What do you think about this topics , should i do them or i leave if for blockchain guy

Cryptography

- ***Data confidentiality***
- ***Data Integrity***
- ***Authentication***
- ***Non-repudiation***

Hardware attacks

Virus Cyber attacks

Phishing attacks

Channel attacks

Software bugs

Holes in operating systems

Advanced persistent threats

Key IoT application domains in Cyber Security and Privacy

The networking of biomedical instruments and databases in hospitals has the potential to dramatically improve the quantity and availability of diagnostic and treatment decisions. It also has substantial implications for rural and remote clinics, providing ready access to specialist opinions. Extending medical instrumentation to the home has improved quality of life and reduced hospital readmissions.The last two decades have seen a surge in the use of electronics in automobiles, based on dozens of networked microprocessors . The next stage of development will be communication between vehicles, and between vehicles and infrastructure. Standardization, security and cost are major drivers. Transport and Logistics are already heavy users of RFID tags for the tracking of shipments, pallets and even individual items. The research direction here is into smart tags which can log and report transport conditions such as shock, tilt, temperature, humidity and pressure. Here the key driver is low cost, as well as orderly communication to hundreds or thousands of tags simultaneously. IoT technology is having disruptive impacts on a very broad range of industries including entertainment, dining, public transport, sport and fitness, telecommunications, manufacturing, hotels, education, environmental science, robotics, and retail. In many of these industries, IoT is becoming a key enabler of innovation and success, and industries are willing to invest in new technologies. Specialist IT support can be provided on staff or from external providers to ensure that the security and availability of their systems is sufficient for their business needs. While there are some reasonably widespread specialized Smart Home standards, such as X.10 power line-carrier communications, these lack any type of security, and were designed before these home control networks were connected to the Internet. There are now a plethora of networking standards that can be used in a home (Zwave, Insteon, Bluetooth, Zigbee, Ethernet, Wififi, RS232, RS485, C-bus, UPB, KNX, EnOcean, Thread). Each has its strengths and weaknesses, and expecting a heterogeneous network with many different protocols to be efficiently and securely managed by a non-expert presents significant challenges.

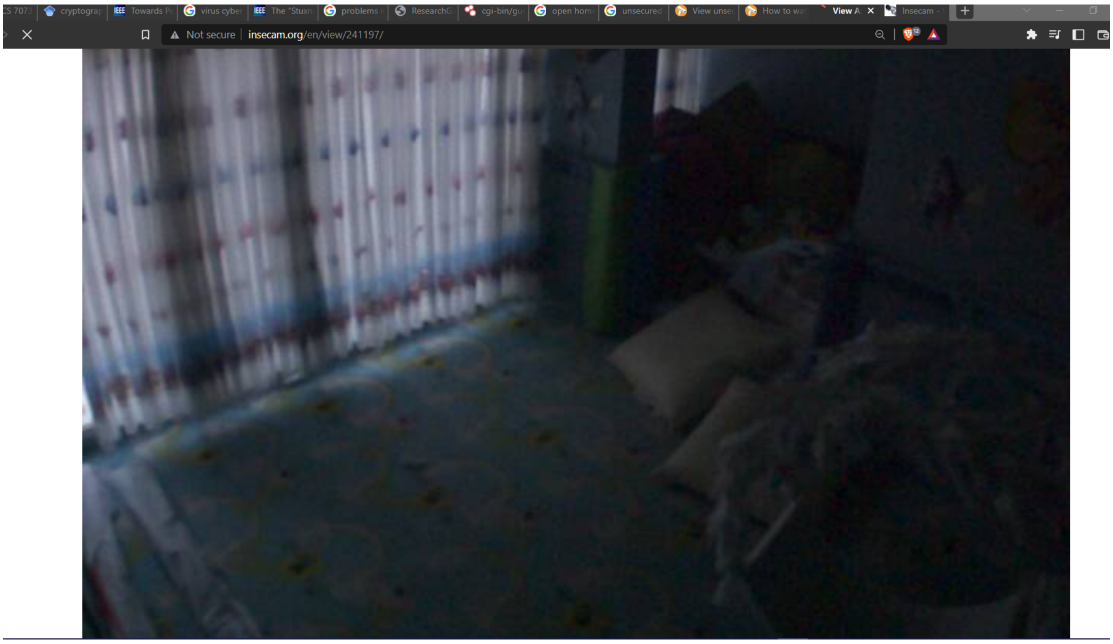
The Smart Home potentially provides additional comfort and security, as well as enhanced ecological sustainability. For example, a smart air conditioning system can use a wide variety of household sensors and web-based data sources to make intelligent operating decisions, rather than simple manual or fixed-schedule control schemes. The smart air conditioning system can predict the expected house occupancy by tracking location data to ensure the air conditioner achieves the desired comfort level when the house is occupied and saves energy when it is not. In addition to enhanced comfort, the Smart Home can assist with independent living for the aging.
The Smart Home can assist with daily tasks such as cleaning, cooking, shopping and laundry. Low level cognitive decline can be supported with intelligent home systems to provide timely reminders for medication. Home health monitoring can signal caregivers to respond before expensive and disruptive hospitalization is needed. However, none of these benefits is likely to be taken up if the Smart Home system is not secure and trusted.

