Article:
Kirkham, T, Armstrong, D, Djemame, K et al. (1 more author) (2014) Risk driven Smart Home resource management using cloud services. Future Generation Computer Systems, 38. 13 - 22. ISSN 0167-739X

https://doi.org/10.1016/j.future.2013.08.006

Risk Driven Smart Home Resource Management Using Cloud Services

Thomas Kirkham, Django Armstrong, Karim Djemame, Ming Jiang

University of Leeds, Leeds, UK

Abstract

In order to fully exploit the concept of the Smart Home, challenges associated with multiple device management in consumer facing applications have to be addressed. Specific to this is the management of resource usage in the home via the improved utilisation of devices, this is achieved by integration with the wider environment they operate in. The traditional model of the isolated device no longer applies, the future home will be connected with services provided by third parties ranging from supermarkets to domestic appliance manufacturers. In order to achieve this risk based integrated device management and contextualization is explored in this paper based on the cloud computing model. We produce an architecture and evaluate risk models to assist in this management of devices from a security, privacy and resource management perspective. We later propose and expansion on the risk based approach to wider data sharing between the home and external services using the key indicators of TREC (Trust, Risk, Eco-efficiency and Cost). The paper contributes to Smart Home research by defining how Cloud service management principles of risk and contextualization for virtual machines can produce solutions to emerging challenges facing a new generation of Smart Home devices.

Keywords:Internet of things; Smart Home, risk, web services

1. Introduction

In the next decade users will be able to get information through the web from most devices in the home. Embedded web services (internet of things) are set to drastically change how we manage our resources in the home environment from the management of consumable goods to energy consumption. The future home will consist of multiple services linked to physical devices or resource monitors. A natural step in the management of these services is integration along the lines of specific applications or business models. Integration of services in this form aligns the future domain of the Smart Home with current challenges facing the Cloud computing community [2].

Likely applications in the home domain will be focused on the improved use of resources. For example, users will benefit from services to better manage their energy consumption and to improve the use of consumables in the home. The application of smart metering technology shares home data with distributed services in order to monitor energy consumption in order to improve eco-efficiency. Research in this domain is leading to the development of home control panel / dashboard technology for individual users and methods to share home energy data with suppliers and other parties interested in eco-efficiency in communities [1].

To date very little research has been conducted around service based management of home resource utilisation. This paper aims to explore the potential of such an approach using risk based integration of home devices in multiple application scenarios linked into a wider Cloud based network of services. The risk assessments are formed by user input and shape the monitoring and integration of devices in the network aiding Smart Home management for both resource consumption and device control.

The paper structure starts with a background section that describes the concept of the Smart Home and the need for input into the management of services. Moving on, the paper then introduces the use cases and then the risk models for improved resource use. This is followed by an evaluation of the risk models and a discussion section focusing on the initial results of the application of the models and the contextualisaton of devices. The paper ends with future work and conclusion.

2. Background

Smart Home is the term given to the application of ubiquitous computing technology into the home environment. The creation of a Smart home environment can embrace a wide range of technologies and is best summarized in research terms within the category of the Internet of Things [3]. The common feature of the Smart Home is the creation of a network of devices that is capable of supporting communication to and from home appliances. Within this domain, research focus can be further separated into device specific categories such as home security, appliance management, digital entertainment, energy management and assistive computing / health care [4].

In terms of research effort the assisted living / health care in the home domain is a well-researched area of work. In this domain the research effort is driven by the cost benefits of remote health provision and constant patient monitoring in the home. However common technologies for assisted living tend to be application specific and the integration of the technologies is often non-standard [5]. This is because many assisted living applications pre-date web services and are designed in vendor specific or application focused environments dominated by specific vendors or procedures set by specific health care providers.

The adoption of wider standards in terms of the Smart Home as in many other domains is linked to the emergence of standards based networking technology and the internet. A good example can be seen in research and applications of Radio Frequency Identification (RFID) technology with the expansion of wireless networks [6]. The integration of home devices depends on the direct adoption of open standards or integration of legacy systems to gateways or services that support open standards such as available in the web services community [7]. Web services not only present standards for local integration but also allow distributed services to integrate with web service enabled devices present on the internet.

Enablement of Web Services at device level is directly linked to the ongoing increase of power in embedded processors driven by demand in devices such as Mobile Phones. Improved processing at device level and the development of standards and technology to aid Mobile device integration with the internet is significant for the Smart Home. Web Service toolkits and groupings of standards such as the Devices Profile for Web Services (DPWS), enable web services to be present on more powerful embedded devices [8]. Direct integration with devices via web services is significant as it removes the need for gateways to bridge technologies allowing direct communication with devices, this also enables standards based integration with web based applications outside of the domain of the home [9]. Thus no local hubs or servers are needed with devices connected directly over the internet. Future applications for the web integration of Smart Home devices range from ideas linked to social network integration of home appliances to the intelligent remote management of devices within Smart Grids [10,11]. In effect the devices in the home become services in wider Smart Home clouds. This remote integration is cited to have the potential to create a new domain of consumer facing computing applications and associated services. But, initial attempts at the compulsory adoption of home based devices have created problems in particularly with respect to data privacy. A good example of such issues can be seen in the domain for Smart Metering. In the Netherlands the government intended to make a compulsory roll out of meters as part of a national energy reduction plan, but this was curbed when privacy issues were raised [12]. The scheme is now voluntary and the issues of recording of device level data in the home can be seen to raise other privacy and trust risks for consumers[28].

The potential of device level services to leverage Smart Home integration with third party services depends on the level of support and protection offered to users. To help solve this problem the user needs to be presented with application processes and data sharing risks that they can understand. One approach to this is via the use of user defined risk assessment based service integration. This approach can be both linked to user preferences and embedded in the data sharing that embraces the Smart Home applications.

3. Use Case

The use case is concerned with how a user can better use resources in his or her home. Typical improvements would deliver lower costs by improved energy and resource consumption in the home. The use case also includes the scenario where an organisation is responsible for the management of multiple homes. This could be in the case of smart meters provided by an energy company, or in the case of domestic appliances the party could be a property maintenance company. To demonstrate how resource can be improved in the context of a single or multiple homes we demonstrate this by focusing on the use of resources by one common appliance. The appliance chosen is a

washing machine. This choice was made because large amounts of test data exist for this type of appliance and the process of washing clothes involves multiple resources from energy, water and washing powder.

