Application of Cloud Based Computing to NFC Mobile Functionality

Vineela Malae, Dr.G.Chenchu Krishnaiah

Abstract **– Near Field Communication (NFC) delivers contactless, short-range communication and data transmission between NFC enabled devices and mobile phones for applications such as payments, NFC-based shopping, ticketing, optimized facebook page or twitter feed, website redirections, intelligent business cards or travel badge cards etc. Marvellous growth of industries in providing NFC Tag enabled services /functionality to consumers with the easiest of just a single tap, has created a massive race for the stakeholders to deploy a single entity high end platform with feasible lowest costs. This paper reviews the benefits of application of Cloud based computing technology to the NFC Mobile functionality delivering a single platform of many services, obtainable with less than couple of mins of deployment and download to the end-users, alongside with the analysis of cost-effective highly secured environment of transactions evaluating the risks and concerns involved with service providers from distributed standardized technologies.**

Index Terms - Near Field Communication, Service Providers, NFC Mobile, Cloud based computing, Usability, Security

I. INTRODUCTION

Maintaining the highest level of confidence of the customers with no compromising of security, usability and mobility of NFC Mobile is one of the key challenges for the NFC stakeholders and mobile industry investors. The future of NFC Mobile technology is in the hands of achieving a well-balanced frame work of factors concerning security, customisability, functionality along with the estimated costs while expenditure playing major role. The internet is full of continues evolutions and revolutions from world wide web to mobile internet, a world of unlimited things. The NFC Mobile makes life easier and more convenient for exchange of digital content, simpler transactions, and to connect electronic devices with less number of clicks to the consumers around the world.

Incredible transformations can be observed thought the 21st century so far with emerging technologies most in internet relevant zones. An increasing number of intelligent systems are highly connected and distributed over the internet. Every single piece of device(s) compels innovative IT services and infrastructures to assure the risk-free environment of safety and reliability. There are number concerns for the NFC enabled Mobiles/devices such as the threats to sensitive NFC services, security levels a mobile device can support, and the stake holders responsible for those services to support, current and future NFC certifications for the simplified yet secure data transmissions. NFC Mobile productions and usage are in its incremental growth along with the risks around the security and, also the budget estimations to meet the maximum output from the available resources. Some banks are in successful implementation of NFC (RFID) Tags on bank notes as a tiny microchip embedded for identification and authorisation functionalities as it hugely benefits from detecting and also in money counterfeiting.

There are 100's of services and apps developed or in continues development to be functional in a NFC Mobile which are consumer fascinating. Storing all these features in the form of NFC tags and accessing them using NFC Mobile is one of the big challenges to the retailers. The services with NFC tags enabled include Travel badge with address details, an intelligent business card known as VCard, mobile optimized facebook page, mobile optimized twitter feed, Textual contents, Website redirections, App-collection card, Loyalty cards, NFC-based shopping, single click purchases skipping long payment Queues and payment at beacons while on the go etc. All these apps and services should and must be always available to the end-user 24x7 and 365 days in a year with a single tap preferably.

A latest research has given shocking results of customer adaptation towards the phone based transactions for day to day life instead of alternative traditional payment methods. Visa International's research shows that 89 percent of people, prefer NFC enabled device as electronic wallet for the use of payment, ticketing and other applications for routine requirements of life. No sooner, we see a world of NFC Mobile wallet replacing debit, credit, loyalty and other countless cards of high usage of past or present routine.

II. PROPOSED SOLUTION

One of the best proposed solutions to support this fast and quickly advancing generation of fascinated end-user is Cloud Based Computing invented in 2006 which has tremendous advantages and proved to be worthwhile application for the best usage of resources and cost. Cloud Computing can be defined in simplest form as providing every single service and, the charge is based on the usage only

i.e., the delivery of services such as networking, servers, storage, databases, software, analytics and lot more via Internet, when and how much is in need rather spending a lot of expenditure for the entire services of infrastructure/software/platform of which may be or may not be used to complete extent. A cloud is visualised as a virtualized data centre which can scale virtual machines resources up or down, add / delete computing power and multiple users access in isolation.

The top most benefits of cloud computing are …

- Cost - eliminates the capital expense of buying hardware and software, and setting up and running on-site data centres.
- Speed - Most services accessible as self service and on demand, so even vast amounts of computing resources can be provisioned in minutes.
- Reliability - With multiple redundant sites on the cloud provider's network, data backup, disaster recovery and business continuity easier and less expensive.
- Performance - Regular upgrade to the latest generation of fast and efficient computing hardware offers reduced network latency for applications and greater economies of scale.
- Productivity - Is on high rate as less resources are invested for hardware setup, software patching and other time-consuming IT management chores.
- Global scale - Delivering the right amount of IT resources exactly when it's needed, and from the right geographic location, the ability to scale elastically.