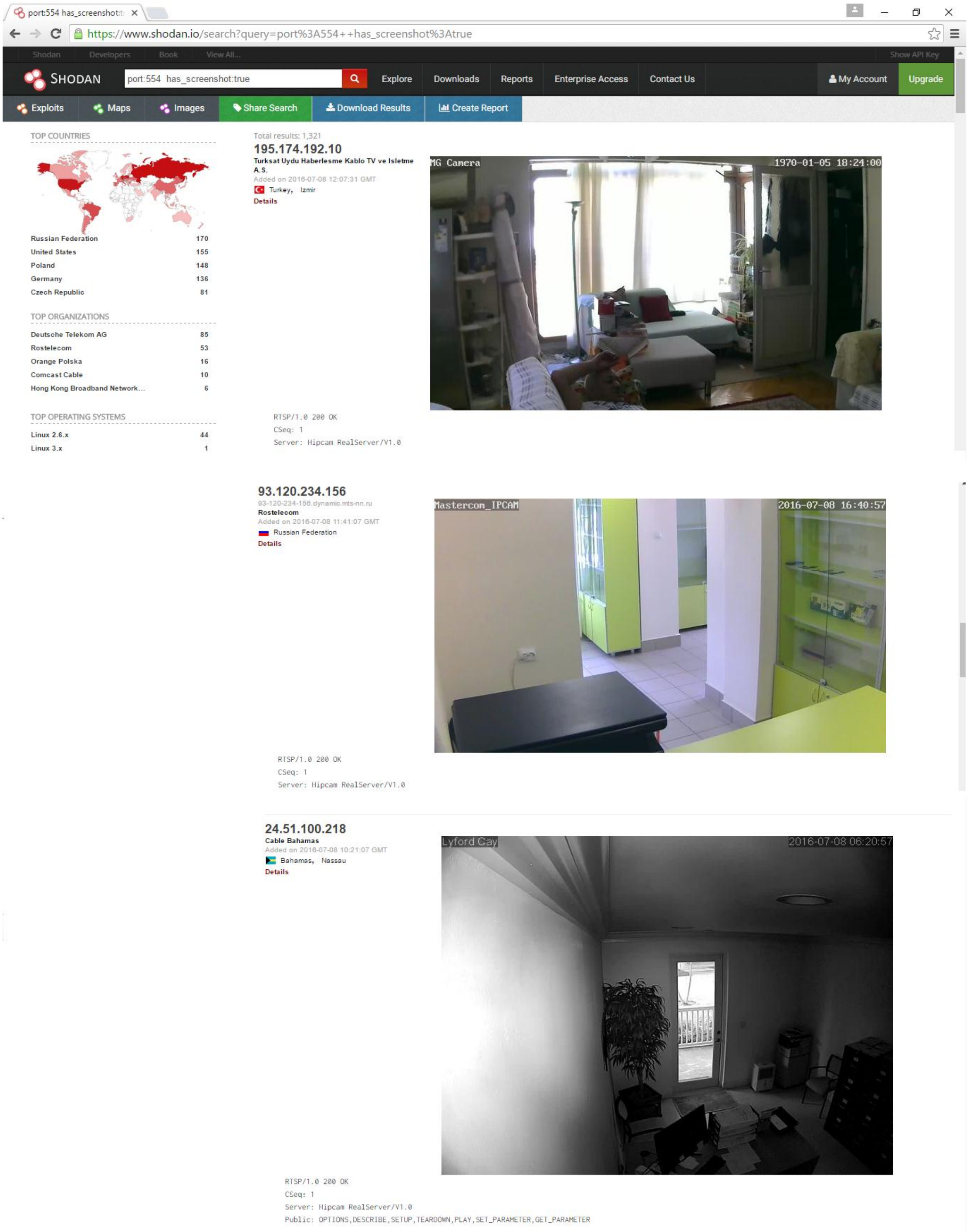
Security Threats in the Smart Homes

The overall nature of security threats is comparable to those in other domains, despite the fact that the Smart Home is a fundamentally different setting.Threats to confidentiality are those that lead to the unintentional disclosure of private information.For instance, privacy violations in home monitoring systems may accidentally result in the publication of private medical information. Even seemingly unimportant information, like the temperature inside a house, Knowing the air conditioning system's functioning settings might be helpful as well as a prelude to burglary, regardless of whether a house is occupied or not. confidentiality is lost in situations like Threats involving unauthorized system access will be caused by keys and passwords. Threats to authentication may result in the alteration of control or sensor data.Unauthenticated system status signals, for instance, could lead a house controller to believe opening windows and doors to facilitate an emergency departure when there is an emergency truth enabling unauthorized admission. Automated software upgrades are one concern that will be brought up later; if these are not properly authenticated, issues may occur. The biggest concerns are presumably those involving access. accessing a system controller without authorization makes the entire system insecure, especially at the administrator level. This is possible by improper handling of passwords and keys, or it can be caused by unauthorized devices connecting to the system. An unauthorized connection to a network can steal data even if control cannot be obtained. either eat up valuable network bandwidth or deny service to legitimate users.Numerous Smart Homes Devices having a low operational duty cycle that are remotely networked and powered by batteries, floods An energy depletion attack, which is a type of denial of service, can occur on a network with requests.