The key characteristics of a washing machine are broken into six assessment categories of energy consumption, appliance reliability, water usage, noise, usability and cost. Using these categories the user performs a risk assessment based on his or her preferences in terms of category weighting. The results of this helps the user choose the appropriate machine.

Once the machine is chosen monitored device contextualisation can take place to deploy specific service types on the machine to suit different application environments. When the machine is being used data transmission takes place using this embedded web service device to send data in to external monitoring services. The user sets preferences for the management of the machine in terms of the wider home including:

- Terms on which to automatically reorder stocks of washing powder linked to best cost efficiency. Linked to supermarket costs and offer fluctuation.
- Energy management of resources such as water and electricity, linked to external costs of resources and energy consumption thresholds.
- Appliance maintenance in terms of when specific items need a deep clean or mechanical service. Linked to usage data.
- Management of the application is linked to requirements set by the user.
- Wider settings in relation to data security and privacy.

Risk management underpins the device, service and user relationships. Risk is associated with all data sharing transactions and agreements reached with third parties to share data, in all cases the security and privacy requirements of the user are taken into account. Risk is calculated from the user requirements set at the beginning of the process and also includes real time need from the environment (for example running low on washing powder). This risk then forms the basis on which third parties are engaged within the application requirements.

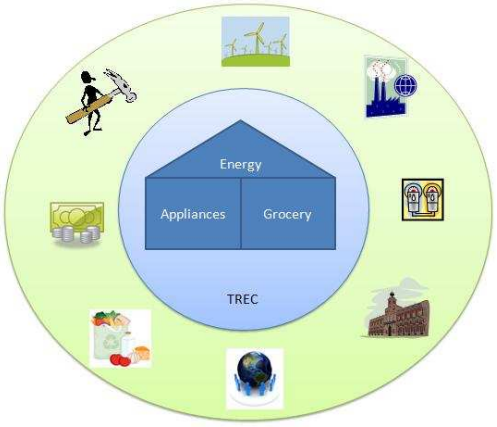

Figure1: Smart Home Use Case

Figure 1 illustrates the types of services provided by third parties that we expect to interact with our home data summarized into Energy, Appliances and Grocery data. Working clockwise from the top the energy company (windmill) would be interested in the energy consumption data for billing; the factory would receive information about appliance usage in order to add knowledge to the monitoring of devices to prevent failure. The metering of resource consumption including energy by meters and waste by bin sensors can be aggregated in one source and presented to government for compliance monitoring or shared online with other users to find best deals. Groceries can be ordered online when prices and supplies at home reach a specific level and banking data for the resident can be used to automate payments and calculate cost thresholds. Finally the maintenance man can be contacted automatically for repairs and servicing of appliances in the home.

4. Architecture

4.1 Overview

The implementation architecture involves the creation of direct communication between device level services and third party services. This communication is monitored and managed by a central service that acts on behalf of the user (the Smart Home Management service (SHM)). Third party services are bound into the framework via the use of Service Level Agreements (SLA). To suit the application environment, integration with third party services and the SLA we envisage the use of contextualisation services to tailor the web services present on the device before run time. These services mirror current contextualisaton in Cloud computing environments. Risks associated with service failure or SLA breach are monitored during operation of the appliance and all architectural blocks can be seen in Figure 2.

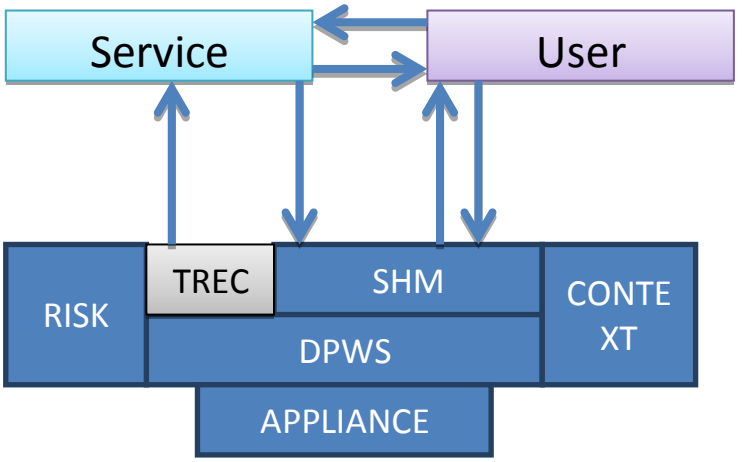

Figure 2: Architecture

As the architecture illustrates the Device Profile for Web Services (DPWS) services link directly to the Risk, Contextualisation and SHM components. The TREC block is the data output from the services linked to the devices which goes directly to the third party services. These third party services communicate with the user and are managed in terms of security and membership by the SHM service.

4.1 Service Management

As illustrated the device level services in the implementation architecture use the DPWS toolkit to present data to other services. The DPWS toolkit supports the following web service standards WSDL 1.1, XML Schema, SOAP 1.2, WS-Addressing, and further comprises WS-MetadataExchange, WS-Transfer, WS-Policy, WS-Security, WS-Discovery and WS-Eventing [13]. The implementation uses the WS-Eventing standard to transfer messages from device level. This creates a pro-active messaging implementation that embraces the publish-subscribe messaging methodology.

The messages from device level go directly to subscribed services. Subscription is achieved via a central SHM that provides authentication and authorization for the requests and also distributes the shared key for transport level security in the system. The model of subscription can be seen in Figure 3.

