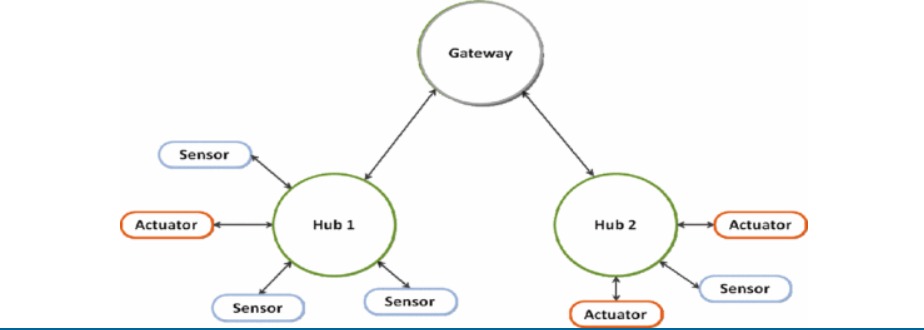
sResearch Papers.

1. Networking Layer for Unifying Distributed Smart Home Entities



* It mentions the concept of a global network level (GNL) and the need to unify intermediaries (hubs, gateways, etc.) in home automation systems to avoid protocol conversions.
* The paper discusses the use of MQTT protocol, which allows for the creation of connections between brokers and the establishment of a GNL for information distribution without protocol conversions.
* It also mentions the possibility of using bridge configurations to pass information between different broker instances in order to create the aimed GNL
* Discusses and analyses AMQP, CoAP, XMPP, MQTT….

For the constrained environment in home automation systems, particularly for endpoint entities, MQTT and CoAP are more suitable than AMQP and XMPP. Very important fact, confirmed with the most common applications, is that MQTT and CoAP are from start made for embedded devices. AMQP and XMPP are made for the applications and it is hard to find library which won’t be an overhead for home automation entities.

1. Smart Home：Architecture, Technologies and Systems

* The communication between home appliances within the internal network can be wired or wireless, using protocols such as Ethernet, Wi-Fi, or Zigbee.
* The home gateway acts as a bridge between the internal network and the external network, and it may use protocols like TCP/IP or MQTT for communication.
* The home gateway acts as a bridge between the internal network and the external network, and it may use protocols like TCP/IP or MQTT for communication.
* Additionally, protocols like HTTP or HTTPS may be used for communication between the intelligent interactive terminal and the smart home system.

1. A REVIEW ON SOFTWARE-DEFINED NETWORKING ENABLED IOT CLOUD COMPUTING

* Software-Defined Networking (SDN) is the network architecture used in this research paper. SDN is a novel approach that separates the Data Plane and the Control Plane, allowing for programmable networks and easier network management.
* The SDN architecture consists of multiple layers: Physical Layer: This layer includes the infrastructure used in the network, such as switches and routers. Control Layer: The SDN controller resides in this layer and provides various network services and provisioning. Application Layer: This is the topmost layer of the SDN architecture and includes applications like firewalls and load balancers.
* The protocols used in SDN include: OpenFlow: A Southbound API protocol supported by Mininet switches for communication and custom routing. REST: A Northbound API protocol used for communication between different layers of the SDN architecture.

1. A review on smart home present state and challenges: linked to context-awareness internet of things (IoT)

* Researchers have proposed frameworks based on web services and SOAP to exchange messages and manage interoperation among heterogeneous smart home devices. SOAP is part of the foundation for web services and plays a significant role in enabling communication between distributed systems on the web.
* An extensible smart home gateway architecture based on the OSGi framework allows seamless integration of heterogeneous devices and protocols during runtime.
* Different frameworks support various architectural styles, such as distributed, centralized, and layered.
* Security and privacy features are supported in some frameworks, with local access control involved in each context manager to analyze contexts against user privacy settings.

1. A Comprehensive Review of IoT Networking Technologies for Smart Home Automation Applications

* Wired technologies such as BACnet, Bluetooth, Dupline, Ethernet, KNX, LonWorks, Wi-Fi, and X10 have been available to consumers for over 20 years and are popular in building automation.
* Wireless technologies include 802.15.4-based technologies (6LowPAN, Thread, and Zigbee), Dash7, EnOcean, LoRa, NB-IoT, mioty, Sigfox, Wi-Fi (802.11ah), and Z-Wave.
* Dual mode technologies combine both wired and wireless connectivity options, providing flexibility in smart home automation applications.
* The communication protocols used in these technologies vary. Most technologies support TCP/IP, which is important for data exchange between different technologies

1. Review and Performance Analysis on Wireless Smart Home and Home Automation using IoT

* The network architecture used in the paper involves the use of mobiles or computers to control the basic home appliances through a designed web page with internet connection/local area network (LAN) servers.
* The proposed system enables the operation of the home automation system from anywhere around the world using the internet.
* The system utilizes Wi-Fi for wireless connectivity, allowing for long ranges over wireless local area connections and an infinite range over the cloud.
* The Wi-Fi module is used to send/receive data over the internet, provided that proper database and domain infrastructure is available.
* It enables the seamless connection of devices to the local area network (LAN) and allows for remote control and monitoring of appliances through the designed web page.
* While the sources do not explicitly mention other protocols, it is possible that other protocols such as Bluetooth or GSM may also be used for specific functionalities within the system.

1. IoT Threat Detection Advances, Challenges and Future Directions.

Network Architectures Used in IoT Threat Detection:

* Fog Computing IoT Architecture - Fog computing is utilized in IoT architectures for early detection and mitigation of attacks. It allows detection of attacks at the fog node and subsequently at the edge node, providing lower storage constraints, cheaper computation, and low latency.
* Edge Computing Architecture
* Cloud and Fog Based Architectures
* Cloud-Fog-Edge Architecture
* Mist Computing Architecture
* S-IoT (Social IoT) Architecture
* IoT-A Architecture
* These are some of the network architectures proposed by researchers for IoT threat detection. Each architecture has its own unique features and advantages in handling intrusion detection in IoT networks. The use of SDN (Software-Defined Networking) network architecture is also gaining popularity in IoT threat detection, as it provides a centralized view of the entire network, making it easier for administrators to defend against cyber threats