Towards NFC Payments using a Lightweight Architecture for the Web of Things

Tor-Morten Grønli[1], Pardis Pourghomi[2], Gheorghita Ghinea[1, 2]

[1]Norwegian School of IT, Oslo, Norway
tmg@nith.no

[2]Brunel University, London, UK
pardis.pourghomi@brunel.ac.uk,george.ghinea@brunel.ac.uk

Abstract. The Web (and Internet) of Things has seen the rapid emergence of new protocols and standards which provide for innovative models of interaction for applications. One such model fostered by the Web of Things ecosystem is that of contactless interaction between devices. Near Field Communication (NFC) technology is one such enabler of contactless interactions. Contactless technology for the Web of Things requires all parties to agree one common definition and implementation and, in this paper, we propose a new lightweight architecture for the Web of Things, based on RESTful approaches. We show how the proposed architecture supports the concept of a mobile wallet, enabling users to make secure payments employing NFC technology with their mobile devices. In so doing, we argue that the vision of the Web of Things is brought a step closer to fruition.

Keywords: NFC, Web of Things, Architecture, Lightweight, mobile wallet, contactless payments

adfa, p. 1, 2011.

1 Introduction

Users have long been accustomed to consuming services offered over the Internet using web browsers. However, with Apple and Google's launch of the smartphone era in 2007-8, users have also started to consume services and acquire vast amounts of information when they are on the move. This trend has grown exponentially since then, with smartphones dominating today's cell phone markets. A separate but related trend has been that of an increasing number of hitherto standalone devices and sensors now being endowed with wired/wireless connectivity. Together, these two have given rise to the Internet of Things (IoT), a global information network consisting of trillions of smart objects in the world we live in [1].

One of the enablers of the IoT is NFC technology. This technology is currently governed by the ISO/IEC 18092:2013 standard [2], which regulates the way two inductively coupled devices operating at 13.56 MHz can communicate through a Radio Frequency (RF) interface using a standardised transmission protocol. This contactless technology can be used as a short-range peer to peer communication method between any mobile device provided it is NFC-enabled via an appropriate chip.

Contactless technology for the IoT requires all parties to agree one common definition and implementation. Having different implementation of one technology blocks interoperability, confuses users and raises the market entry barrier for companies. The idea of having a technology in mobile phone allowing everybody to participate in the IoT will only work if tags, devices, readers and application work seamlessly together and if there is an open market for these components. To this end, in this paper, we propose a new lightweight architecture for the Web of Things (WoT), based on RESTful (REpresentational State Transfer) approaches. Taking the particular case of NFC-enabled mobile payments, we show how it supports the proposed architecture and that the WoT, rather than being a distant promise over the horizon, is indeed a component part of daily lives for an increasing number of consumers. This work, which is built on our previous work [3], has the following main contributions:

- ***Application of the light weight architecture [3] to NFC-enabled mobile payments:***
  NFC-based payment is believed to be one of the emerging areas in mobile commerce, but has been largely overlooked by current IoT/WoT research [4-11]. This, in spite of the fact that mobile phone providers have started to equip smart phones with NFC tags, which will greatly facilitate and improve on the current payment practice.
- ***Flexible, secure and personalized payment applications/transactions:***
  This work exploits cloud computing services in order to manage NFC payment applications. The potential outcome is to ensure flexible and secure management, personalization and ownership of the payment applications. Our proposed architecture supports intelligent profiling functions by managing customized information relevant to each user in certain environments, which updates the service offers and user profiles dynamically.

The rest of the paper is organised as follows. Sections 2 and 3 respectively describe the fundamental technologies and research challenges. The aim is to establish a rationale for the proposed approach. Section 4 presents the proposed architecture and section 5 illustrates an application scenario that's implemented within the proposed architecture. Section 6 introduces the case of NFC-based mobile payments, whilst Section 7 specifically looks at how the proposed architecture facilitates them. Section 8 then concludes the paper.

2 Web of Things – Basic Concepts and Technologies

This section describes the basic concepts and technologies, which can potentially be used to design and develop Web of Things applications.

2.2 Internet of Things

In its current guise, the IoT is dominated by machine-to-machine communication. Accordingly, application areas such as such as supply chain management [7], healthcare [8,9], and workplace support [10] have been identified; however, issues raised by the new infrastructure include managing and making sense of the massive amount of data generated [11,12], privacy and security [13,14], as well as user acceptance of an increasingly monitored and sensor-rich world [15], to name but a few.