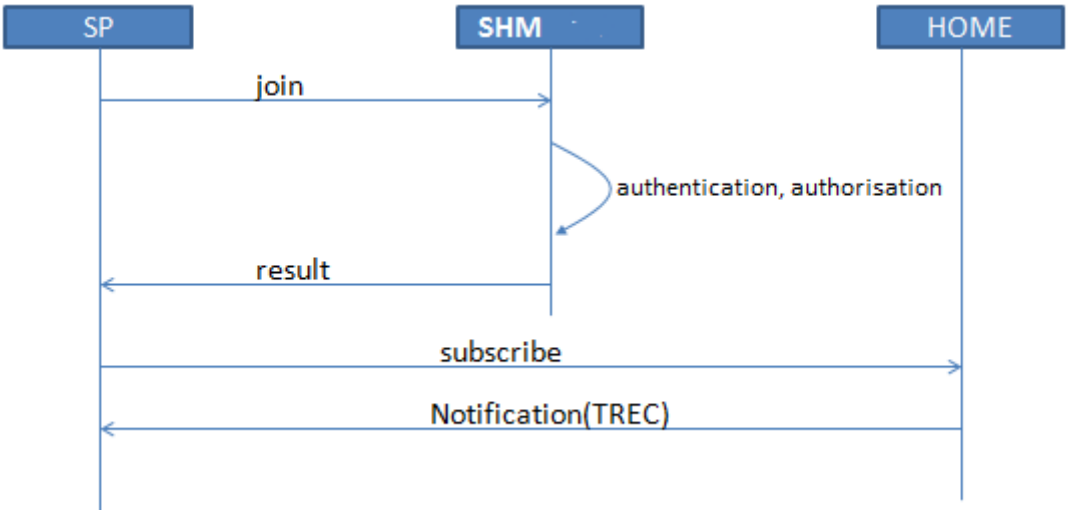

Figure 3: Service Provider enrollment

As Figure 3 illustrates the central Smart Home service is referred to as the SHM service, apart from security and access the key function of the service is manage devices to ensure improved resource use in the home. Two main interfaces are presented by the service; one for the user / resident of the home and the other is for the third party services. The interface for the user (user side) is where the user sets security / privacy controls of data release and also selects the applications which will run on the network of services. The Service Provider (SP) side is used for SP joining of the network. As mentioned previously the data is sent directly to successfully subscribed service provider side services. The SHM service also receives the messages from the devices for monitoring purposes and can disconnect external services from receiving messages. Certain messages received by the SP will be further encrypted in order to protect privacy and the decryption of this data is done by further authorization by the SHM service on request from the third party receiver.

4.2 Service Contextualisaton

Prior to service execution service contextualisation can take place. Smart devices in the home need to be self-aware of the context in which they are used and the environment that surrounds them. We look to manage the integration of third party services with devices but also to enable devices to be reconfigured to suit specific environments. In cloud environments in particular a device needs to be primed with a given configuration for its surrounds after deployment. Our previous work has defined the process of giving cloud services an identity as "contextualization" [20], where a service can be deployed to self-configure as it comes online. In the smart home matters are complicated further by the heterogeneous nature of device hardware, where by unified software solution is difficult to develop and maintain as new device enter the market.

We envisage a potential solution to the problem of ensuring that a device performs to a predefined Quality of Service (QoS), through the application of a hardware agnostic contextualization. This step involves the deployment of a specific service instance onto the device in order to configure smart devices using sensory input from the environment as well as by bootstrapping to other devices in the vicinity. An example washing machine that could use this would deploy taking into account water alkalinity, mineral content and later after deployment usage patterns. This could have an impact on the environmental footprint and running costs of the device. Figure 4 shows how context data could be gathered from multiple sources to provide a smart device with an contextualised configuration.

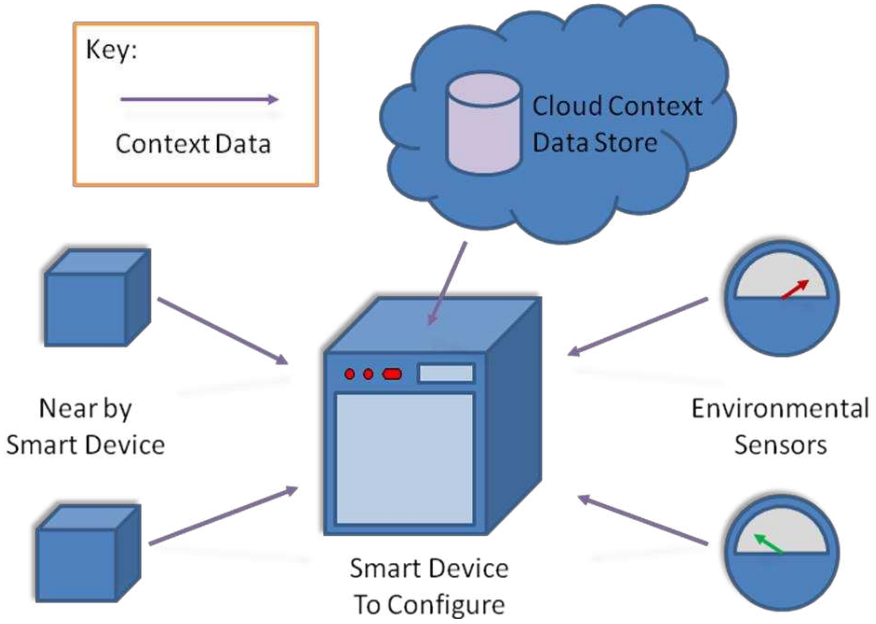

Figure 4. Contextualization of a smart device

We have shown that the contextualizing of a software service can be achieved with minimal overhead [25] and the use of contextualization to aid device management is a key element of our approach. When the device level services are executed they form part of a composite application with the goal to improve overall home resource consumption. Guiding this at application level is the management of risk in terms of failure to deliver specific application goals, this will be explored in more detail in the implementation section.

4.3 Risk Based Application Management

Risk spans all data sharing relationships in the implementation and is the cornerstone to the management to the applications we envisage in our Smart Home. Risk is initially calculated based on user input from the SHM service. Risk is inferred from asset data related to cost, eco-efficiency in the Smart Home or data sharing with third parties. The SLA between the SHM and the SP on behalf of the user is the first use of risk and the SLA formed is used to underpin live risk assessments of data sharing in the framework. External integration with components is based upon negotiated SLA, and is monitored using both third party services and policy enforcement points around specific shared data objects. The SLA negotiation can be seen in Figure 5.