Vulnerabilities

Networked system accessibility is a serious vulnerability. Due to the Internet connectivity of contemporary Smart Home systems, assaults can be carried out remotely by either installing malware to devices or gaining direct access to networked control interfaces. Another difficulty is the physical accessibility of the system. The networks can be physically accessed from outside the house for both wireless and power-line carrier technologies, even if the house is securely closed. System resource limitations are the next weakness. Device controllers are typically tiny 8-bit microcontrollers with constrained computing and storage capabilities, making it difficult for them to apply sophisticated security methods. System heterogeneity poses a risk. Numerous vendors produce devices with various networking standards and software update capabilities.Frequently, the devices' internal software, operating systems, and installed security measures are not well documented, if at all. Another problem is updated firmware. There aren't many smart home products that offer any kind of frequent software update service to fix security flaws. One has the suspicion that there is now little motivation to update software often in order to stay ahead of security flaws for inexpensive devices. One weakness is the adoption of standards slowly. While some proprietary systems, such as a subsystem for monitoring health, may have well-designed security that complies with standards, the majority of existing Smart Home gadgets use few, if any, security measures. The biggest vulnerability, in our opinion, is the absence of specialized security experts that can handle the intricate nature of a Smart Home network. Few homeowners can afford to hire a professional to operate their home networks on an ongoing basis. Instead, novice home owners must be able to easily, securely, and operate their own systems.