The next big leap in the evolution of this communication infrastructure will be when machine to smart object communication is facilitated. The first step along this road is to create smart devices or enrich everyday objects with smart communication capabilities, laying the premises for a smart environment. Smart objects can be recognized by:

- Sensors to measure light, temperature, position etc.
- Information (data) persistence
- Communication capabilities
- Machine-to-Machine communication

IoT embeds intelligence in the components enabling communication, exchange of information, recommendations, make decisions and provide services. It represents a convergence of different visions emanating from its key stakeholders; accordingly [16] distinguished things-oriented, semantic-oriented, and Internet-oriented perspectives in the IoT's many guises. Although the IoT has gained significant research and industry interest, the key challenge is to make this widespread, commonly accepted and part of the global Internet. Currently, one such approach is described by Web of Things (WoT). WoT emerges from IoT and continues the vision of embedded technology and smart devices from IoT [17]. This is taken a step further by incorporating the use of standard web technologies and thereby reusing existing, well-accepted standards and practices such as HTTP, URI and REST.

Such RESTful technologies [18] have obvious advantages when compared against approaches based on the by now traditional Web Services Architecture (SOAP, WSDL, UDDI) – they are lightweight, loosely coupled, require relatively little comI resources and virtually no operating system support, and scale well. All of this means that one can embed tiny Web servers and, by using the REST architectural style (which is the same as that of the web, i.e. based on HTTP, URIs and HTML/XML) one can build scalable interaction models at the application layer [19, 20].

Thus, a scenario whereby smart objects on the Web start abstracting and describing their services using either XML or JSON (JavaScript Object Notation), which are both human and machine readable, can easily be envisaged. In so doing, such smart objects can be accessed and interacted with via Web browsers. Indeed, assuming a user with appropriate technological skills, there is no reason why such users cannot create mash-ups, combining real-world physical devices with virtual services made available over the Web – all combining towards a Web of Things [21, 22].

2.2 Cloud Computing

Cloud computing has received considerable attention in the software industry. It is an established architecture used for hosting services, virtual machines and web based applications. Cloud computing refers to the applications delivered as services over the Internet and the hardware and systems software in the data centres providing these services. The idea is built around an economy of scale, where the ultimate goal is to provide more resources, better scalability and flexibility for less money. Cloud computing indicates a movement away from computing as a product that is owned and towards computing as a service [23]. Service in this context is a concept that deals with the utilisation of reusable fine-grained components across a vendor's network. The cloud, as an open, distributed, resource-full platform, contains promising opportunities for creating a framework for wrapping WoT solutions. To this end Kovatsch et al. [24] propose, in analogy with the thin client concept, that of the thin server. Here tiny servers embedded on physical devices use RESTful approaches and export only their elementary functionality to application servers running application logic. Thereby separating the application logic from the firmware and devices can export their functionality without hosting application logic, which is all found on the cloud. Application development is thus completely decoupled from the embedded domain.

2.3 Cloud as backbone for WoT

There have been a considerable number of research efforts targeting IoT/WoT application areas, but the same cannot be said in respect of the infrastructure capable of supporting this vision. We believe that the cloud is ideally placed in this respect. Whilst the literature mostly treats the issue from a high-level perspective [25], in this paper we take the effort one step further and show a detailed implementation map of WoT characteristics to cloud features. By taking advantage of the event-based frame-

work named Node.js [26] we are provided with a framework intended for enabling applications to be scalable, concurrent and event based. This framework communicates asynchronously and non-blocking [26], which makes it suitable for new protocols and standards such as WebSocket and Server-Sent Events, which rely on having an open connection to the server. To this end, we use JSON, which enables the use of a shared format for expressing and transferring data between application endpoints/servers, reducing the need for custom formats. Further, Node.js facilitates for modern WoT application architecture, and we show in our proposed framework architecture how this can be applied in theory and practice to gain an advantage. The idea of using cloud computing within NFC ecosystem introduces a new layer towards managing stakeholders that are involved in the whole NFC ecosystem.

2.4 Near Field Communication (NFC) as a backbone for Cloud Payment

Having several parties involved in the NFC ecosystem with lack of standards to define their roles and accesses to NFC components and applications, companies are increasingly looking into use the cloud environment as a single entity. Cloud-based payment solution can help the adaption of NFC as it can be integrated with mobile architectures or downloadable applications for both retailers and customers. However, it might bring more openness towards the security of customer's credentials (e.g. bank account details) but it terms of flexibility and manageability, it makes the whole process much clearer and easier to handle.

Cloud computing introduces a new method of storing payment credentials which improves the manageability of the NFC ecosystem. Rather than having all the sensitive information in NFC handset, Cloud can store this information and transmit when required. When a client scans his NFC phone on merchants POS terminal, encrypted payment credentials are taken out from a virtual SE that is stored in the Cloud and transfer to the SE that is stored in the NFC handset. The purpose of having a SE in NFC handset is to provide temporary storage in order to store authentication assets. Examples of this approach include PayPal and PayCloud Mobile Wallet. Although in this approach, most of the concentration has been towards vendor gift cards however, the cloud-based approach is also feasible in open payment systems.