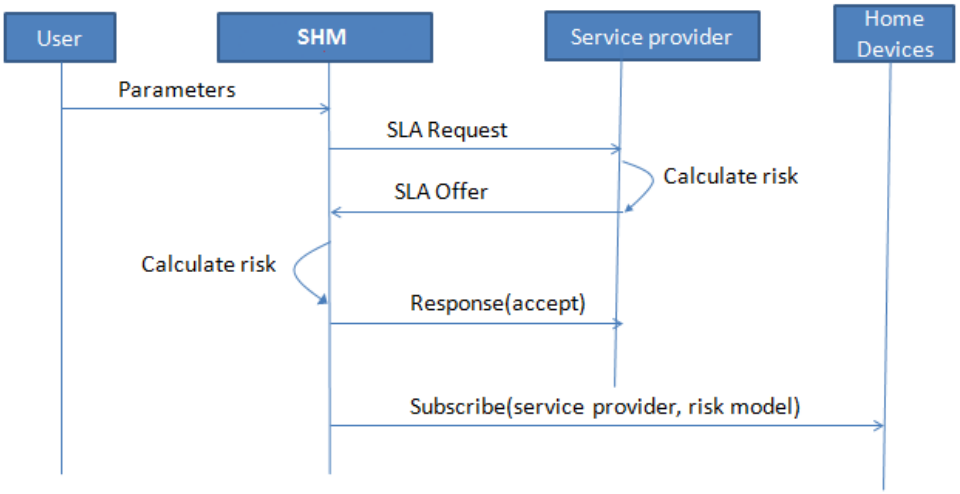

Figure 5: Risk based service management

The SLA Offer is legally binding from the sender so if the offer is accepted and this is notified to the party who offered it the contact is complete. Once the SLA is agreed this is translated back into a risk model which is deployed at the device level. Thus all data released to specific service providers fits within the user defined and SHM negotiated risk model. The SLA is enforced by the SHM based on third party monitoring of services and the service interaction with devices in the home.

When the device is in operation risk is managed at two points in the architecture. The first is the SHM service, and here risk is calculated to aid the initial SLA negotiation for new service providers and also for the monitoring of this SLA during device level communication by third party service providers. The second of the risk points occurs at at the device level service. Figure 6 illustrates how the device level services interact with risk assessment.

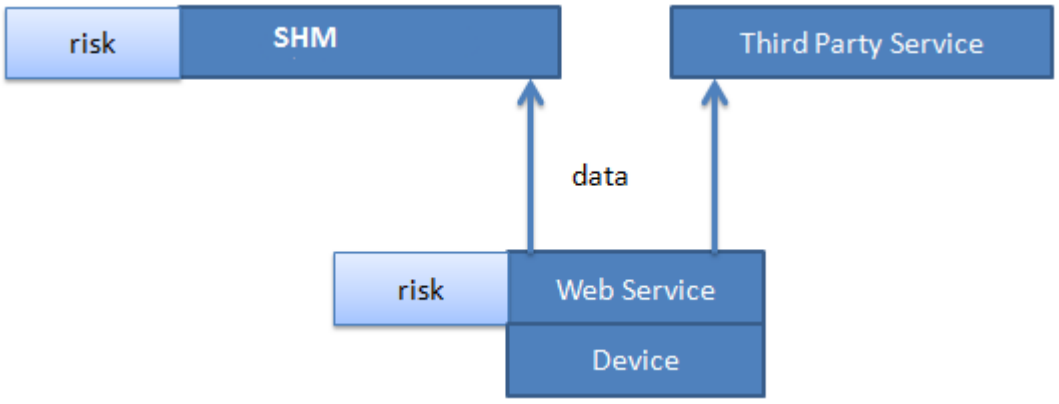

Figure 6: Risk positioning and device integration

Risk calculation at device level acts as a safety gauge for the devices. Although risk is also managed at the wider SHM service level, live data is not checked by the SHM and sent direct from the device to third party services. In some cases this data maybe sensitive and a risk assessment at device level could ensure that this data is checked and not shared. Such a case could be to transfer energy consumption weekly rather than in real time in order to disguise when the house is empty or occupied.

5. Risk Models

We calculate risk in terms of legal risk, appliance failure risk and resource security risk. The three were chosen to fit the use case. The legal risk model underpins the security in the framework ensuring data remains private and used in the right contexts. The failure model presents the risk associated with the device breaking the agreed SLA and resource security risk models link the use of the device with external threats. All risk assessments share a common risk inventory where risks and events are recorded.

5.1. Legal Risk

The legal risk model underpins the implementation and is concerned with data sharing and legal compliance of the service provider in terms of privacy legislation and wider data processing law. Threats to the expansion of applications built on Smart Meter data have already illustrated that privacy concerns can set back application development and technology adoption. Legal and privacy issues have been adopted at design level and embedded into the core data sharing activities.

In the implementation we have focused on the location of the service provider to determine legal risk and the need to get consent from the user. The need for consent is in line with emerging EU data processing law designed to protect user's privacy and the location data will help determine compliance with this. For example some locations offer similar levels of protection with schemes such as Safe Harbor in the USA being designed as a bridge to EU data protection law.

During data sharing between devices and service providers the SHM monitors the legal risk using a rule-based risk model. The rule based approach mirrors existing use of policy in web service frameworks [27]. This is chosen as any finer grained legal approach would require the development of specialist domain knowledge and legal tooling, such tools would allow the comparison of laws to make automated legal decisions that is beyond the scope of this implementation. The rule based approach allows certain threats to be detected, when found an alert is triggered concerning the particular threat in the risk inventory. For example, the threat of data moving to a location that is in breach of the user requirements or local legal rules that will cause failure of the SLA will be detected by the monitoring of service provider location data. While monitoring the service provider the rule-based model will repeatedly fire the following rule:

```
If (location == 'unknown_ip_address') then
        Check risk inventory where "Asset==Data", Output "Impact Level of Risk"
```

The levels of risk are set by the user at the SHM level and in cases of increased risk the user can be notified in order to take action, or the SHM can act on behalf of the user. Either way a decision can be made on which mitigation strategy should be employed, whether to accept the risk or prevent data transfer to the service, if the impact level is too high.

5.2 Appliance Failure Risk

Application failure risk is concerned with elements of the environment that may cause the wider Smart Home applications to breach the SLA. In this scenario we use real appliance data which users weight in terms of priority. For each appliance this data is then ranked. We can get this data from integration with the appliance manufacturers and other shared user data.