TOP COUNTRIES

Russian Federation	170
United States	155
Poland	148
Germany	136
Czech Republic	81

TOP ORGANIZATIONS

Deutsche Telekom AG	85
Rostelecom	53
Orange Polska	16
Comcast Cable	10
Hong Kong Broadband Network...	6

TOP OPERATING SYSTEMS

Linux 2.6.x	44
Linux 3.x	1

Total results: 1,321

195.174.192.10
Turksat Uydu Haberlesme Kablo TV ve Isletme A.S.
Added on 2016-07-08 12:07:31 GMT
Turkey, Izmir
Details

```
RTSP/1.0 200 OK
CSeq: 1
Server: Hipcam RealServer/V1.0
```

93.120.234.156
93-120-234-156.dynamic.mts-nn.ru
Rostelecom
Added on 2016-07-08 11:41:07 GMT
Russian Federation
Details

```
RTSP/1.0 200 OK
CSeq: 1
Server: Hipcam RealServer/V1.0
```

24.51.100.218
Cable Bahamas
Added on 2016-07-08 10:21:07 GMT
Bahamas, Nassau
Details

```
RTSP/1.0 200 OK
CSeq: 1
Server: Hipcam RealServer/V1.0
Public: OPTIONS,DESCRIBE,SETUP,TEARDOWN,PLAY,SET_PARAMETER,GET_PARAMETER
```

Figure 1-2 - A list of home surveillance cameras from Internet devices–scanning search engine Shodan , insecam and earthcam.

An owner of a webcam, for instance, might believe that only users who know its host name and port number can access it. However, many devices are already recognized and visible because of Internet device-scanning search engines like Shodan (https://www.shodan.io) and Census (https://censys.io), which genuinely look for accessible sensors.

The traditional search engines, like Google and Bing, retrieve web pages from the Internet and then follow the hyperlinks to index webpages, images, or some common file types.

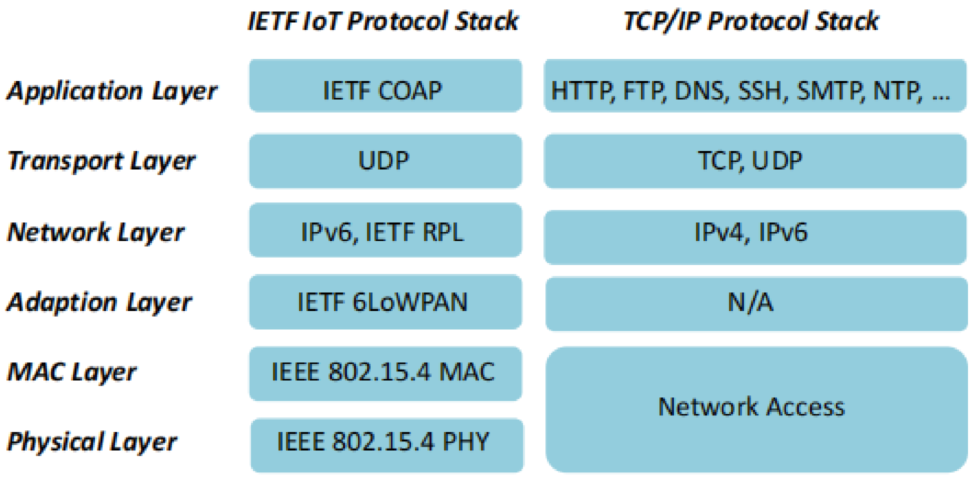
On the other hand, network scanner-like search engines for the Internet scan the open ports of Internet nodes and index the header or banner data returned by connected devices;The device type, model, vendor, firmware version, and other details are frequently included in the headers or banners of the response. In addition to HTTP and HTTPS, Internet device-scanning search engines connect to nodes' open ports using a number of other protocols, including FTP, SSH, DNS, SIP, and RTSP. These search engines also offer an application programming interface (API) for programmatic access to their search results to ease access. These search engines can be used by attackers to discover online susceptible devices. For instance, Shodan will return a list of home security cameras with their IP addresses, geographical locations, and screenshots if you search for "has screenshot:true port:554"

Security types for Home systems IoT

IoT computing devices are typically less powerful than conventional desktop and laptop computers because of their low cost. The majority of Internet of Things (IoT) devices have minimal power, basic microcontrollers, and little memory. These controllers are perfectly suited to the needs of standalone controllers in an air conditioner or washing machine. However, because the current Internet protocols are not often created for these embedded devices, these characteristics have made the transition to networked IoT controllers more difficult.