2.5 Cloud-based Mobile Payment

One of the major companies that operate a concept of cloud-based mobile payment is the implementation of Google Wallet from Google [27]. The communication between the mobile phone and the point of sale is carried out through NFC technology that transmits the payment details to a merchant's sale system. Customer credentials are not stored in the mobile phone rather they are stored in the cloud. The customer will have an account with Google Wallet, which includes the relevant registered credit/debit cards. Transaction operates in the form of a virtual prepaid MasterCard card

that transfers from Google Wallet into the merchant's sales system at the time of purchase. MasterPass [28] is a service that has been developed by MasterCard as an extended version of PayPass Wallet Services [29] that provides digital wallet service for safe and easy online shopping. MasterPass stores all the payment and shipping information in one central, secure location. The MasterPass service is comprised of three main parts, representing the wallet, the checkout process and extra-added beneficial services.

These models suggest the idea of using cloud computing in order to manage NFC payment applications, which results in flexible and secure management, personalization and ownership of the applications. We will detail how architecture can provide easy management of multiple users and delivers personalized contents to each user. It needs to supports intelligent profiling functions by managing customized information relevant to each user in certain environments that updates the service offers and user profiles dynamically. Depending on the mobile operators network's reception, deployment of this service takes around one minute and deployments can be scaled to any number of users.

In the next two sections, this will be further detailed when looking at application growth, interoperable communication and performance results.

3 Research Challenges

The future of WoT holds many promising ideas, and generates great research interest from researchers, businesses and industry. All application domains can benefit from WoT solutions and areas such as disaster prediction; smart homes; medical applications; transport systems; smart cities and security systems are some of the most common examples. Some of the possibilities and research challenges of the WoT and cloud computing are highlighted in the following table.

Web of Things requisite	Counterpoint in Cloud Computing
Dynamic demand of resources	Cloud elasticity
Real-time needs	Service Level Agreement and Quality of Service
Expected growth in application use	Scalability and infrastructure
Security of data	Cloud privacy and security elements
Open, interoperable communication	Cloud standards and architecture

Table 1: WoT and Cloud properties comparison

Other and related areas represent as well research challenges for WoT and commonly mentioned are identification of objects, sensing of environment, information ownership, continued absence of standards and security/privacy [30][31]. Although highly important and relevant, we would like to draw the attention to the somewhat less commonly discussed one level higher of abstraction. The application layer, which allows for the *use* of IoT data/information and which ties everything together in WoT solutions, will be the primarily focus. From the above descriptions of cloud, NFC and payment, issues of integration of financial institutions with mobile network operators as well as the integration of cloud with the same operators are raised. To be able to have WoT solutions incorporate the standards from these actors in a seamless manner to create novel applications needs to be investigated further.

From Table 1, we do see all properties as important, independent research issues with unique attributes, and we would like in this article to focus on how growth in application use and interoperable communication in the context of mobile NFC payment can be explained and exemplified in an WoT architecture. We focus on architectural issues, interoperability and growth as we do think they are of essential value and need to be in place for the technology to gain sufficient importance, adaptation and availability.

4 The Proposed Architecture

The architecture of the proposed framework is represented in Fig. 1. The architecture is multi-layered which includes*: Things Interface Layer, Things Management Layer, Things Service Layer,* and *User/Application Layer.* Each of the layers is briefly explained in the following sections.

4.1 Things Interface Layer (TIL)

This layer represents the interface of the proposed system to the physical devices (things), such as interfaces to CCTV camera, mobile phones, light bulbs and sensor devices. There are various tools that provide interfaces to physical devices. In the proposed architecture we make use of Arduino[1] in order to enable communication between the physical devices and the computer systems, to create an interactive environment for communication with (smart) objects. Arduino, a lightweight single-board microcontroller, is an open source electronics prototyping platform which offers interface for communicating with and collecting information from a variety of sensing devices.

