基于物联网的智能家居的安全和隐私问题

摘要：

物联网（IoT）可以支持各种领域的众多应用和服务，如智能城市和智能家居。 IoT智能对象与其他组件（例如，代理，移动设备和数据收集器）进行交互，以在所提供的服务的上下文中进行管理，数据共享和其他活动。虽然这些组件有助于解决各种社会挑战并为用户提供新的高级服务，但其有限的处理能力使其容易受到众所周知的安全和隐私威胁。到目前为止，各种研究工作已经研究了物联网中的安全和隐私，验证了这一说法。然而，据我们所知，文献缺乏关于通过支持智能家庭架构的不同设备之间的交互在物联网中引入的安全和隐私缺陷的研究。特别是，我们为使用现成组件的典型智能家居架构设置了安全和隐私威胁分析的场景。为此，我们采用智能家居物联网架构，使用户能够通过支持智能住宅管理的各种设备与其交互，并且我们分析不同的场景以识别用户可能出现的安全和隐私问题。

一，导言

新型传感器和执行器的开发与日益强大和普及的网络连接的部署相结合，正在形成物联网（IoT）的概念。目前互联网进入物联网的演变有几个因素，包括物联网设备的市场价格较低以及客户对新服务的需求较高。

制造商现在能够为移动，可穿戴或嵌入式设备提供更多的存储器，处理能力和更多不同的传感技术。因此，物联网设备的这种增加的能力也增加了可用于服务的数据量以及它们对最终用户的价值。然而，即使物联网能够支持新的商业模式，提高许多应用程序的效率，并通过新服务丰富公民的生活，风险也显着增加。收集更大量的数据并合并网络和物理世界意味着隐私和安全问题的数量高于仅限网络的互联网。

更具体地说，我们在本文中的重点是智能家居方案。在这种情况下，如果我们考虑直接和明确收集关于居住在房屋中的个人的数据，隐私泄露的可能性就会受到限制。但是，这些人的活动可以

通过观察其相连的家用设备，辅助生活系统或智能电表的网络和身体活动来间接追踪。在不同实体和物联网技术共存和协同工作的复杂情况下保护隐私需要新的方法和解决方案。即使在文献中提出了各种隐私支持技术（PET），其市场采用率仍然相对较低，许多具体的威胁仍然存在。

在本文中，我们为典型的智能家居架构设置了安全和隐私威胁分析的场景，该架构依赖于现有的和现成的市场IoT设备和平台。与物联网场景的现有安全和威胁分析相比，我们的目标是部署在测试平台上的真正的物联网智能家庭环境，重点关注不同物联网组件之间的交互。在这种体系结构中，我们确定对手可能操纵的兴趣点，以获取未经授权的信息或导致拒绝服务。除了具体的威胁分析之外，我们的贡献是对已确定的漏洞的实际可行性评估，显示如何在实践中实施漏洞利用。

本文的其余部分的结构如下。在第二部分中，我们概述了智能家居的体系结构，第三部分我们分析了它的威胁模型。在第四部分中，我们研究了在测试平台架构中实现威胁模型，并分析了安全和隐私方面对最终用户的可能后果。在第五部分中，我们提供了消除威胁存在的准则和保护措施，而在第六部分中，我们概述了相关的工作。最后，在第七部分，我们总结本文，并为今后的工作提出一些指引。

II。基于物联网的智能家居架构

智能家庭可定义为不同元素的共生关系，即构建动态异构体系结构的传感器，连接和应用程序，旨在有效管理家庭设备，并向用户提供高级服务。

由于物联网设备之间的通用互操作性标准仍然存在缺失，在这种体系结构中，没有损失通用性，组织在岛上的物联网设备连接到相应的集线器，并且不会被其他设备直接访问。而且，大多数商用传感器不提供直接的互联网连接;而不是中间人枢纽是负责提供这种联系的组成部分。

物联网设备和集线器之间的通信通常是无线的，取决于设备制造商的不同协议。最受欢迎的是：

•Zigbee1;

•Z波2。

然后，集线器通过以太网或Wi-Fi接口连接到智能家居路由器，具体取决于其功能，以便将物联网设备与外界连接。

用户可以与物联网设备进行交互，并通过PC，智能手机和平板电脑等不同平台管理他们的智能家居。互动模式通常是两种：

1）使用集线器提供的连接和服务直接与它们进行交互;

2）访问与IoT中枢和所连接的IoT设备交互的互联网云服务。

这两种情况经常同时出现，并混合在一起以支持与IoT对象的本地和远程交互。在远程管理的情况下，通过云服务将所有信息转发到智能中心，而如果用户从安装智能中枢的同一网络进行操作，则流量将直接路由到它，因此不需要互联网访问。

但是，为了使用户能够启用物联网设备管理，无论他们的位置如何，他们都必须先执行将其设备与相应集线器相关联的过程。在大多数情况下，对于成功完成此过程的现成解决方案而言，涉及用户的身体动作，例如按下智能中枢上的按钮。

此外，物联网制造商还支持简单服务发现协议（SSDP）[1]等协议，以便在需要最少用户交互的即插即用模式下实现智能家庭设备的透明配置。在这种情况下，智能中枢为多播信道（即，默认的IoT设备的网关）生成呈现宣告。任何搜索可用服务的设备都会向组播频道发送发现请求，并接收可用请求的服务作为响应。然后设备可以直接与新发现的服务进行通信。这个过程如图2所示。

因此，考虑一个例子，其中用户希望在他在家之外时使用他的移动电话来控制智能家居的灯光状态。要做到这一点，首先他必须已经成功完成了关联程序，否则无法远程访问智能家居的设备。一旦设置完毕，他可以启动移动应用程序并请求灯的状态。该请求到达云服务，该服务代表用户将其转发到负责控制灯的集线器，使用通过房屋路由器保持打开的反向通信信道，由集线器本身。集线器一收到这样的请求，它就立即向灯发送相应的命令，即状态以接收其响应，并通过云服务将其转发给用户。图1说明了智能住宅不同组件之间的所有交互。

III。智能家居威胁模型

智能家居网络威胁模型的制定应考虑两种类型的对手;内部和外部实体，可以根据他们的目标以被动或主动的方式恶意行事。一方面，前一类包括位于智能家居场所附近或内部的恶意实体。另一方面，外部攻击者只能通过互联网连接进行交互。在这两种情况下，对手都瞄准智能家居的基础设施或存储在相关云服务中的信息。请注意，在这项工作中，我们不认为敌手可以物理访问物联网组件。这是因为，网络实体只能虚拟访问提供服务的组件。