The risk is calculated using the following functions. Given the Time To Fail (TTF) of an appliance is Weibull distribution, and its Probability Density Function (PDF) as in [28]:

$$f(t) = \frac{\alpha}{\lambda}\left(\frac{t}{\lambda}\right)^{\alpha-1} e^{-\left(\frac{t}{\lambda}\right)^{\alpha}}$$

Where, α is the shape parameter (or slop) and λ is the scale parameter; its Cumulative Density Function (CDF):

$$F(t) = 1 - e^{-\left(\frac{t}{\lambda}\right)^{\alpha}}$$

Hence, the Probability of Failure (PoF) of an appliance in future time x, given it has been used until time t:

$$PoF = P\{X \leq t + x | t\} = \frac{(t+x) - F(t)}{1 - F(t)} = 1 - e\frac{t^{\alpha} - (t+x)^{\alpha}}{\lambda^{\alpha}}$$

The α and λ parameters of Weibull distribution can be estimated by using the standard Maximum Likelihood Estimation (MLE) algorithm.

Historical data of appliance failures (i.e time durations) is collected by the SHM and assessed using the functions in order to provide a risk assessment (RA), as further information comes in from sources such as community sources an update is performed on α and λ parameters. This data includes changes in factors such as appliance reliability from updated figures from the data source that feeds the risk assessment.

The risk assessment is used when the appliances are in use in the home so the PoF of a physical host in future time service x can help the resident with servicing planning and third party supplier with greater information on their product lifecycle.

5.3 Resource Security Risk

Resource security is concerned with possible threats to the leakage of resources to both rogue service providers and malfunctioning devices. In addition the resource security is focused on cost management in the system and that resource consumption does not threaten both eco-efficiency and cost goals set in the environment. The user is presented with a series of options to rank risk associated with threats to resources.

- Cost change (cost fluctuation in products)
- Reduction in service reliability (ability for the service to complete tasks)
- Loss of service reputation (gathered from third party sources such as social network)
- Service unavailability (technical downtime of service)
- Service non-compliance (certification of service provider in terms of compliance with third party security audit schemes.

Table 1: Security Risk

Based on this information, resource security risk can be calculated as:

Security_risk_deployment(usecase)
1. Calculate the number of threats recorded at deployment stage and usecase 2. For each threat: a. probability (likelihood given asset affected) (p(B|A)) = likelihood/ 5.0 b. probability (asset priority)(p(A)) = priority/5.0 c. probability (likelihood regardless of asset) (p(B))= p(B|A) * p(A) + p(A') *1 d. probability of threat occurring (p(A|B)) = ((p(B|A) * p(A))) / p(B) 3. Resource security risk = Sum all probabilities of threats occurring / threats found

We choose to base our security calculations using probabilities of the risk occurring. This probability depends on up to date information on security threats and information on the chances of these threats occurring. It is envisaged that a key source of this information would be from logs of service providers and devices in the Smart Home

ecosystem. We chose to range likelihood and priority from 1-5 with 5 being the highest priority / most likely. To make the assessments more accurate data shared from other external sources would also be of use to increase the sample size and to include any possible latest threats to be used for the calculations of threat probability.

Information regarding the risk criteria is taken by the SHM before the service is subscribed to the home devices. Thus, based on the rules of Bayesian dependencies, the probability of each threat affecting the particular device assets can be calculated before decision are made as to whether to accept the service subscription or not.

At the operation stage, along with the calculated resource security risk for this stage, the risk assessment will be interacting with sources of information that present live data on subscribed services like reputation services from third parties. Depending on the value of relative risk, the SHM or device level services can make a decision whether to accept or apply a mitigation strategy stored in both the devices and SHM to compensate for the risk.

6. Evaluation

Using the risk models described in the previous section we have taken real data and produced risk assessments in line with the use case.

6.1 Application Failure

We determine application failure as influenced by multiple factors listed in table 1. We have taken scores collated for individual devices from Which? (Which.co.uk) who have tested and scored over 200 washing machines available on the UK market. Which? is a product testing and consumer campaigning UK charity. The scores for categories within this data is already broken down between 1-5. For all scores we calculate the likelihood based on the POF calculations in the previous sections. For our three types of washing machine the scores are listed below.

Table2: Machine Ratings and User Weightings

Measure	machine1	machine2	machine3	User Importance weighting
Energy	0.8	0.8	0.8	9
reliability	0.6	1	0.6	5
Water	0.8	0.8	0.8	6
Noise	0.4	0.8	0.4	2
usability	0.6	0.8	0.8	4
cleaning	0.8	0.8	0.8	7

The results can be seen in Figure 7 below.

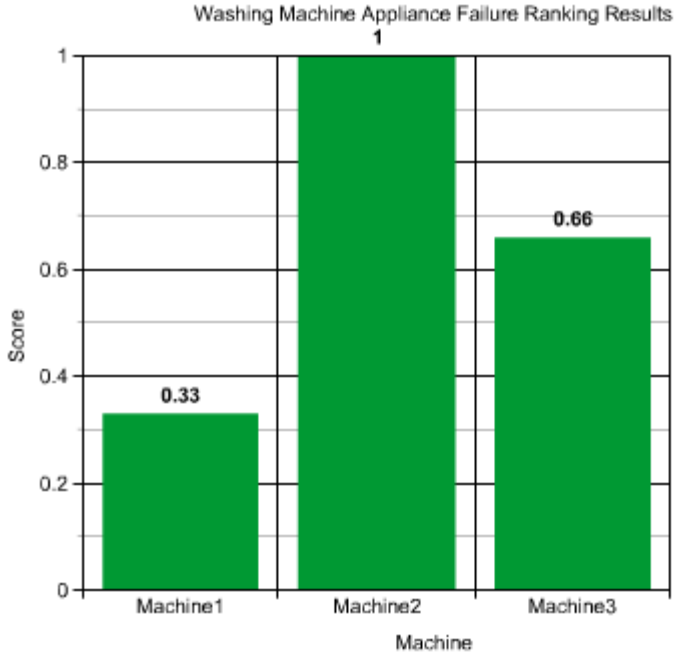

Figure 7: Washing Machine Failure Ranking

The output of this initial risk assessment influences the choice of machine by the user. Depending on the weighting the choice could relate to the purchase of new equipment or to establish the best time of day to run a machine for example what scores best when the Noise measure is the highest. For a large organisation running multiple machines the ranking could help determine the most effective use of a organisations equipment. Eitherway once chosen the risk is constantly monitored using TREC and any changes in TREC will affect the scores that the machine has for the factors and thus trigger a change in score on future risk assessments.