[1] http://www.arduino.cc/

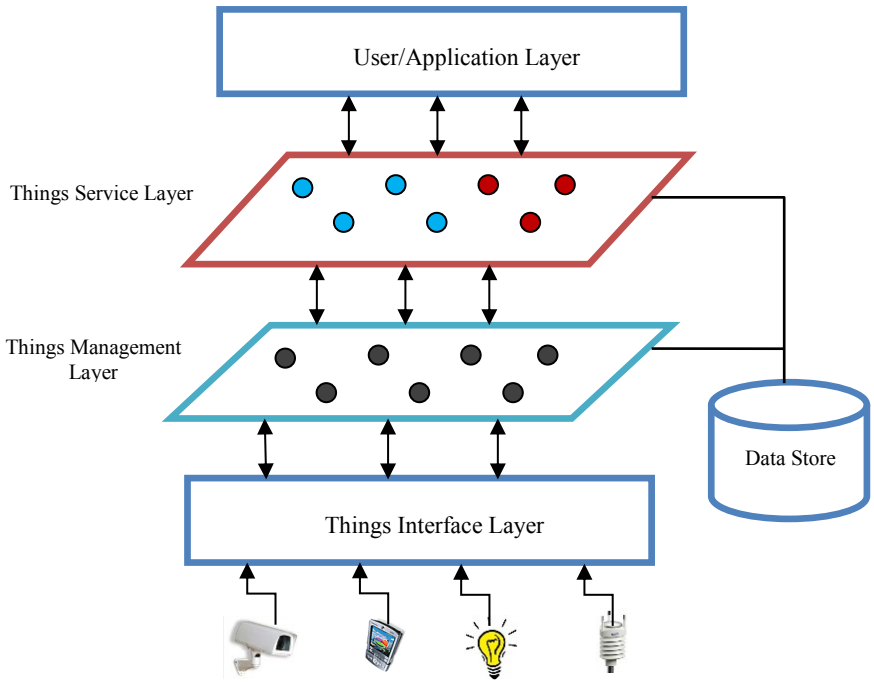

Fig. 1. Architecture of the Proposed Framework

4.2 Things Management Layer (TML)

This layer represents the devices at a higher level of abstraction. In other words, it abstracts the data and functionality of the devices into programmable components such as web services. In the proposed architecture, we exploit the RESTful architecture of web services in order to transparently represent the data and functionality of the physical devices and to hide their underlying complexity and low level details. RESTful architecture is more appropriate to the characteristic of the devices in WoT as it is lightweight and loosely coupled. We enable information exchange through the use of JSON structured data, and business logic is applied through common software engineering components.

4.3 Things Service Layer (TSL)

This layer processes the data and functionality of the devices represented as RESTful services. For instance, it interacts with the user layer and receives user requests in order to provide them with required services. Further, this layer can also collect information from the underlying devices and store in the data store using appropriate format and structure such as JSON or XML.

In addition to the RESTful approach, we suggest to employ Node.js [26] in the web components. Node.js implements an event-based framework for writing scalable and efficient Web applications using JavaScript. Node.js is based on non-blocking I/O calls and its light footprint makes it an excellent candidate for real-time, distributed and data-intensive applications. We argue that given the resource-scarcity of IoT devices, a lightweight web component and programming model is necessary to process and manage RESTful web services.

4.4 User/Application Layer (UAL)

This layer represents user applications that interact with the TSL in order to make requests and consume services. For example, user request can be checking the temperature of a given location or adjusting lights in a room or building. Communication will go through the web services described in the TSL and they can be accessed from virtually any web component, device and implementation language.

5 Conceptual WoT Scenario

In a vibrant city environment we are constantly overloaded with information from various sources. As more and more objects are becoming smart and interactive there are constant feeds trying to communicate with us. Such communication is often achieved through connection with our mobile devices. The mobile device can through Bluetooth, RFID and NFC be an integrated part of the environment, consuming information from nearby posters, bulletin boards or integrated sensors. They can actively push and pull information facilitating for, i.e., commercial displayed information on devices tailored accordingly to context, location and interests. In such an environment with potential information overload, the information acquired needs to be precise and tailored. Various forms of distribution or filtering of this information networks are available, but we take this one step further to propose a proactive model for this by using our proposed architecture framework (Fig 2).

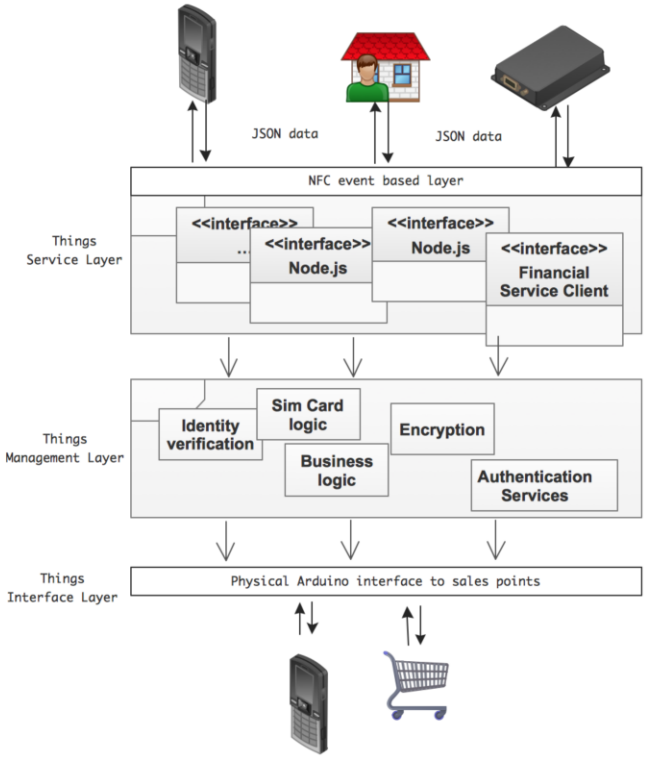

Fig. 2. Proposed Framework Architecture in Applied Scenario

By using this framework a user moving around in a city would end up with filtered, tailored and personally adapted information on his/her mobile device. General utilization could be: the customer needs to find the fastest route to a specific address; a recommendation for a particular shop to purchase the desired product from based on IoT information aligned with personal preferences; recommendation of shops to visit in order to fulfil the needs of the shopping list. Application usage and examples scenarios are numerous, but nevertheless it is important how this information is going to be made available. By applying a service, management and interface layer we provide three levels of abstractions allowing for service composition in each step. The physical Arduino devices will be wrapped in the interface layer, concealing all communication needed for physical IoT sensor access. Through the management layer business logic can be built and wrapped for access from the service layer. The service layer will then provide the physical IoT sensors available as services to end users/applications. This will then facilitate taking advantage of a modern event based architecture communication from Node.js.