在这种情况下，类似于任何其他基于IP的服务，被动行动的对手会尝试窃听可用的通信，以获取可用于监视用户行为的信息，或者可以在主动攻击的后续步骤中积累和利用。为了获取这种类型的信息，对手将尝试根据智能家居架构的功能和目标来捕捉智能家居架构不同点的流量。通过这种方式，攻击者可以影响用户的机密性和隐私，因为他们可以收集与智能家居相关的信息。举例来说，如图1所示的架构，如果对手监控智能中心和智能房屋内路由器之间的通信链路（1），他可以识别智能中心与哪个实体通信，而如果他监控通信链接（4）他可以推断出用户的日常习惯，例如，当灯打开和关闭时可能对应于用户离开家时的习惯。

另一方面，积极的对手将与IoT组件积极互动，而不是只窃听底层通信。他可以通过不同的网络设备生成适当的探针来识别组件的存在。而且，敌手可能会尝试冒充合法用户以访问智能家居设备。然后，他可以控制它们，使用它们甚至从中提取敏感信息。活跃的对手不仅会影响用户的隐私和所提供的服务的机密性，还会影响数据的完整性，获得未经授权的访问并最终破坏所提供服务的正常功能。

显然，在更复杂的情况下，攻击者可能会结合被动攻击和主动攻击。例如，考虑智能插座向卫生设备供电的情况。如果对手通过歪曲通信流量来了解其唯一标识符，他可能会导致对IoT的拒绝服务，从而可能对用户的安全产生直接影响。出于这个原因，这类信息应该被认为是非常重要的。

除了被动和主动的网络层威胁之外，软件开发是积极攻击者利用其他方面来访问私有域的另一个方面。这是因为，物联网依赖于众所周知的操作系统的轻量级版本，攻击者希望利用极少的资源进行攻击。而且，大多数主要使用的物联网设备都具有相应的移动应用程序，充当控制器。移动应用程序的执行环境可以用作对手的攻击媒介，因为他可以利用底层操作系统中众所周知的软件漏洞。

表I概述了他们可以对智能家居的基础设施造成的威胁和可能产生的后果。

IV。基于物联网的智能家庭网络缺陷

为了研究第三部分报告的通用威胁的可行性，我们部署了类似于图1所示的测试平台架构。该架构基于商用产品，通过智能集线器连接到物联网传感器网络和通过传统无线路由器连接到互联网。具体而言，将支持WiFi网卡和互联网连接的计算机（A）配置为具有IoT管理应用的移动设备连接到的接入点。在连接到计算机的A WiFi以连接互联网的第二台计算机（B）中，附加了IoT设备或集线器（取决于设备类型）。这样，计算机A监视图1中点3和4所示的流量，而计算机B监视点2的流量。通过在两台计算机上运行wireshark，我们能够捕获所有通过特定点的数据包。

由于我们的目标是一般性地说明物联网的安全和隐私问题，而不是批评特定产品，因此我们不提供任何相关信息。请注意，由于我们有兴趣研究不同组件之间的交互，我们假设强大的对手[2]可以访问基础通信，例如通过利用特定设备或协议漏洞，使用默认或普通WiFi和路由器密码，破解不安全的密码，社会工程等，但是，这样的分析超出了这项工作的范围。

在下面的小节中，我们将讨论第三部分中描述的威胁的实现，并考虑我们从我们的测试平台架构以及其他相关研究报告中收集的信息。

A.窃听

考虑到其异构架构，攻击者可能使用不同的工具和技术来捕获基于IoT的智能家居基础架构不同组件之间的流量。这些技术与攻击者的位置和能力高度相关。

如果攻击者设法连接到智能家庭网络组件，例如adsl路由器，他能够捕获智能中枢与本地或远程用户之间的所有流量;这对应于图1的参考点2,3和4.在那种情况下，攻击者依赖诸如tcpdump3，wireshark4等众所周知的工具来访问数据。在通信无线的情况下，攻击者可能会使用特定的硬件设备，例如WiFi Pineapple5，它可以欺骗接入点并拦截底层通信;这对应于图1的参考点1,2,4。

因此，考虑到拦截参考点1,2和3之间的交通的对手，他可以识别：

1）智能集线器是否与云支持的服务进行通信，例如（cloud.iot.com:80）

2）用户设备的类型（例如，Linux，Android 7.1.1; Nexus 5X Build / NMF26F）

3）用户访问智能中心服务的唯一标识符

4）通过流量分析设备的状态

5）智能集线器的操作系统（例如，像OS一样的unix）

6）可用于向智能发送命令的方法

集线器（例如，POST，GET，DELETE等）

清单1举例说明了本地网络中智能中心服务通知期间的窃听信息示例。在这种情况下，攻击者可以推断出智能集线器运行的操作系统，IP地址和唯一ID。在这一点上，应该提到的是，根据物联网制造商的不同，这些信息可能会有所变化。

B.冒充

对手可以尝试冒充并代表合法用户行事。要做到这一点，他需要访问用户的凭证或提供访问物联网资源的任何其他信息。前一种情况用于要求远程访问IoT设备的IoT体系结构，而后者通常用于从本地网络访问IoT资源（在这种情况下，所需的关键信息的例子是例如智能集线器在设备注册过程中生成以启用本地访问）。请注意，智能中心通常会根据他的IP地址识别用户的位置。因此，如果攻击者捕获到这样的消息，他可以冒充用户，并可以代表用户与智能中心进行交互。这可以通过简单地用适当的参数制作对智能中心资源的适当请求来实现，例如：http：// ip-address / api / unique-id / rsrc

回想一下，在对手窃听攻击期间，对手可以拦截唯一标识符。在这一类别中，我们还将重播攻击分类为攻击者重复使用先前的请求，以便向中心或基于云的服务发送请求，以便用户不具备有关其设备状态的正确信息。尽管这种攻击假定攻击者在智能集线器所在的同一网络上运行，但在对手可以从外部到达智能家庭路由器的情况下，它会在智能家居架构中引入一个漏洞。

C. DoS

同样，对于其他基于IP的服务，使用不同技术的对手可能会尝试向集线器或传感器本身导致拒绝服务（DoS）。由于攻击者通过窃听知道智能中枢的IP，他只需发送大量请求即可轻松发起单个DoS或分布式DoS（DDoS）攻击。请注意，由于物联网设备依赖低功能处理硬件，因此它们也易受低速率DoS攻击[3]。

或者，攻击者可能会尝试制作特定的消息，例如格式错误的消息，以便所提供的服务无法正确处理它们，并导致DoS或提供未经授权的访问。

DoS也可以直接在物联网设备上进行，而无需通过智能中心。具有使他能够使用物联网设备协议的适当硬件的对手可以将消息直接发送给他们并试图干扰他们的正常功能。

最后，还可以在路由器或云服务处发生DoS攻击。这可能是一种普遍攻击，与物联网无关，但对最终用户的后果将是相同的。如果没有工作路由器或无法提供服务，他将无法通过互联网访问其智能家居的物联网设备。

