algorithm) or solar power availability (regression algorithm).

Azure Functions: Once AML has defined the light predictions, it will use Azure Functions to process the data and send control commands for devices to AWS.

AWS Fargate: Will receive control commands for actions to be taken on IoT devices, fargate will be used to reduce the maintenance of compute and achieve scalability if the device estate increases substantially, with little overhead to the administrator.

Site-to-Site VPN: since the solution is for a household rather than a corporation (low bandwidth), a site-to-site VPN would provide a secure means of data transfer over the internet whilst minimising costs (compared to a private, dedicated connection like Direct Connect). It is also relatively quick to setup, though it is imperative that secure encryption protocols are used i.e. AES-256 to ensure data is secure. Additionally, digital certificates will be used instead of pre-shared keys.

DESIGN FOR SECURITY

To address security within this solution:

- **Configuration of Home WiFi Network** - hardening the home router by changing default login credentials, turning on firewalls, using strong passwords, verifying all connections, etc.
- **Device Maintenance** - ensuring that the smart devices are patched in a timely manner and unsupported devices are avoided where possible, to ensure devices are secure.
- **Security Patching** - ensure that all cloud components are patched on a regular schedule
- **Identity and Access Management -** ensuring that policies are created to allow access between services instead of hard coding credentials and ensuring all devices are authenticated before allowing connection.
- **Encryption -** ensuring that Secure Communication Protocols are used for comms between devices and data is encrypted at rest.
- **Logging and Monitoring** - to maintain an audit trail of actions taken within the cloud environment
- **User Education** - teaching users about the best practice for securing smart devices such as strong passwords, purchasing from reputable suppliers and choosing devices with support available.
- **Cloud Governance** - Across AWS and Azure there will be monitoring in place to ensure that the solution is aligned with best practice (AWS Trusted Advisor & Azure Monitor)
- **Leverage built-in security functionality** - ensuring the security features in the cloud services are being used, for example encryption on S3

CONTINUOUS IMPROVEMENT

Over time, I will aim to improve this cloud deployment. Since it is a home-scale cloud deployment I will focus on cost, automation and security improvements.

Cost

- Seeking opportunities to ‘right size’ resources by using AWS CloudWatch/Azure Monitor to evaluate the resource usage and adjust as needed to make cost savings.
- Implement a data retention policy to ensure that data is only retained for a necessary duration, saving on storage costs.

Automation

- In the long run using Terraform (IaC) for the provisioning and management of infrastructure, allowing both AWS and Azure to benefit from automation, compared to using CloudFormation (AWS only).

Security

- Monitoring AWS Trusted Advisor and Azure Advisor on an ongoing basis for areas of improvement and advisory for improving performance of the solution.

THANK YOU

Thank you for your time, I would love to hear your feedback on my work.

Please feel free to contact me to discuss further.

Karimah Ayinde-Usman
karimahayinde97@gmail.com