We have taken some performance measurements in order to test the feasibility of our proposed approach. Thus, Fig. 3 and Fig. 4 show the comparative performance between Jetty, a traditional client server approach, and Node.js in terms of how scalable the two frameworks are in terms of concurrent requests. As can be easily ob-

served, an considerable increase in the number or concurrent requests, results in a much lower number of failed requests coupled with considerably lower CPU usage when the Node.js approach is used. Indeed, it is noteworthy to remark the relatively constant gap of around 80% in relative CPU usage between the traditional Jetty and the flexible Node.js implementation.

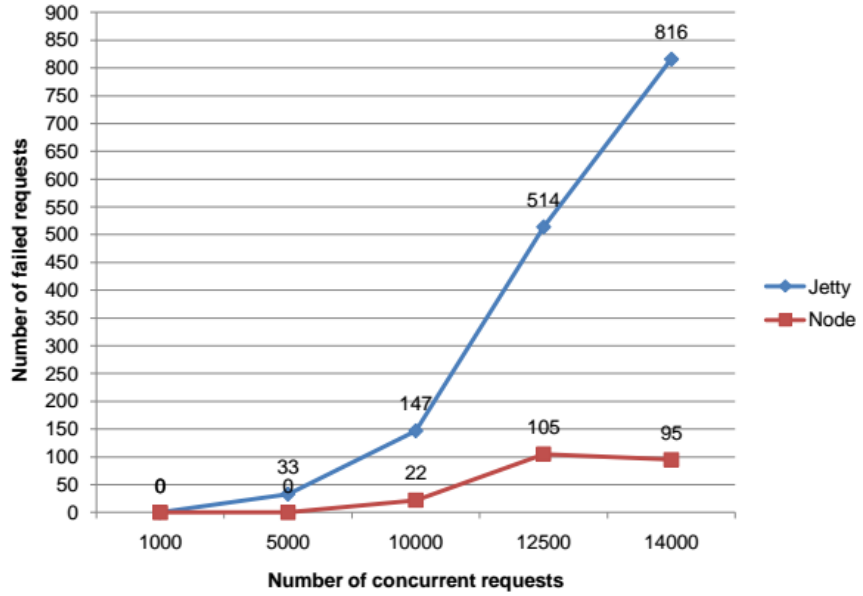

Fig. 3. Proposed Framework Architecture in Applied Scenario

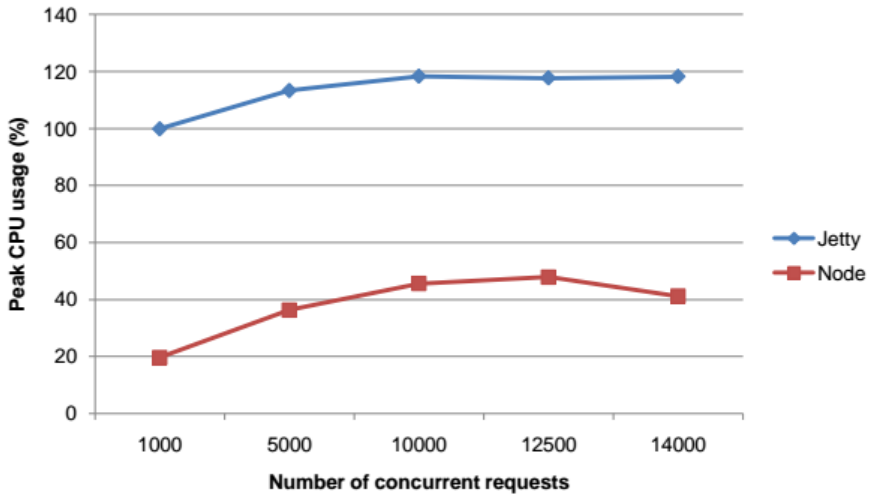

Fig. 4. Proposed Framework Architecture in Applied Scenario

6 The Proposed Scheme for NFC Payment

This section presents the proposed scheme for the NFC-enabled payment. It first describes the NFC payment case study, highlights the main challenges and illustrates the existing industrial solutions towards NFC payment. It then presents the proposed scheme that integrates the lightweight WoT architecture and cloud order to ensure flexible, secure and personalized NFC payment transactions.