D.软件开发

恶意软件（恶意软件）可能会影响物联网服务和设备。随着物联网设备自主运行，众所周知的操作系统攻击者的轻量级版本将搜索软件漏洞并利用它们访问其他私人信息。

但是，目前物联网正在成为执行DoS的攻击目标，以便增加产生的流量的放大因子来打破目标。例如，物联网设备已被利用来发起针对DNS服务器的DoS攻击[4]，以瘫痪互联网访问。在这种情况下，攻击者利用这些设备通过默认配置（例如默认密码）通过互联网运行的事实，而大多数这些设备在大多数情况下都没有针对安全缺陷进行修补。

恶意软件可以通过不同渠道到达物联网设备：

1）设备采集：当设备被最终用户购买时，存在购买感染恶意软件的设备的风险。例如，对手可以购买许多新设备，感染它们，并通过在线拍卖网站（例如eBay6）将其出售给用户。

2）固件升级和受信任的引导：在收购期间正交于设备感染，攻击者可能能够使用恶意代理版本升级物联网固件。例如，这是一个在Mirai恶意软件的情况下被攻击者利用的渠道[5]。

3）应用程序和服务：用户通过相应的应用程序和在线服务来控制他们的物联网设备。最近，管理设备的最常见方式是在用户的移动设备上使用移动应用程序。几乎所有的制造商都提供可直接从移动操作系统应用市场下载的应用程序。由于这些应用程序是在用户的个人设备上执行的，因此它们可能会受到设备上已存在的恶意软件的感染，或被攻击者利用移动应用程序或操作系统的漏洞直接利用。

此外，一些物联网制造商认为他们可以将安全委托给智能家庭的底层架构，例如路由器的防火墙。 但是，这个假设不应被视为理所当然。 正如Sivaraman等人 在他们的工作[6]中展示，部署在智能家庭中的安全措施可以轻松地被恶意软件移动应用程序绕过。

与移动应用程序类似，与智能中心直接交互的在线服务可能会在物联网架构链中造成薄弱环节。 如果通过标准的Web服务攻击方法设法访问它们，他就可以轻松操纵所有连接的物联网设备。

五，讨论

考虑到目前智能家居架构中的上述讨论，攻击者可以访问下面的基础设施并利用它。因此，智能家庭应该像其他基于IP的高级资源服务一样处理安全“缺陷”。

因此，在智能家居的情况下，由于物联网不同组件之间缺乏端对端加密，攻击者可以窃听底层通信并提取不同的信息。这也是IoT构建的现有协议的一个缺陷;例如，SSDP协议不使用任何加密，因此攻击者可以利用这一事实并识别可用的智能集线器及其功能。

此外，智能家庭部署遵循的当前访问控制方法，例如，在用户设备与智能中枢相关联期间生成唯一标识符，将IoT服务暴露给模拟攻击，因为攻击者可以窃听唯一标识符并将其用于未来攻击企图。但是，如果部署了适当的完整性和身份验证机制，则可以减轻这些类型的攻击。

针对DoS及其分布式对应方（DDoS）的防御是一项具有挑战性的任务，尤其是考虑到IoT体系结构有限的功能，而目前我们甚至缺乏高效安全基础设施支持的基于IP的服务的有效解决方案。据我们所知，只有研究相关的解决方案如[7]已被提出用于保护物联网免受DoS攻击。但是，这种方法并不关注应用层，而主要是处理网络层保护。

由于大多数低成本物联网制造商通常不考虑在安装，升级和执行期间验证固件完整性的机制，例如使用受信任的引导，物联网设备会面临可能的软件缺陷。为了消除软件开发，用户还应该使用通过众所周知的渠道提供的应用程序和服务，因为未知的第三方应用程序可以操纵现有的基础设施，为未来的攻击引入后门。

一个主要问题是可以使用默认配置部署物联网安装。正如前面的部分所解释的，这是使DNS攻击[4]成为可能的原因。其中的建议可能是强制用户正确配置设备，否则服务无法启动（即，默认情况下路由器不能打开端口，只有设置了强密码才能启用远程登录，才能启动IoT服务并且只有在设置好密码的情况下才被访问。）接下来，针对无线通信的问题，打开的连接不应该作为默认配置，

路由器只能在默认密码更改时启动，易受攻击的协议应该被弃用并从配置选项中删除。

VI。相关工作

Jacobsson等人在[8]，[9]中介绍了一个在涉及领先工业主体的研究项目中开发的智能家庭自动化系统的风险分析结果。他们的架构与本文讨论的架构相同，包括传感器/设备，内部网关，云服务器，移动设备和应用程序。风险分析在与安全专家，领域专家和智能家庭系统开发人员等9人的合作研讨会期间进行。这次讨论是使用用于推理，识别，分析和评估威胁的开放式信息安全风险评估问卷进行组织的。确定的威胁与各自的系统漏洞相关联，并且每个参与者使用五级标度（1-5）评估每种威胁的相关概率，发生的可能性以及潜在影响，这些标准来自不同的/可忽略的/可能/惨重。风险分析结果分为五类：软件，硬件，信息，沟通和与人相关的风险。每个类别中排名较高的风险分别与应用程序和API中的软件安全性，物理安全性不足，访问控制策略/机制不足，认证和机密性不足，密码管理不佳有关。他们的风险分析结果是高水平的，与我们在本文中的发现一致。此外，在他们的工作中，主要的观察是需要基于经验的方法来支持智能家居环境中的风险评估，这正是本文的重点。

科兹洛夫等人。在文献[10]中描述了整个物联网架构的威胁分析，包括安全，隐私和信任问题。他们的威胁分析主要是考虑到许多场景和应用领域（例如，智能家居，道路交通，智能电表和移动应用）在文献中讨论的高级威胁选择。所讨论的情景说明了对个人数据隐私，可用性以及安全性的威胁，例如，当道路交通系统中被利用的漏洞可能导致事故时。与他们的工作相比，本文所做的分析在确定的威胁和漏洞方面更加具体，并且还专注于部署的智能家庭方案。我们不仅展示高层次问题，而且展示如何在真实物联网设备中实现攻击者。

佩雷拉等。在文献[11]中提出了一种针对物联网应用和平台进行评估的隐私设计框架，该框架被提出作为一种系统的方法来指导基于30条指导方针的物联网中的隐私分析和设计。每个准则应在数据生命周期的不同阶段应用，包括同意和数据采集，数据预处理，数据处理和分析，数据存储和数据重新分配。准则解决的主要隐私风险是未经授权的访问和信息的二次使用，意味着使用已收集的数据用于数据所有者最初不允许的目的。作者展示了他们的框架在两个开源IoT中间件平台中的应用：OpenIoT和Eclipse SmartHome。对于每个中间件，构建一个表格，显示数据生命周期中每个阶段是否支持，可扩展或不支持指南。可扩展的支持意味着中间件提供了一个插件机制，可以使其直接实现功能。通过比较每条指南的支持，可以比较中间件的隐私设计功能和差距;从某种意义上说，遵守这些准则意味着隐私风险较低。与本文中的技术贡献相比，拟议的指导方针更加抽象（例如，数据匿名化，加密等），并且可以映射到本文中详述的威胁和漏洞。