To address these issues, a number of working groups within the Internet Engineering Task Force (IETF) have been established. The development of the requisite light-weight communication protocols for limited contexts over the current IP network has been greatly aided by IETF standardization work on the Internet of Things.These include Constrained Application Protocol, IPv6 Routing Protocol for Low Power and Lossy Networks, and IPv6 over Low-Power Wireless Personal Area Networks. In Figure 2, the IETF IoT and TCP/IP protocol stacks are compared. Any Internet security issue that affects other connected devices could likewise jeopardize the security and privacy of IoT. We examine the present security implementations for these common IoT protocols in the sections that follow.

To address these issues, a number of Internet Engineering Task Force working groups have been established. The development of the requisite light-weight communication protocols for limited contexts over the current IP network has been greatly aided by IETF standardization work on the Internet of Things. These include Constrained Application Protocol, IPv6 Routing Protocol for Low Power and Lossy Networks, and IPv6 over Low-Power Wireless Personal Area Networks. In Figure 2, the IETF IoT and TCP/IP protocol stacks are compared. Any Internet security issue that affects other connected devices could likewise jeopardize the security and privacy of IoT. The implementations of these standard I security measures are reviewed in the sections that follow.



	IETF IoT Protocol Stack	TCP/IP Protocol Stack
Application Layer	IETF COAP	HTTP, FTP, DNS, SSH, SMTP, NTP, ...
Transport Layer	UDP	TCP, UDP
Network Layer	IPv6, IETF RPL	IPv4, IPv6
Adaption Layer	IETF 6LoWPAN	N/A
MAC Layer	IEEE 802.15.4 MAC	Network Access
Physical Layer	IEEE 802.15.4 PHY	

Figure 2. The comparison between IETF IoT and TCPIP protocol stacks.

WPAN and security

The 802.15.4 standard for wireless personal area networks has been established by the Institute of Electrical and Electronics Engineers (IEEE) (WPANs). Under the low-bandwidth, low-cost, low-speed, and low-energy conditions typical of these networks, IEEE 802.15.4 specifies how the physical and media access control layers should function. As a result, the IETF created the 6LoWPAN [23] light-weight protocol to enable the delivery of IPv6 packets across IEEE 802.15.4 wireless networks.

To provide data integrity, secrecy, origin authentication, and anti-replay protection for IPv6 packets, the Internet Protocol Security (IPsec) suite has specified Authentication Headers (AH) and Encapsulating Security Payloads (ESP). Compressed AH and ESP characteristics were suggested by the authors of [24] for 6LoWPAN in order to implement IPsec and offer end-to-end secure communications between wireless devices.The authors have suggested an improved authentication and key establishment technique (EAKES 6Lo) for 6LoWPAN networks in [25]. The security of 6LoWPAN networks is improved by EAKES6Lo, which is split into two phases. System setup and authentication and key establishment are the two processes. The network's data transit in Phase 1 is encrypted using the symmetric cryptography technology Advanced Encryption Standard (AES). Secure Hash Algorithm (SHA) or Message Digest Algorithm 5 (MD5) hash functions are used to check the data's integrity. To complete the authentication and key establishment procedure and establish a mutual authentication, six messages will be sent in Phase 2.

So, even for devices with little resources, 6lowPAN offers a model for safe wireless communications.