6.2 Security of Resources

Breaches in device security are another source of application failure. For the deployment of the security model we are using three factors to assess the risk. The table is split between the likelihood statistics and user ranked priority associated with the category. First is listed theft of the device, secondly we list malfunction of device and finally human error as a cause for device failure. The priority scores are taken from user input. For the likelihood scores we take data from two sources. For theft we take the crime data listed for the postcode where the device is located, this data is then checked against the freely available UK crime statistics on the Police.uk portal (www.police.uk). We break these statistics down to a ranking of 1-5 based on the average UK crime levels sitting at 3 and the two scores below and above evenly distributed. The Malfunction data and Human Error data is taken from Which as in the previous risk assessment.

The inputs for the security risk based on the postcode NG197SX are illustrated below:

Table 3: Security Risk Table

	Priority	Likelihood
Theft	4	2
Malfunction	2	1
Human error	1	3

The results of the security risk assessment can be seen in bar chart below:

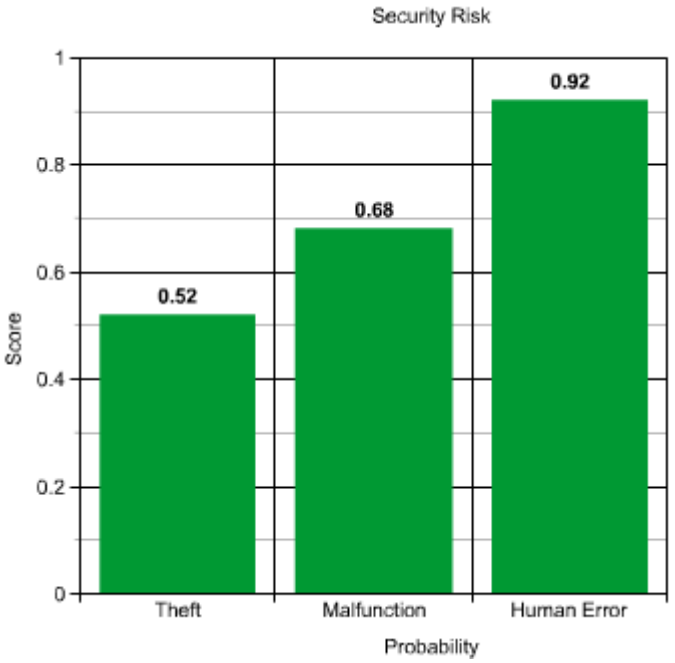

Figure 8: Security Risk Results

The probabilities denote the total security risk based on crime data and user weighting to be 0.7067. It is up to the household to accept the service being offered depending on this probability for security risks. If the household does accept it, it can then monitor this probability by keeping track if the probability goes up depending on the occurrence of events expressed in TREC data from service providers, which increase the likelihood of the threats. If the probability goes up, the household can decide to mitigate the threat by calling external help or chose to accept it for itself.

6.3 Contextualisation

.

In order to test contextualisation we have ported the environment to the Cloud, this is because we don't have any reconfigurable devices yet developed. The tests we ran are designed to confirm that the contextualisation of devices adds minimal overhead on operation. The tests involved the contextualisation and deployment of 1 service on a device, 5 services and 10 services across devices. The time taken for these deployments was recorded and can be seen in Figure 9 below.

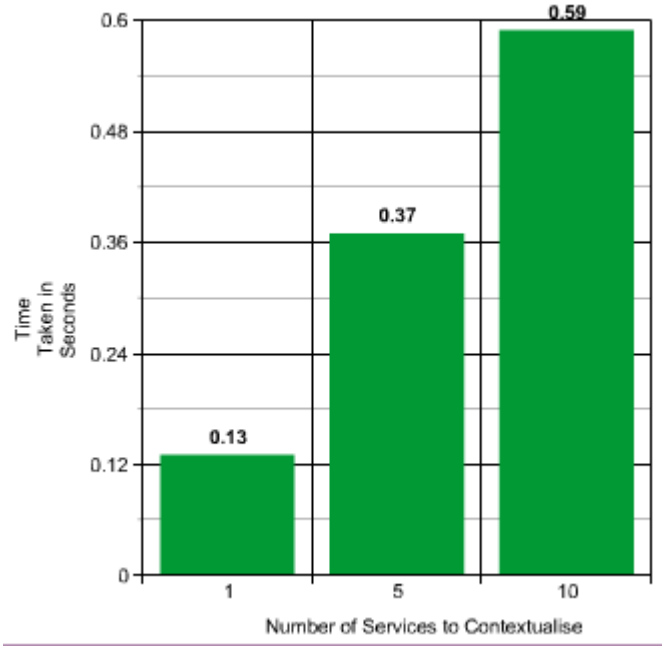

Figure 9: Contextualisation Results

The contextualisaton approach we used involves the deployment of the operating system to the device with the service as part of this setup. The deployment of the operating system is an approach from the cloud where machines are virtualised and new machines are effectively new deployments of operating systems. The table illustrates the average additional execution time (over 10 iterations) taken to configure the operating system and associated software dependencies of a number of cloud platform services during boot time, running within a cloud resource (Virtual Machine). The contextualization process has little impact when compared to the time it can take to provision a service's virtual cloud resources, which is often in the order of several minutes. Thus extrapolating from these results we predict a similar overhead will be obtainable for the software stack of smart devices in the home and will not have an effect on their operation or usage.

7. Discussion

7.1 Smart Home and the Cloud

Smart home implementations using web services will embrace Cloud technology. This is because not only are services increasingly being presented in cloud computing environments but the cloud provides the ability for application specific environments to be created from third party services to suit specific processing needs. For improved home resource consumption this type of remote processing and also knowledge management holds real potential.

The architecture in this paper demonstrates an innovative approach by which third party Cloud services can integrate directly with device level web services inside private homes. To support this we have introduced the SHM service and the provision of risk and contextualization tools. The architecture ensures that the user is well placed to manage both the risk in the environment and also communications with third party services. Security and privacy cross both risk management and traditional enforcement methods provided by the SHM.