齐格尔多夫等人。在[12]中对广义的RFID隐私威胁进行了分类和检查，目标是提出未来部署中应该克服的相关挑战。在他们的参考模型中，他们考虑收集用户环境中设备的信息，以及利用RFID技术的服务处理和传播信息。在他们的分析中，他们列出了隐私的主要威胁，即：识别，本地化，跟踪，分析，违反隐私的交互和演示，设备退役，库存攻击以及RFID相关组件的链接。由于他们的分析，分析被认为是最严重的威胁。与我们的方法相比，这项工作专注于基于RFID的物联网系统，而我们专注于智能家居组件威胁分析。

七。结论和未来的工作

物联网架构将成为未来互联网的重要组成部分，因为它缩小了物理和虚拟物体之间的差距。其中，智能家居是物联网环境的主要发展之一，因为它增强了用户使用家庭设备的体验。

尽管物联网为智能家庭用户提供的优势不仅使家庭受到众所周知的攻击，而且（物联网）传感器也应该处理先前未曾考虑过的缺陷。这是由于这样的设备具有有限的处理能力，并依赖异构网络体系结构，这增加了所提供服务的攻击面。

在本文中，我们引入了智能家庭威胁模型，并在我们的测试平台架构中考虑了现成的组件来分析它。我们的初步分析表明，现有的智能家庭物联网基础设施在特定条件下可能容易受到窃听，模仿，DoS和软件开发攻击媒介的攻击，例如，考虑到攻击者设法访问底层网络。

目前，我们正在计划扩展我们的分析，详细阐述其后果和影响

针对用户和物联网基础设施的不同威胁，并提出加强智能家居安全的相应对策。在这个方向上，我们设想一个能够自动识别智能家居架构中易损点的框架。

物联网隐私和安全挑战智能家居环境

摘要：物联网（IoT）通常被认为是一个单一的问题领域，所提出的解决方案旨在应用于广泛的应用。但是，关键工程基础设施或敏感商业运营的隐私和安全需求与国内智能家居环境的需求大不相同。此外，可用于实施安全和隐私的财务和人力资源在不同应用领域之间差异很大。在国内环境中，人类问题可能与技术问题同等重要。在调查了用于增强IoT安全性的现有解决方案之后，本文确定了可信智能家居系统未来的关键要求。网关体系结构被选为最适合资源受限设备和高系统可用性的体系结构。确定了两项帮助系统自动管理的关键技术。首先，支持系统自动配置将增强系统安全性。其次，需要系统软件和固件的自动更新以维持持续的安全系统操作。

1.介绍

物联网（IoT）近年来引起了人们的关注，这个术语描述了非传统设备（如工厂机械，医疗设备或家用电器）与互联网的连接。在过去的几十年里，基于微处理器的控制器在从烤面包机到航空公司的应用中已经变得无处不在。通过将这些控制器连接到互联网，物联网可以看作是这些控制器发展的下一步。此外，RFID（无线电频率识别）标签被视为一种物联网技术，用于在互联网上提供位置以及潜在的标签对象状态。 Atzori等人[1]等等，对物联网技术的应用范围进行了回顾。

评论者对于物联网技术渗透的重要性和深度的理解各不相同。思科的未来学家Dave Evans将他的评论翻译为“互联网的下一个演进如何改变一切”。其他人，如Hurlburt等。 [3]，担心期望不切实际。自2011年进入Gartner Hype Cycle以来，物联网在过去几年一直处于“高涨的期望值”[4]。

欧盟委员会已将“物联网”确定为其重要工作计划之一，并得到AIOTI-物联网创新联盟的支持。该联盟承认物联网将负责未来的颠覆性技术，同时还需要将新技术与多供应商生态系统协调一致：“建立AlOTI的总体目标是创建一个动态的欧洲物联网生态系统，以释放物联网的潜力“[5]。早在

2008年，美国国家情报委员会将物联网列为“到2025年潜在影响美国利益的六种技术之一”[6]。

虽然关于物联网技术的深度和未来十年采用率的争论仍在继续，但很明显，物联网渗透迅速且具有破坏性的领域很多。本文调查的一个新兴领域是将物联网应用于智能家居。

与网络计算的所有领域一样，安全和隐私是物联网中可信系统操作的主要要求。适用于安全关键系统和企业安全的许多原则同样适用于物联网安全。然而，虽然企业可以将专门的专业资源用于系统安全和系统架构设计，但智能家居通常是一个相对特殊的系统，没有专门的系统管理资源，并且没有家庭成员的深入技术知识。这对安全和隐私提出了特别的挑战。提出的解决方案可以解决安全问题，但仍有一些领域需要进一步开展工作。本文的两个主要贡献是总结现有的可用于保护智能家居的网络技术，然后介绍需要进一步开展工作的两个特别关注的领域（系统自动配置和安全更新）。

本文的其余部分的结构如下。在第2节中，给出了隐私和安全问题的简短介绍。在第3节中，将探讨物联网技术影响的不同应用领域的范围，以表明物联网不是“一刀切”的技术集合，并将特别强调物联网应用智能家居应用程序。第4节介绍了智能家居中的安全威胁和漏洞，第5节介绍了一些现有的解决方案。第6部分证明了我们的首选系统架构，第7部分展示了我们未来的研究方向，然后才在第8部分得出最终结论。

2.关键问题在于网络安全和隐私

互联网已经从一个有用的大学研究工具发展成为一个基本的实用工具，与电力，水和天然气一样重要。无论哪里都有宝贵的资源，也有一些犯罪试图从非法使用该技术中获得价值，或者拒绝将该资源用于其他人。互联网的互联性意味着互联网资源可能受到来自世界任何地点的攻击，这使得网络安全成为关键问题。网络安全围绕三大主题展开。

保密是关于保持数据私密性，以便只有授权用户（包括人和机器）才能访问这些数据。加密技术是实现机密性的关键技术。

验证是关于验证数据没有被篡改，并且数据可以被验证是由声明的作者发送的。不可否认（即避免发件人拒绝实际发送邮件）有时会分开考虑，但我们将其作为认证的一个子集包含在此处。

访问是指只允许经过适当授权的用户访问数据，通信基础设施和计算资源，并确保不会阻止这些授权用户访问。

信息安全违规调查是由英国商业，创新和技能部委托由PriceWaterhouseCoopers进行的年度网络威胁报告。 2015年的最新调查[7]显示，安全漏洞呈上升趋势; 2015年，90％的大型企业遭遇网络违规行为，2014年为81％，74％的小型企业也遭遇安全漏洞，同比增长率为14％，达到两位数。