6.1 Case NFC payment

Recently, mobile wallet and mobile payment concepts have become hot topics in developing industries and it seems that people have found it easy and convenient to pay with their mobile phones. Up to now, people seem to accept that the future is in mobile devices but the problem has just begun for industrial stakeholders. There are several unanswered questions regarding the method(s) that a mobile payment process should follow in order to be deployed in a satisfactory manner. One of the main concerns of stakeholders is bringing the idea of cloud computing into the concept of NFC payments. Challenges associated with choosing the correct solution as well as the right strategy for mobile payments [32] are issues open to be investigated. Thus, there is not much agreement in the minds of mobile wallet stakeholders. PayPal, Telefonica/O2, and Best Buy have announced wallets that are using cloud technology and they are classified as cloud wallets [33]. Additionally, Google, ISIS and Visa have developed solutions that are using NFC as the main technology and they are called wallets. We further investigate how Web of Things can help in this ambiguity and show how the scenario of mobile wallet maps to our proposed architecture.

6.2 Integration of WoT Architecture and Cloud in NFC Payment

The above scenario of NFC payment can be exemplified in our proposed architecture for Internet of things, by using cloud computing in order to manage NFC payment applications. This results in flexible and secure management, personalization and ownership of the applications. Our proposed architecture provides easy management of multiple users and delivers personalized contents to each user. It supports intelligent profiling functions by managing customized information relevant to each user in certain environments, which updates the service offers and user profiles dynamically. Depending on the network's reception, deployment of this service is low (minutes) and deployments can be scaled to a large number of users. We will further highlight how this solution maps to the different layers in our architecture.

Things Interface Layer

The communication between the shop sales point terminal and the mobile device is wireless using NFC technology. The mobile device has a valid SIM card and existing features from GSM network operator are applied for mutually authenticating the

MNO and the NFC phone. In practice, when a client scans his phone on the shop sales point terminal to make a payment, transaction credentials are transmitted from a temporary secure storage (e.g. NFC controller) in the device to the sales terminal. A NFC controller is responsible for handling the authentication between NFC phone and sales terminal.

Things Management Layer

When a mobile device signs into a network, the Mobile Network Operator first authenticates the device explicitly the SIM. The authentication stage verifies the identity and validity of the SIM and ensures that the subscriber has authorized access to the network. The Authentication Centre of the mobile network operator is responsible for authenticating each SIM that attempts to connect to the core network through Mobile Switching Centre. An authentication center stores two encryption algorithms, as well as a list of all subscribers' identity along with corresponding secret key.

When the NFC enabled phone sends a request to its cloud provider to get permission to make a payment, the cloud provider sends a SMS requesting a PIN number to identify the user of the phone - this is how cloud provider ensures the legitimacy of the phone user. For verification purposes, the customer sends the PIN back to the cloud provider as an SMS. This process in enabled by exploit the RESTful architecture of web services. Instead of low-level incorporation of core functionality, the architecture supports for ad hoc resources instead. This enables an abstraction from the implementation and the details given in the *Things Interface Layer* and it is possible to concentrate on security and application behaviour in this layer instead.

Things Service Layer

Firstly, the financial institution can be the cloud owner from which the payment application can be downloaded from/into the customer's mobile device; Mobile network operators can be linked to the financial institution, that is the cloud owner in this case, or it can stand as a separate party. Secondly, the financial institution could have a contract with a third party company such as PayPal that has its own cloud infrastructure or the financial institution uses other company's cloud service such as IBM, Microsoft, etc. The mobile network operators can thereby be linked with either financial institution, cloud provider or it can stand as a separate party.

This approach provides a comprehensive leadership of the cloud provider towards managing and controlling customer's information where it allows a secure element within an NFC phone to deal with authentication mechanisms rather than storing and managing the required transaction information, as described in *Things Interface Layer*. Our proposed cloud-based WoT architecture allows multitenant use and supports intelligent profiling properties, enabling the delivery of personalized content to each user. By managing the content associated with each NFC tag deployed within a particular environment, information, campaigns and service offers can be dynamically updated or customized for specific user profiles.

This service layer can hereby be specialized in service composition and service deliver. Given the resource-scarcity of IoT devices, a lightweight web component and

flexible programming model is necessary to process and manage RESTful web services. This is all enabled by such cloud provider solutions as described, and it furthermore enables the providers to focus on their core values to deliver first class services to the customer about to pay with NFC. This also enables a parallel development of cloud and/or operator specific solutions for fulfilling payments such as the previously described wallet solutions.

User/Application Layer

The user interaction with the system is reduced to single interaction making it user-friendly. The user feels more secure as the transaction can be protected by PIN verification. There are chances that a user withdraws his device from the WoT terminal as a psychological move to enter PIN. This will break NFC link, but as the PIN is stored in the SIM, it does not require NFC link for verification. Instead appropriate fallback mechanisms build into the architecture at the interface layer applies and visualizes how flexibility can be achieved by WoT. Once the user PIN has been verified by the SIM, the user places his mobile device back on the NFC terminal and the protocol resumes from the same point.