The use of risk assessments both at device and SHM level enables user driven risk management of the Smart home environment. DPWS enabled devices and TREC integration presents the opportunity to manage devices in the home in real time. The risk assessments help ensure that data release and sharing from home devices is done in both the users and Smart Home applications best interests.

Contextualization of devices offers the potential to further enhance integration with the cloud and management of devices in the wider ecosystem. However, the tests so far have used a Cloud based contextualization involving the

deployment of operating systems. It is likely on the Smart Home we will just deploy contextualized services in to already established operating systems supporting reconfigurable web services. Although the time taken in comparison with the Cloud Virtual Machine approach may be similar but requires testing.

In terms of improved resource usage, the use cases illustrate that via the use of risk assessments decisions can be made at device and service level to improve the use of home resources. As web based services become more integrated and automated the concept of automated supply chain management in business is one such advance that could be applied in the home. Thus, the further developments of home services could lead to the concept of the home enterprise and a mirroring of business enterprise management applications such as Enterprise Resource Planning (ERP) for the home.

On the flip side of this approach, the data from the home can also further aid the utilization of resource usage in the enterprise too. In this case the usage data from appliances use case can aid manufacturers in the design and manufacture of products in sight of a full lifecycle of product data. This can improve both appliance efficiency and aid the manufacturer in terms of warranty and other forms of product support.

7.2 Wider TREC Usage

As mentioned at the beginning of the paper risk data is collected alongside other TREC data in the implementation. The development of wider risk management involves a holistic view on how the TREC factors complement each other.

With respect to trust, in our work we have looked at trust from a reputation perspective. Metrics to calculate trust of service or infrastructure in the project is taken from the behavior of the elements with respect to negotiated SLA. Thus poor quality of service leading to SLA breach is recorded and reflected in low trust scores for infrastructure or service providers. From a risk perspective the trust ranking can contribute to the calculations of risk in terms of probability of SLA failure for a party.

Eco-efficiency is calculated from two perspectives using energy monitoring meters in the home and data centre. The first is the raw energy efficiency of the home and the other is the eco-efficiency per unit of CO_2. Both calculations should be expanded to include the energy consumption of the wider cloud infrastructure supporting the home. Thus, the washing machine energy consumption should be combined in terms of calculation with the consumption of a percentage of the supporting physical infrastructure in the Cloud. The eco-efficiency is calculated using the electricity suppliers average CO_2 per unit of energy score.

In terms of cost the potential cost impact upon SLA failure is fed into the risk calculations. Also, cost is a key factor in the calculations of energy efficiency linked to risk. Thus, a risk could be a home that is costing too much in terms of energy to run. However, going back to eco-efficiency the cost like the CO2 output is also linked to choice of the supplier so one potential TREC driven impact could be the change of the electricity supplier to the Cloud or home.

8. Related Work

The domain of Smart Home or home automation is viewed as a key element of the future internet [14]. The implementation of the concept of the Smart Home has taken many approaches and embraced various technologies. From specific application driven implementations such as energy management in the Smart Metering community to more sensor based approaches focused on wider interaction with the home environment [15,16]. In some cases the application goals are similar but the implementation technology for the device level service differs, and can range from web service based technologies such as DPWS to more message orientated technologies like ZigBee [17,18]. Our choice to use DPWS was made simple by the core concept of the project of the need to integrate with a Web Service based cloud.

Improved resource usage in networks of services can be seen as routed in the Enterprise computing community around concepts of supply chain management [19]. Work in the cloud computing community is emerging on the contextualization of services from an appliance perspective via the deployment of resources to suit specific negotiated environments [20]. Within the Smart Home improved use of resources has largely looked at the issue of energy consumption in the home although interest exists with regards to the amount of waste produced in the home [21]. The latter work on waste however is largely linked to the concept of compliance of residents rather than

improving how the residents use their resources. The work discussed in this paper presents a possible new approach to such problems of consumption and waste in the home linked to targets and the risk associated with not meeting them.

Risk assessments in service based computing environments is an emerging area of research particularly around the management of service level agreements (SLA) in applications consisting of multiple services [22]. Here, work has largely focused on the relationship between the formation of SLA and risk, the need for the SLA to match the risk profile of the application and the risks in that it could break during service execution [23]. In the smart home the SLA is an important part of third party service provider integration but risk assessments are also needed to filter data release by devices to multiple service providers. This requirement is further enforced by emerging EU law for the protection of the privacy of the individual and the need for consent of personal data release [24] or where this is not possible some proof of accountability by the service provider, this can be provided by risk assessments at device level.

9. Future Work

The application of improved resource usage in the home environment needs more research in terms of integration with cloud based services and how current enterprise approaches can translate through to the home. To date no standard device interface exists for the establishment of web services on devices such as home appliances or remote contextualisation of these devices. Most home appliances are produced with no possible way of integrating them into a Smart Home environment. More work is needed in terms of platform standardization in order to create the stable environment in which exploit device level services.

In terms of risk management the link between the user, risk assessments and monitoring to date is application specific. In future applications consisting of multiple devices across various application domains the integration of risk calculation and the expression of risk are in need of more development. More investigation is also needed in the best ways to present risk assessments to non technical users and also how to communicate risks to users when they occur.

The adoption of TREC is also limited to a small community but to date no other XML standards exist to aid device and cloud integration, official standardization effort is needed to encourage the adoption of TREC as both a standard and principle. More sources of data that is needed for the probabilistic risk assessments as in the resource security and appliance failure assessments need to be identified. Any future Smart Home applications that embrace risk need good sources of data in order to evaluate risk in domains such as device security. This applies to all TREC factors and is vital for any control of devices based on TREC data. The problem of quality data for decision making is not limited to the Smart Home as issues exist in the Cloud Community to establish repositories of Cloud risk data separate from general threats from internet computing.

10. Conclusion

Increasingly the home is no longer a private enclosed environment. The future home will consist of home based integrated networks of services that send data and take management from remote Cloud based networks of services. To support this model privacy of data and clear contracts of data sharing and usage are needed in the form of SLA and user notifications. Central to this relationship as explored by the use of TREC in the OPTIMIS project is the categorization of monitored data for management purposes. Using automated risk assessments linked to SLA and user / application requirements the Smart Home can get smarter.