既然互联网已经成为现代企业的关键任务组成部分，网络安全已经成为信息系统不可缺少的组成部分。但是，随着网络安全性的增强，网络犯罪正在演变为更广泛，更具破坏性和更复杂的网络犯罪。在智能家居中，户主能够安全地管理他们的系统需要可靠和直观的自动化系统来协助网络管理。没有这样的系统，智能家居的安全和隐私威胁可能会超过其优势。

3. IoTApplicationDomains

通过部署物联网技术，许多应用领域特别适合于提高生产力。工厂和工厂自动化应用通常归入工业物联网的标题下。 Xu等人[8]审查这个应用领域。可靠性（包括通过冗余，安全性和适用于恶劣环境的适用性）是一些关键问题。

医院中生物医学仪器和数据库的联网有可能显着提高诊断和治疗决策的数量和可用性[9]。它对农村和偏远的诊所也有实质性的影响，可以随时获得专家的意见[10]。将医疗器械扩展到家中可提高生活质量并减少住院率[11]。

在过去的二十年中，基于数十个网络微处理器，汽车中的电子器件的使用激增[12]。下一阶段的发展将是车辆之间以及车辆和基础设施之间的交流[13]。标准化，安全性和成本是主要驱动因素。

运输和物流已经成为RFID标签的重要用户，用于追踪货物，托盘甚至单个物品[14]。这里的研究方向是智能标签，可以记录和报告冲击，倾斜，温度，湿度和压力等运输条件[15]。这里的关键驱动因素是低成本，并且可以同时有效地与数百或数千个标签进行通信。

物联网技术正在对娱乐，餐饮，公共交通，体育和健身，电信，制造业，酒店，教育，环境科学，机器人和零售等广泛行业产生破坏性影响。在许多这些行业中，物联网正在成为创新和成功的关键推动力，行业愿意投资新技术。可以向员工或外部提供商提供专业IT支持，以确保其系统的安全性和可用性足以满足其业务需求。

物联网和智能家居

本文讨论的是一个非常不同的环境 - 智能家居。当智能电子设备作为新建住宅的一部分时，可能会提供专业的系统设计，安装和设置。但是，在大多数情况下，智能家居物联网技术可能会根据需要逐个改装到现有的家中。在智能家居的物联网部署设计或运营阶段，通常没有持续的专业支持。虽然有一些相当普遍的专用智能家居标准，例如X.10电力线载波通信，但这些标准缺乏任何类型的安全性，并且是在这些家庭控制网络连接到互联网之前设计的[16]。现在有许多网络标准可以用于家庭（Zwave，Insteon，蓝牙，Zigbee，以太网，Wifi，RS232，RS485，C-bus，UPB，KNX，EnOcean，Thread）[17]。每个企业都有自己的优势和劣势，并期望具有许多不同协议的异构网络能够由非专家进行高效安全的管理，这带来了重大挑战。

智能家居可能提供额外的舒适性和安全性，以及增强的生态可持续性。例如，智能空调系统可以使用各种家用传感器和基于网络的数据源来做出明智的操作决策，而不是简单的手动或固定时间表控制方案。智能空调系统可以通过跟踪位置数据预测房屋的预期占用情况，以确保空调在房屋被占用时达到所需的舒适水平，并在没有空调时节省能源。

除了增强舒适性之外，智能家居还可以帮助老年人独立生活。智能家居可以协助日常工作，如清洁，烹饪，购物和洗衣。智能家居系统可以支持低水平的认知衰退，以及时提醒

用药。家庭健康监测可以指示护理人员在需要昂贵且破坏性的住院治疗之前做出反应[11]。但是，如果智能家居系统不安全且值得信赖，则这些好处可能都不会被采用。

4.安全威胁在智能家居

4.1。威胁

尽管智能家居是一个非常不同的环境，但安全威胁的整体性质与其他领域相似。

保密威胁是那些导致不必要的敏感信息发布的威胁。例如，家庭监控系统中的机密违规可能会导致敏感医疗数据的无意释放。即使看起来无害的数据，如家庭内部温度，以及空调系统运行参数的知识，也可以用来确定房屋是否被占用，作为爆窃的先兆。诸如密钥和密码之类的机密信息的丢失将导致未经授权的系统访问威胁。

身份验证威胁可能会导致传感或控制信息被篡改。例如，未经身份验证的系统状态警报可能会使房屋管制员认为存在紧急情况，并打开门窗以允许紧急出口，实际上允许非法入境。稍后会提出的一个问题是自动化软件更新 - 如果这些问题没有经过适当的验证，则可能会出现问题。

访问威胁可能是最大的威胁。未经授权访问系统控制器（特别是在管理员级别）会使整个系统不安全。这可能是通过不恰当的密码和密钥管理，或者可能是未经授权的设备连接到网络。即使无法获得控制权，未授权的网络连接也会窃取网络带宽，或导致合法用户拒绝服务。由于许多智能家居设备可能以电池供电并以低运行工作周期进行无线联网，因此用请求淹没网络可能导致能量消耗攻击 - 一种拒绝服务形式。

4.2。漏洞

网络系统可访问性是一个重大漏洞。由于现代智能家居系统连接到互联网，因此可以通过直接访问网络控制接口或将恶意软件下载到设备来进行远程攻击。

系统物理可访问性也是一个问题。对于无线和电力线载波技术，即使房屋本身安全锁定，也可以从房子外部物理访问网络。

下一个漏洞是受限制的系统资源。设备控制器传统上是小型8位微控制器，其计算和存储资源非常有限，限制了它们实现复杂安全算法的能力。

系统异构性是一个漏洞。设备来自许多制造商，具有不同的网络标准和不同的软件更新功能。通常这些设备几乎没有关于其内部软件，操作系统和已安装的安全机制的文档。

固定固件是另一个问题。很少有智能家电提供任何常规软件更新服务来修补安全漏洞。有人怀疑，目前没有什么动力持续补丁软件，以保持花费数美元的设备的安全漏洞。

标准缓慢采用是一个漏洞。尽管一些专有系统（如健康监测子系统）可能具有设计良好的符合标准的安全性，但大多数当前智能家居设备实施的安全方法（如果有的话）很少。

我们认为最大的漏洞是缺乏专门的安全专家，他们可以管理智能家庭网络的复杂性。很少户主可以负担专业的持续家庭网络管理协助。相反，业余户主需要能够简单，安全和可靠地自行管理他们的系统。