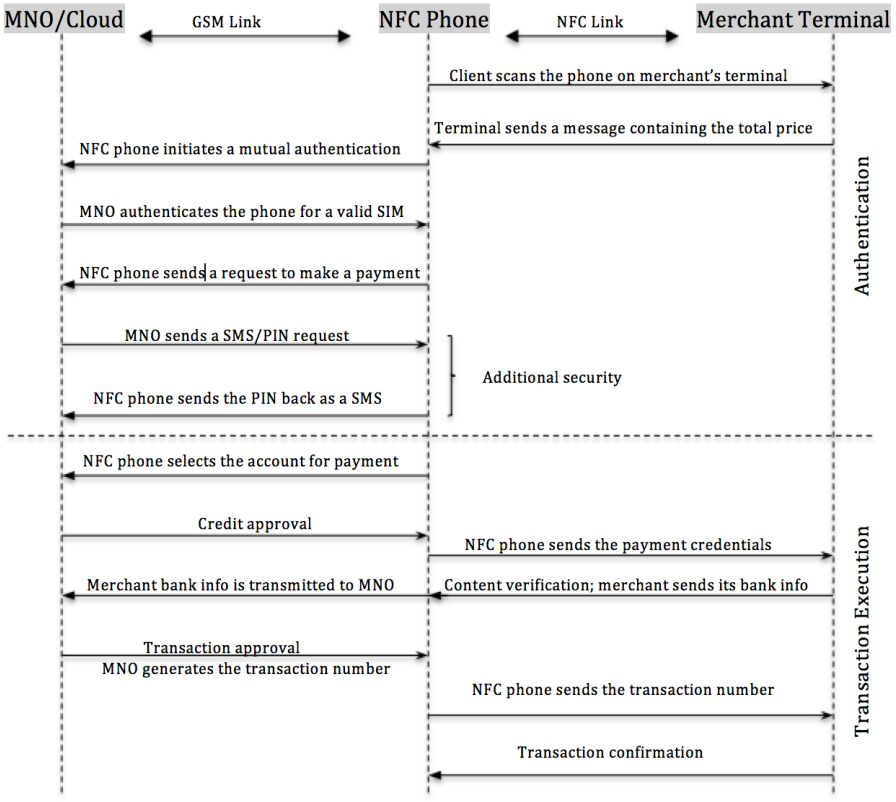

Fig. 5. Interactions between NFC Payment Parties

7 Conclusion

Users have long been accustomed to consuming services offered over the Internet using web browsers. This trend has grown exponentially since then, penetrating the consumer smartphone market as well. A separate but related trend has been that of an increasing number of standalone devices/sensors now communication wired/wireless. Together, these two have given rise to the Internet of Things (IoT). We have proposed a new lightweight architecture for NFC applied for payment over Internet of Things (WoT). This approach is grounded in a NFC cloud wallet scenario, and we show how RESTful services can be used as an advantage. We see this as an incremental step towards further eliminating the borders between smart objects, services and the data consumed by mobile clients. Future research should further explore the possibilities for strengthening and standardizing such a service environment, expanding the proposed architecture, as well as addressing important issues such as privacy and real-time response needs.

References

1. Kortuem, G., et al., *Educating the Internet-of-Things Generation.* Computer, 2013. 46(2): p. 53-61.
2. ISO, "ISO/IEC 18092:2013". 2013 Available from http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56692
3. Grønli, T-M., Ghinea, G., and Younas, M. 2013. A Lightweight Architecture for the Web-of-Things. In *Proceedings of the 10th Conference on Mobile Web Information Systems* (MobiWis), 26-29 Aug. 2013, 8093, 248-259.
4. Chander, R.P.V., Elias, S., Shivashankar, S., and Manoj, P. 2012. A REST based design for Web of Things in smart environments. In *Proceedings of the 2nd IEEE International Conference on Parallel Distributed and Grid Computing* (PDGC), 6-8 Dec. 2012, 337-342.
5. Kosmatos, E., Tselikas N., and Boucouvalas, A. 2011 Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture, *Advances in Internet of Things*, 1(1): 5-12.
6. Kortuem, G., Kawsar, F., Fitton, D., and Sundramoorthy, V. 2010. Smart objects as building blocks for the Internet of things, IEEE Internet Computing, 14(1): 44-51
7. Konomi, S., and Roussos, G. *Ubiquitous Computing in the Real World: Lessons Learnt from Large-Scale RFID Deployments*. 2007. Personal and Ubiquitous Computing, 11(7): pp. 507–521.
8. Bui, N. and Zorzi, M. 2011. Health care applications: a solution based on the internet of things. In *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies* (ISABEL '11). ACM, New York, NY, USA, Article 131, 5 pages.
9. Ghose, A. Bhaumik,C., Das, D., and Agrawal, A.K.. 2012. Mobile healthcare infrastructure for home and small clinic. In *Proceedings of the 2nd ACM international*

workshop on Pervasive Wireless Healthcare (MobileHealth '12). ACM, New York, NY, USA, 15-20