Acknowledgements

This work has been partially supported by the EU within the 7th Framework Program under contract ICT-257115 - Optimized Infrastructure Services (OPTIMIS).

References

1. Parks, B. (2009). Home energy dashboards. Make: Technology on Your Own Time. 18, 48-51 http://makezine.com/18/dashboards/
2. IBM Whitepaper "A Smarter Home Enabled By Cloud Computing 2010 http://www.ibm.com/smarterplanet/global/files/uk__uk_en__cloud__a_smarter_home_enabled_by_cloud_computing.pdf?ca=content_body&met=uk_smarterplanet_cloud_computing_ideas&re=spc
3. N. Gershenfeld, R. Krikorian, D. Cohen, The internet of things, 1697 Scientific American 291 (4) (2004) 76–81.
4. T. Perumal, A.R. Ramli, C. Y. Leong, S. Mansor, and K. Samsudin, "Interoperability for Smart Home Environment Using Web Services", International Journal of Smart Home, vol. 2, no. 4, Oct. 2008, pp. 1-16.
5. Q. Wang, W. Shin, X. Liu, Z. Zeng, C. Oh, B. Al-Shebli, M. Caccamo, C. Gunter, E. Gunter, J. Hou, K. Karahalios, and L. Sha. I-Living: An open system architecture for assisted living. In Proceedings of the IEEE SMC, 2006.
6. E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, G. Borriello, Building the internet of things using RFID, IEEE Internet Computing 33 (3) (2009) 48–55, doi:10.1109/MIC.2009.52.
7. Aiello, M., Dustdar, S., 2008. Are our homes ready for services? A domotic infrastructure based on the web service stack. Pervasive and Mobile Computing 4 (4), 506–525.
8. André Bottaro, Eric Simon, Stéphane Seyvoz, Anne Gérodolle, "Dynamic Web Services on a Home Service Platform", 22nd International IEEE Conference on Advanced Information Networking and Applications (AINA-08), Okinawa, Japan, March 2008
9. Oliver Dohndorf, Jan Kruger, Heiko Krumm, Christoph Fiehe, Anna Litvina, Ingo Luck, and Franz-Josef Stewing. Towards the Web of Things: Using DPWS to bridge isolated OSGi platforms. In PerCom Workshops, pages 720{725. IEEE, 2010.
10. A. Kamilaris and A. Pitsillides. Social networking of the Smart Home. In IEEE 21st International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC 2010), September 2010.
11. Warmer, C., Kok, K., Karnouskos, S., Weidlich, A., Nestle, D.: Web services for integration of smart houses in the smart grid. In: Grid-Interop 2009. pp. 1{5 (2009)
12. S. McLaughlin, P. McDaniel, and D. Podkuiko, "Energy theft in the advanced metering infrastructure," in 4th International Workshop on Critical Information Infraestructures Security, 2009
13. OASIS page for DPWS http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01
14. Vincent Ricquebourg, David Menga, "The Smart Home Concept: our immediate future," E-Learning in Industrial Electronics, 1st IEEE International Conference, pp.23 – 28, 2006
15. H. Farhangi, "The path of the smart grid," IEEE Power Energy Mag., vol. 8, no. 1, pp. 18–28, Jan./Feb. 2010.
16. Cook, D.J., Youngblood, M., Heierman, E., Gopalratnam, K., Rao, S., Litvin, A., & Khawaja, F. (2003) MavHome: An agent-based smart home, in Proceedings of PerCom 2003, 521-524.
17. Para J., Hossain M.A., Uribarren A., Jacob E, Saddik A.E., Flexible smart home architecure using device profile for web services: a peer–to-peer approach. Int. J. of Smart Home, 2009, vol. 3, no. 2, pp.39-56
18. Osipov, M. (2008). Home Automation with ZigBee. The 8th International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking (NEW2AN) (pp. 263-270). St. Petersburg: Springer-Verlag.
19. Kelle, P. and Akbulut, A. (2005) 'The role of ERP tools in supply chain information sharing, cooperation, and cost optimisation', International Journal of Production Economics, Vols. 93–94, No. 8, pp.41–52.
20. Armstrong, K. Djemame, S. Nair, J. Tordsson, W. Ziegler, Towards a Contextualization Solution for Cloud Platform Services D Proceeding of the Third IEEE International Conference on Cloud Computing Technology and Science (CloudCom'2011), Athens, Greece, November 2011
21. M. Chetty, D. Tran, and R. E. Grinter. Getting to green: understanding resource consumption in the home. In UbiComp 2008.
22. Battré D, Birkenheuer G, Hovestadt M, Kao O, Voss K. Applying risk management to support SLA provisioning. The Eighth Cracow Grid Workshop, Academic Computer Center CYFRONET AGH, 2008.
23. K. Djemame, D. Armstrong, M. Kiran and M. Jiang, A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems,Cloud Computing 2011, Proceedings of the Second International Conference on Cloud Computing, GRIDs, and Virtualization
24. V. Reding "How Europe is dealing with online privacy" http://edition.cnn.com/2012/02/23/opinion/reding-europe/index.html 2012.
25. A.J. Ferrer, F. Hern´andez, J. Tordsson, E. Elmroth, C. Zsigri, R. Sirvent, J. Guitart, R.M. Badia, K. Djemame, W. Ziegler, T. Dimitrakos, S.K.Nair, G. Kousiouris, K. Konstanteli, T. Varvarigou, B. Hudzia, A. Kipp, S. Wesner, M. Corrales, N. Forg´o, T. Sharif, and C. Sheridan. OPTIMIS: a Holistic Approach to Cloud Service Provisioning. Future Generation Computer Systems
26. E. Yuan and J. Tong. Attribute based access control (ABAC): a new access control approach for service oriented architectures. Ottawa New Challenges for Access Control Workshop, April 2005.
27. Kiran, M., Jiang, M., Armstrong, D. & Djemame, K. 2011, Towards a Service Life Cycle-based Methodology for Risk Assessment in

Cloud Computing, International conference on Cloud and Green Computing (CGC 2011), Australia, December 2011.

28. Cuijpers, Colette, and Bert-Jaap Koops. "Het wetsvoorstel 'slimme meters': een privacytoets op basis van art. 8 EVRM." Universiteit van Tilburg (2008).