4.3。漏洞举例

由于其低成本，物联网计算设备通常不像传统桌面那样强大

举个例子，一个家庭户可能会认为他们的网络摄像头只能被那些用户访问

和笔记本电脑。大多数物联网设备都是低能耗的，使用低端微控制器并具有

已经被赋予其主机名和端口号。但是，借助Internet设备扫描

有限的记忆。这些控制器与独立控制器的要求非常匹配

搜索引擎如Shodan（https://www.shodan.io）[18]和Censys（https://censys.io）[19]，洗衣机或空调。

合法搜索可访问的传感器，许多设备突然知道和可见。传统的搜索引擎，例如Google和Bing，通过检索网页并按照这些网页中的超链接来索引网页，图片或一些流行的文件类型来爬网。另一方面，互联网设备扫描搜索引擎像网络扫描仪一样工作，扫描互联网节点的开放端口并索引连接设备返回的标题或横幅信息;答复的标题或横幅通常包括设备类型，型号，供应商，固件版本和其他信息。除HTTP和HTTPS协议外，Internet设备扫描搜索引擎还使用各种协议（FTP，SSH，DNS，SIP和RTSP等）连接到节点的开放端口。为了方便访问，这些搜索引擎还提供应用程序编程接口（API）以编程方式访问其搜索结果。攻击者可以利用这些搜索引擎在互联网上找到易受攻击的设备。例如，使用搜索关键字

Shodan的“has\_screenshot：true port：554”将返回一个家庭监控摄像机列表，其IP地址，地理位置和屏幕截图如图1所示。

5.一些现有的安全支持

由于其低成本，物联网计算设备通常不像传统桌面那样强大

和笔记本电脑。大多数物联网设备都是低能耗的，使用低端微控制器并具有

有限的记忆。这种控制器与a中的独立控制器的要求非常匹配

洗衣机或空调。

信息2016,7,44 7 of 16然而，这些特性使得联网的物联网控制器向更多的方向发展

因为现有的互联网协议通常不是为这些嵌入式设备设计的。

已经创建了几个互联网工程任务组（IETF）工作组来解决这些问题

已经创建了几个互联网工程任务组（IETF）工作组来解决这些问题

问题。 IETF对IoT的标准化工作在该项目的建立中发挥了至关重要的作用

问题。 IETF关于物联网的标准化工作在确立必要的方面发挥了至关重要的作用

必要的轻量级通信协议用于现有IP上的受限环境

轻量级通信协议，用于现有IP网络上的受限环境。

网络。这些包括基于低功耗无线个人区域网络的IPv6（6LoWPAN：RFC

这些包括基于低功耗无线个域网的IPv6（6LoWPAN：RFC 6282）[20]，6282）[20]，用于低功耗和有损网络的IPv6路由协议（RPL：RFC 6550）[21]和

用于低功耗和有损网络的IPv6路由协议（RPL：RFC 6550）[21]和约束约束应用协议（CoAP：RFC 7252）[22]。图2显示了之间的比较

应用协议（CoAP：RFC 7252）[22]。图2显示了IETF IoT和IETF IoT与TCP / IP协议栈之间的比较。一旦设备连接到互联网，任何安全

TCP / IP协议栈。一旦设备连接到互联网，任何安全威胁

互联网上的威胁也可能危及物联网的安全和隐私。在下面的

互联网也可能危及物联网的安全和隐私。在接下来的部分我们会回顾

我们将回顾这些标准IoT协议的当前安全实现。

这些标准IoT协议的当前安全实现。

5.1。 6LoWPAN和安全

图2. IETF IoT和TCPIP协议栈之间的比较图2. IETF IoT和TCPIP协议栈之间的比较

电气和电子工程师协会（IEEE）已经定义了802.15.4标准

电气和电子工程师协会（IEEE）定义了802.15.4标准

无线个人区域网络（WPAN）。 IEEE 802.15.4定义了物理和媒体访问的方式

用于无线个人区域网络（WPAN）。 IEEE 802.15.4定义了物理和媒体

控制层应该在低带宽，低成本，低速度和低能量下运行

接入控制层应该在低带宽，低成本，低速度和低能耗的情况下运行

这些网络的典型条件。因此，6LoWPAN [23]是一个轻量级协议，由其设计

这些网络的典型条件。因此，6LoWPAN [23]是IETF设计的一种轻量级协议，允许IPv6数据包通过IEEE 802.15.4无线网络传输。互联网协议安全（IPsec）套件定义了认证头（AH）和封装安全性负载（ESP）为IPv6数据包提供数据完整性，机密性，原始身份验证和防重放保护。文献[24]中的作者提出了针对6LoWPAN实现IPsec的压缩AH和ESP特性，从而为无线设备之间提供端到端的安全通信。

针对6LoWPAN网络（EAKES6Lo）的增强认证和密钥建立方案已由作者在[25]中提出。 EAKES6Lo分为两个阶段来提高6LoWPAN网络的安全性。这两个阶段是：（1）系统设置;和（2）认证和密钥建立。在阶段1中，对称加密机制高级加密标准（AES）用于加密网络中的数据传输。为了验证数据的完整性，采用散列函数消息摘要算法5（MD5）或安全散列算法（SHA）。在阶段2中，将交换六个消息以完成认证和密钥建立过程并建立相互认证。

因此，6lowPAN为安全的无线通信提供了一个模板，即使对资源有限的设备也是如此。

5.2。 RPL和安全

路由协议是传统网络的核心组件，这也适用于6LoWPAN网络。 RPL [21]是由IETF设计的一种优化的IPv6路由协议，特别适用于低功耗和有损网络（LLN），主要由6LoWPAN网络使用。 RPL是一种距离矢量路由协议，其映射拓扑结构基于面向目标的有向无环图（DODAG）结构。在[26]中已经提出了一种称为用于RPL的信任锚互连环路（TRAIL）的通用拓扑认证方案。 TRAIL可以通过发现和隔离伪造节点来阻止伪造节点的拓扑不一致性攻击。 TRAIL已经使用往返消息验证向根节点的向上路径完整性，并帮助树中的节点获得真实的等级信息。 TRAIL的创新之处在于树中的每个节点都可以验证其到达根的上行路径并检测任何伪排名攻击。

在DODAG树中，节点必须选择正确的父节点，因为除根之外的每个节点都必须有父节点。 RPL等级用于描述树状拓扑中节点的位置。在[27]中，作者提出了一个安全的选择方案来帮助孩子节点选择一个真实的父节点。在其选择算法中，节点的阈值将根据来自其邻居节点的平均和最大秩值来计算，以排除欺骗节点成为其父节点。

所以现有解决方案可以确保智能家庭网络中的安全路由表生成。

5.3。 CoAP和安全

CoAP [22]是一个类似于HTTP的应用层协议，专为受限设备网络而设计。由于IoT网络中存在诸如群组通信等特殊要求，因此CoAP提供了HTTP不具备的组播支持。为了更好地适应低带宽连接和低计算能力设备环境，CoAP采用用户数据报协议（UDP）协议。与其对应的传输控制协议（TCP）相比，UDP是一种更简单，低延迟和无连接的传输层协议。 CoAP是一种无状态协议，基于客户机 - 服务器体系结构模型。它使用请求/响应式操作在客户端和服务器之间交换消息。与HTTP类似，CoAP还基于表示性状态转移（REST）模型，其中服务器上的每个资源都有自己的统一资源标识符（URI），客户端可以通过向服务器发出请求来访问资源，而请求可以是以下四种方法之一：GET，POST，PUT和DELETE。