10. Efstratiou, C., Davies, N., Kortuem, G., Finney, J., Hooper R., and Lowton, M. 2007. Experiences of designing and deploying intelligent sensor nodes to monitor hand-arm vibrations in the field. In *Proceedings of the 5th international conference on Mobile systems, applications and services* (MobiSys '07). ACM, New York, NY, USA, 127-138.
11. Doody, P. and Shields, A. 2012. Mining network relationships in the internet of things. In *Proceedings of the 2012 international workshop on Self-aware internet of things* (Self-IoT '12). ACM, New York, NY, USA, 7-12.
12. Ma, Y., Rao, J., Hu, W., Meng, X., Han, X., Zhang, Y., Chai, Y., and Liu, C. 2012. An efficient index for massive IOT data in cloud environment. In *Proceedings of the 21st ACM international conference on Information and knowledge management* (CIKM '12). ACM, New York, NY, USA, 2129-2133.
13. Li, Y. and Teraoka, F. 2012. Privacy protection for low-cost RFID tags in IoT systems. In *Proceedings of the 7th International Conference on Future Internet Technologies* (CFI '12). ACM, New York, NY, USA, 60-65.
14. Kozlov, D., Veijalainen, J., and Ali, Y. 2012. Security and privacy threats in IoT architectures. In *Proceedings of the 7th International Conference on Body Area Networks* (BodyNets '12). ICST Brussels, Belgium, Belgium, 256-262.
15. Jia, H., Wu, M., Jung, E., Shapiro, A., and Shyam Sundar, S. 2012. Balancing human agency and object agency: an end-user interview study of the internet of things. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (UbiComp '12). ACM, New York, NY, USA, 1185-1188.
16. Atzori, L., Iera, A., and Morabito., G. 2010. *The Internet of Things: A survey*, Computer Networks, 54(15): 2787-2805.
17. Stirbu, V. 2008. Towards a RESTful Plug and Play Experience in the Web of Things. In *Proceedings 2008 IEEE International Conference on Semantic Computing*, 4-7 Aug. 2008, 512-517.
18. Richardson L. and Ruby S. 2007. RESTful Web Services. O'Reilly Media, Inc
19. Duquennoy, S., Grimaud, G., and Vandewalle, J. 2009. The Web of Things: interconnecting devices with high usability and performance. In *Proceedings of the 6th IEEE International Conference on Embedded Software and Systems* (ICESS'09). HangZhou, Zhejiang, China
20. Guinard, D., Ion, I., Mayer, S. 2011. In Search of an Internet of Things Service Architecture: REST or WS-*? A Developers' Perspective. In *Proceedings MobiQuitous 2011*, 326-337.
21. Castro, M., Jara, A.J., Skarmeta, A. 2012. *Architecture for Improving Terrestrial Logistics Based on the Web of Things*. Sensors, 12(5):6538-6575.
22. Guinard, D. and Trifa, V. 2009. *Towards the Web of Things: Web Mashups for Embedded Devices*, Proc. WWW2009, Madrid, Spain.
23. Khajeh-Hosseini, A., Greewnood, D., Smith, J.W., and Sommerville, I. 2012 *The cloud adoption toolkit: supporting cloud adoption decisions in the enterprise.* Software: Practice and Experience, 42(4): 447-465.

24. Kovatsch, M., Mayer, S., and Ostermaier, B. 2012. Moving Application Logic from the Firmware to the Cloud:Towards the Thin Server Architecture for the Internet of Things, In *Proceedings 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* (IMIS 2012), Palermo, Italy.
25. Alhamad, M. Dillon, T., and Chang, E. 2010. Conceptual SLA framework for cloud computing- In *Proceedings 4th IEEE International Conference on Digital Ecosystems and Technologies*, pp. 606-610.
26. Joyent Inc. *Node.js - Evented I/O for JavaScript*. 2013; Available from: http://nodejs.org/.
27. Google Wallet, "Google Wallet" 2013, Available from: http://www.google.com/wallet/
28. MasterPass, "Introducing MasterPass" 2013. Available from https://masterpass.com/
29. MasterCard PayPass, "Just tap and go" 2013. Available from https://www.paypass.com/
30. Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamtac, I. 2012. *Internet of Things: Vision, Applications & Research Challenges.* Ad Hoc Networks, 10(7):1497-1516.
31. Hurlburt, G.F., Voas, J., and Miller, K.W. 2012. *The Internet of Things: A Reality Check*, IT Professional, 14(3): 56-59.
32. Kanniainen, L. 2010, Alternatives for banks to offer secure mobile payments, *International Journal of Bank Marketing*, 28(5):433-444
33. Chen, W., Hancke, . G., Mayes, K., Lien, Y., and Chiu, J.H. 2010-NFC mobile transactions and authentication based on GSM network- *In Proceedings International Workshop on Near Field Communication,IEEEComputer Society*, 83–89.