RPL and Security

Routing protocols are a fundamental part of traditional networks, and 6LoWPAN networks are no different. RPL is a 6LoWPAN network-specific IPv6 routing protocol that has been improved by the IETF for Low Power and Lossy Networks (LLNs). The mapping topology of RPL, a distance-vector routing system, is built on a destination-oriented Structure of directed acyclic graphs. Trust is a general-purpose topology authentication system. In , the Anchor Interconnection Loop (TRAIL) for RPL was presented. TRAIL is able to stop the by identifying and isolating the forged nodes, we defend against topological inconsistency attacks from fake nodes.TRAIL has utilized a round-trip message to confirm upward path integrity to the root node and assist the tree's nodes in receiving accurate rank data. TRAIL's breakthrough is that each node in The tree can verify the root-to-stem path and identify any attacks with false ranks. Since each node in the DODAG tree has a parent node, it is crucial for nodes to choose the appropriate parent node. other than the root, which demands a parent node. A node's placement in the network is described by its RPL rank. tree topography A node's threshold value will be calculated by the selection algorithm based on the maximum and average rank values of its neighbor nodes to weed out spoofing nodes turning into its parent.Therefore, secure routing table construction in Smart Home networks is ensured by existing methods.

Future home systems (IoT) Security Directions

The three examples above show that there is already a lot of work being done to protect mission-critical IoT applications. A lot of work has gone into creating IP-compatible secure communications networks that use cutting-edge security methods and are appropriate for devices with limited resources. To develop and maintain a secure IoT system, many of these strategies need thorough, unified, system-wide architecture and skilled network engineers.

Our work focuses more on the system management element of Smart Home security, i.e., how to correctly install and maintain the protection made possible by these potent instruments, than on this kind of "technical" security.

Security-friendly Smart Home Architecture

There have been numerous suggestions for alternate Smart Home architectures, all of which have unique security concerns. Middleware, cloud, and gateway architectures are three of the most significant and well-liked designs. The security concerns and implementation challenges for various architectural designs are examined in the following sections.

Middleware Architectures and Security

Middleware sits between the low-level layer of devices and the high-level application layer. It provides a common interface and a standard data exchange structure to abstract the complex and various lower-level details of the hardware. Security and privacy protection should be considered at all levels of the middleware, from the lower hardware interaction level to the higher common interface level.

While middleware has been widely used in corporate systems with desktop-class machines to manage complex heterogeneous networks, currently proposed IoT middleware solutions call for the implementation of a significant number of additional complex software layers and cryptographic routines on devices that lack the memory and processing power to support them. In addition to performance issues, middleware developers' unintentional introduction of coding errors raises security concerns for

IoT devices. This is a worry for middleware architecture. Because many IoT-class devices are currently infeasible, we reject middleware solutions.