目前，传输层安全性（TLS：RFC 5246）[28]是HTTP的主要加密协议，但TLS的实现对资源有限的物联网设备过于复杂。为保证通信安全，CoAP采用数据报传输层安全（DTLS：RFC 6347）[29]作为其安全协议。 DTLS提供与TLS提供的相同的安全服务。 TLS和DTLS的主要区别在于TLS基于TCP协议，而DTLS基于UDP协议。 CoAP规范定义了四种不同的安全模式。设备可以处于四种安全模式之一：NoSec，PreSharedKey，RawPublicKey和Certificate。

IETF标准再一次为受约束网络内安全的基于网络的通信提供了安全机制。

5.4。未来的物联网安全指示

如上述三个例子所示，目前已经开展了重要的工作来确保关键任务物联网应用的安全。开发适合资源受限设备并使用最新安全技术的IP兼容安全通信网络已经付出了很多努力。然而，这些技术中的许多技术都需要谨慎统一的全系统设计，并需要有经验的网络工程师来设计和维护安全的物联网系统。我们工作的重点不在于这种“技术”安全方式，而在于智能家居安全的系统管理方面，即如何正确安装和维护这些强大工具所支持的安全性。

6. ASuitableSmartHomeArchitectureforSecurity

智能家居架构有许多不同的建议，其中每个建议都有特定的安全问题。三种最重要和最受欢迎的体系结构是中间件，云和网关体系结构。接下来的部分将探讨这些架构风格的安全问题和实现困难。

6.1。中间件体系结构和安全性

中间件是位于低层设备和高层应用层之间的软件层。它通常提供一个通用接口和一个标准的数据交换结构来抽象硬件的复杂和各种底层细节。当中间件收到来自高层应用程序的请求时，它将高级标准化资源访问请求转换为相应的设备特定方法。当设备回应应用程序时，中间件处理低级方法和数据转换，然后将相关的抽象命令和数据发送回应用程序。应用程序不需要知道硬件不同实现的底层细节，只需调用中间件提供的命令和函数。安全和隐私保护应该在中间件的各个层次上考虑，从较低的硬件交互层次到较高的通用接口层次。

VIRTUS中间件[30]是基于开放式可扩展消息和呈现协议（XMPP）协议的中间件解决方案。它采用简单身份验证和安全层（SASL）协议进行身份验证，并采用传输层安全（TLS）进行数据安全和隐私保护。

面向嵌入式对等系统的安全中间件（SMEPP）[31]是一个专注于在智能节点之间提供点对点安全通信的中间件。在设备可以与其他人通信之前，它需要通过提供有效的证书来加入一个组。有三种不同的安全级别，但只有级别1和级别2占用安全机制。 SMEPP在级别1下实施预共享密钥加密，在级别2下实施用于组许可的公钥加密。另一方面，SMEPP在级别1下采用认证，在级别2下采用加密方式进行认证，以保护数据安全。

虽然中间件已被广泛用于具有桌面级机器的公司系统中以管理复杂的异构网络，但目前提出的物联网中间件解决方案需要大量额外的复杂软件层和加密程序，以在既没有存储器也没有计算能力的设备上实现他们。除了性能问题之外，中间件体系结构的另一个问题是开发人员无意中引入的中间件编码缺陷可能会对物联网设备构成安全威胁。所以我们拒绝中间件解决方案，目前许多物联网设备是不可行的。

6.2。云架构和安全

设备之间的协作是物联网的一个重要方面。这种可互操作的功能需要大多数物联网设备所不具备的高处理能力。为了解决物联网设备的性能问题，研究人员为物联网提出了基于云的解决方案。云有资源来监视，收集，存储和处理来自物联网设备的数据。通过分析这些数据，云可以根据用户定义的策略触发操作，以实现复杂的智能家居控制。物联网的云架构也被称为物联网（CoT）。

[32]中的作者提出了一个基于IETF的CoAP协议的物联网云架构[22]。该架构由三个解耦阶段组成，这三个阶段是网络，协议和业务逻辑阶段。每个阶段都包括传入事件队列，线程池和处理阶段逻辑的事件处理程序。这种体系结构将轻量级DTLS [29]用作其身份验证和通信的安全协议。

在[33]中已经介绍了基于云计算的家庭区域网络（HAN）的安全方案。家庭管理系统（HMS）管理设备和策略，并为用户提供接入点。在本文中，作者在云中实施HMS功能，HMS与云服务接口。该方案使用对称密钥加密来应用端对端通信之间的机密性，并为每个智能对象分配一个唯一密钥。

基于云计算的解决方案消除了对独立家庭控制器的需求，并为物联网提供了连接和协作的良好方式;然而，它取代了对需要大量互联网通信的本地计算的需求。由于物联网的资源有限性，物联网设备生成的大量原始数据必须传输到云端而无需预处理;因此，家中的设备需要高速，低延迟，永远在线的互联网连接，但这种始终在线的高速互联网连接并不总是可用的，尤其是在农村或偏远地区。控制延迟增加，特别是如果服务器在海外或网络拥塞。

所有设备都必须能够通过互联网访问，因为互联网提供了广泛的攻击面，每个设备都需要足够的资源来实现完整的网络安全协议。以限制访问更广泛的互联网为目标的拒绝服务攻击，或偶尔的网络中断可能导致家庭医疗和物理安全系统等任务关键型任务失败。此外，由于用户不能完全控制其云服务，他们必须信任云提供商为其数据实施适当且充分的安全措施，但情况并非总是如此。

由于基于云的系统在没有永远在线的网络连接的情况下发生故障，我们不相信他们能够自己提供安全可用的智能家居系统，而且他们还将所有网络设备暴露给网络攻击。

6.3。网关架构

物联网网关是一个相对资源丰富的网络处理器，与其他物联网终端在同一LAN上工作。它不仅可以成为处理物联网设备协调的中心管理点，还可以提高不同制造商的智能设备之间的互连性和互操作性。此外，它可以充当连接本地物联网基础设施与云的桥梁。由于网关拥有更多的计算能力和资源，高计算和内存丰富的任务可以从物联网设备卸载到网关。在安全方面，网关可以集中用户身份验证并应用访问控制，以防止未经授权的访问或修改受限制的数据。它还充当防火墙，保护智能设备和隐私免受网络威胁，并减少攻击面。

在文献[34]中，作者提出了一种集成接入网关（IAGW）架构，通过智能家居环境的标准接口来支持各种应用节点。该体系结构包括无处不在的传感器网络层，网络层和服务层。 IAGW包含一个安全模块来实现认证，授权和加密。这种架构的好处之一是它具有服务质量（QoS）模块，为流量分配优先级并为关键任务操作保证资源。

一种称为基于服务器的物联网架构（SBIOTA）[35]的系统概念是提议的网关服务器，为物联网提供有效，高效，安全和合作的集成解决方案。这种概念架构在网关上包含一项新颖的自动配置服务，以促进设备的部署和管理过程，从而使设备可以插入网络并在该网络上以最少的手动配置完全正常工作。其最初的方法是网关和设备之间的身份验证和通信通过单独的网络端口或物理上与服务器相邻的短距天线进行。在将设备连接到网络之前，用户需要将它们放置在与网关物理接近的地方进行身份验证并交换相关信息，以确保只有合法设备才能连接到网络。

网关可以在功能强大的处理器上实施复杂的管理算法，并且可以运行关键的智能家居功能。即使在临时缺少互联网连接的情况下，它也可以为物联网设备提供复杂的防火墙和代理支持，从而使他们对直接网络攻击的暴露程度最小，并且可以在没有复杂中间件的情况下与资源受限的物联网设备配合工作。因此，这是我们首选的智能家居架构。

7. FutureSmartHomeSecurityChallenges

我们的研究目前正在研究基于网关的智能家居体系结构所需的两项增强功能，以使其足以保证广泛采用。我们的工作仍处于早期阶段，所以我们将问题和整体系统架构作为迈向解决方案的第一步。

7.1。自动配置支持

预计越来越多的智能家电将与智能家居网络相互连接。缺乏技术支持是家庭环境中最大的挑战。在家庭网络中添加和管理这些智能设备可能会造成重大的安全风险，因此，家庭成员将承担繁琐，重复且容易出错的手动任务。因此，为了成功实施智能家居，应该进一步研究安全的自动配置方法，不仅要简化智能家居设备的安装和维护，还要增强自动配置过程的安全性。

我们的方法需要网关和基于云的服务的功能。当新设备连接到网络时，网关将使用设备ID来询问可信的Web服务，以发现设备的细节 - 它的功能是什么，它的命令是什么，它理解什么加密和网络协议，以及任何现在可用的基本固件更新。这是大多数自动配置方法的一种不同方法，这些方法需要将大量信息存储在设备本身上，并且设备能够实现深度协议栈。使用我们的方法，简单的设备ID和Web服务可确保此信息易于获取并保持最新状态。

图3显示了典型的网络架构以及启动此自动配置所需的一系列步骤。

7.2。物联网软件和固件更新

随着安全漏洞被识别和修补，桌面操作系统会定期自动更新。智能手机等移动设备也会定期收到软件更新，其中包括验证更改真实性的机制。这样的系统在经济上是可行的，因为操作系统变体和操作系统制造商的数量很少，并且部署的设备数以百万计。数百种不同的物联网设备没有这种定期更新服务。

物联网设备是硬件和软件的组合，可执行特定的专用任务。固件是一种被编程到智能设备的非易失性存储器中的软件。它是任何物联网系统的重要组成部分，因为固件是直接与硬件接口，控制系统操作和功能，从初始化设备，与用户交互，处理请求和执行任务的程序。因此，智能设备固件保持最新以解决安全漏洞，改进功能，添加新功能并修复其他错误至关重要。与拥有专门的IT部门或技术团队来管理和部署软件更新的企业级环境不同，智能家居环境通常缺乏技术支持。智能家居的物联网设备应具有自动实施安全和可靠固件更新的机制，很少或不需要用户干预。这种功能可以由家庭网关管理。

为确保更新的完整性和真实性，并防止可能的固件篡改（例如恶意软件注入），应对更新应用基于证书的数字签名。在更新之前，每次更新都必须根据其数字签名进行验证，并且应检查数字证书以确保其有效并由供应商或受信任的第三方签发。用于下载新更新的方法也需要仔细考虑。如果更新检查机制遭到破坏，黑客可能会阻止安装新更新并对未修补的固件执行攻击。攻击者还可能将具有安全漏洞的合法旧版固件伪装为最新版本，导致固件恢复为错误版本。因此，设备供应商或制造商应该对更新的版本信息进行加密和数字签名，而不会给网络犯罪分子提供干扰更新版本维护流程的机会。由于许多智能设备的带宽和资源有限，delta更新大大提高了效率并缩短了安装任务时间，因为增量更新只包含已更改的数据。这可以显着减少更新失败的可能性，特别是对于电池供电的设备而言，由于在耗时的固件升级过程中电池电量耗尽。

文献[36]中的作者提出了一种新的适用于物联网设备的软件更新机制，称为物联网架构（GITAR）的通用扩展，可应用于现有的物联网操作系统。根据作者的说法，这种架构能够使用标准的文件结构，工具和方法在运行时为协议和应用程序应用部分代码更新（增量更新）。该体系结构包括三个级别：静态系统级别，动态组件级别和内核级别。核心操作系统组件和硬件驱动程序在系统级执行。为了提高软件可移植性，系统级分为硬件抽象（HAL）和硬件接口（HIL）层。系统级别的静态代码只能通过升级整个固件来更新。与系统级别相反，应用程序和网络协议组件在组件级别运行，组件级别的代码非常灵活，这意味着可以动态更新此代码，而不是替换整个固件。内核级别是系统和组件级别之间的接口。它将动态组件绑定到另一个以及系统功能。作者已经在流行的开源IoT操作系统Contiki中展示了他们的方法，而不需要对现有网络协议和应用程序中的源代码进行重大修改。

我们提出的方法，类似于自动配置，依赖于两个关键组件。第一个是作为基于网络的服务实施的。制造商或受信任的第三方（在自动配置过程中确定）保留最新版本的软件和固件，可将其推送到自动配置过程中识别的网关。网络服务可以区分操作系统中的漏洞或特定的设备应用程序代码，也可以下载补丁程序。网关在本地管理更新过程。网关可以在本地方便的时候自动安排这些更新。如果更新安装导致网关进行更新软件的自动测试时意外丢失功能，网关还可以管理回滚信息的更新。网关还可以自动响应关键漏洞，例如阻止网络访问不安全的设备，直到有补丁可用。

8.结论

物联网并不是一个单一的应用领域，国内智能家居应用中使用的安全方法与行业或公用事业中的关键任务应用所提供的安全方法完全不同。一个特别的问题是，网络的安全性取决于大部分未经培训的员工的安装和配置。这使得有效的安全策略和机制难以开发，实施，执行和维护，除非这可以自动完成。网络服务支持智能家居网关架构，用于自动设备和网络配置以及自动系统更新，这是我们解决这些问题的首选方法。

致谢：这项工作得到了昆士兰大学信息技术和电气工程学院的支持。

作者贡献：林慧珍研究并撰写了第2,4,7章。 Neil Bergmann编写了第1,3和8部分，并为其他部分提供了编辑支持。两位作者都阅读并批准了最终稿件。

利益冲突：作者声明不存在利益冲突。