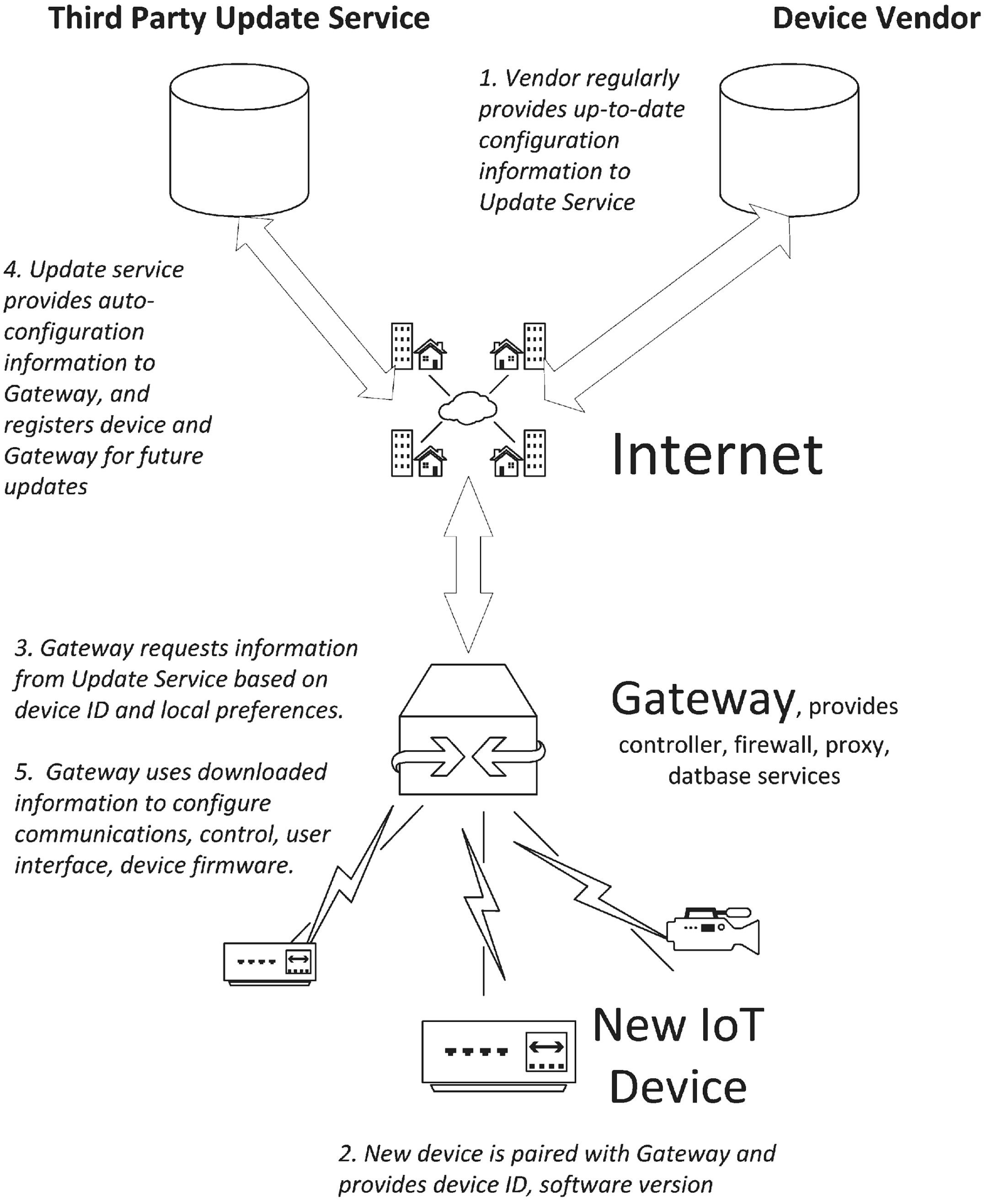
Cloud Architectures and Security

Cloud computing could solve the performance problem of IoT devices. The cloud can analyze raw data and trigger actions according to user-defined policies to achieve complex Smart Home control. A secure scheme for the Home Area Network (HAN) based on cloud computing has been introduced. This scheme employs symmetric key encryption to apply confidentiality between end-to-end communications and each smart object is assigned a unique key.

Future Security Challenges for Smart Homes

Auto-Configuration Support

A lack of technical support is the biggest challenge in the household environment. When a new Smart Home device is attached to the network, the gateway will use the device ID to interrogate a trusted web service to discover the details of the device. This is a different approach to most auto-configuration approaches which require a lot of this information to be stored on the devices themselves.


Third Party Update Service
Device Vendor
1. Vendor regularly provides up-to-date configuration information to Update Service
4. Update service provides auto-configuration information to Gateway, and registers device and Gateway for future updates
Internet
3. Gateway requests information from Update Service based on device ID and local preferences.
5. Gateway uses downloaded information to configure communications, control, user interface, device firmware.
Gateway, provides controller, firewall, proxy, datbase services
New IoT Device
2. New device is paired with Gateway and provides device ID, software version

Home systems (IoT) Software and Firmware Updates

Firmware is a type of software that is programmed into the non-volatile memory of a smart device. Unlike the enterprise-scale environment which has its own dedicated IT department or technical team to manage and deploy the software updates, the SmartHome environment usually lacks technical support. The IoT devices for Smart Homes should have mechanisms to implement safe and secure firmware updates automatically, with little or no user intervention. Each update must be verified against its digital signature and the digital certificate should be checked to ensure it is valid and is issued by a vendor or trusted third party. If the update-checking mechanisms are compromised, a hacker could block the new updates from being installed and conduct an attack on unpatched firmware. Attackers could also disguise a legitimate old version of firmware with security vulnerabilities as the latest version.