III. APPLICATION

Application of cloud computing services to NFC mobile is based mutually on, hardware (i.e., mobile phones, NFC tags), software (i.e., applications) and communication (i.e. infrastructure, protocols and data delivery techniques). Nevertheless, combining two major subjects to work together is not less than big challenge with many risk factors to be resolved before a green go-ahead sign. In 2016, the NFC Forum has delivered a Connection Handover specification, a powerful tool to establish wireless connection between short range NFC devises with the possibility of exchanging of information via cloud provided services. The ability of this tool makes a lot life easier than before to the customers. To detail it with an example, consider a scenario where a ticket needs to be printed from a printer in an airport. The simplest way would be that the customer will tap the printer with NFC Mobile, where NFC Mobile displays the printer properties detailing what that printer can support for the requirement and can prepare to print the document.

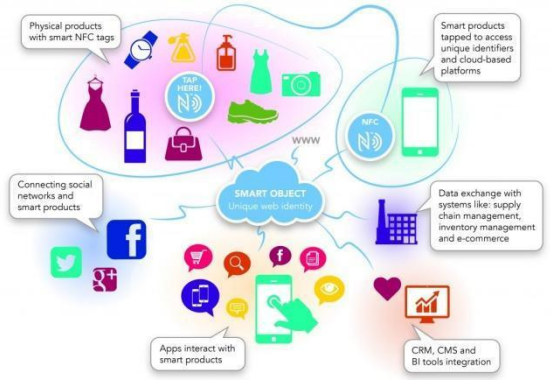

Fig. 1 NFC Mobiles and NFC Tag enabled devices access through the Clouds

IV. KEY ACTORS

The main concerns to be addressed will include A. several service providers B. benchmarks and C. security.

A. Service Providers

As of its name NFC and Cloud is a multi-tenant with more than one (stakeholder) getting involved such as cloud provider, service provider and end user each holding their own expectations, capabilities and security management from/to other stakeholders, leads to number of risks in many areas including security processes, defining assets, sharing resources, transfer of systems, compromising of requirements, standard notations, configurations, infrastructure and cost, and also end user confusions of what exactly the usability and security levels are. To shape every stakeholder without compromising to anything, the technology should make the management and maintenance of cloud services more transparent, flexible, scalable, cost-effective and auditable with detailed knowledge transfer to each other.

B. Benchmarks and Certifications

The lack of benchmarks and convincing approaches for the development of NFC services through the cloud based computing leads in to a vital conflict between several key actors. Globalplatform, an independent and non-profit organization defined a model where each stakeholder/service provider can be add/remove applications in their own fully controlled secured domain which enables division of responsibilities, roles and accesses across NFC ecosystem. It enables intelligent profiling properties i.e., Dynamic NFC tag content update and deployment of information such as campaigns, service offers or customized tourism information etc. while the

quality and speed of network certainly defines the deployment process, download time.

C. Security

SE (Security Controller) is a microcontroller (i.e., a chip) delivers storage within the mobile phone and it holds hardware, software, protocols and interfaces. SE provides secured mechanisms of authentication processes along with holding a secure area for the protection of the payment assets. The Secure Memory Card (SMC) and Universal Integrated Circuit Card (UlCC) are two best supported and highly secured examples of removable and reliable components to be used as SE. While, the Cloud Computing is suggested, the architecture will be a big change in its own replacing the entire structure with a single entity.

Clouds are available depending upon the user requirement and again the security is addressed to type of Cloud been adopted. Public cloud available over internet owned by third-party service providers whereas Private cloud, a physically located on-site data centre owned by single organisation. A mix of these two methods called Hybrid (i.e., a shared technology of data and application) stretches greater flexibility and supplementary deployment options.

Hence, the NFC Cloud Computing essential challenges of compatibility, application software security and trusted cloud environment.

Service providers must address number of high risks such as access to corporate information, access to content management and access to mobile banking or mobile Wallets while trying to maximise usability of resources and maintain efficiency with cutting the expenditure. To minimise/stop the hacking, third-party NFC stakeholder's commitment to address and understand the accountabilities,

Precision on areas of responsibility and explore ways to confidently enhance security. These risks can be addressed with different service-level agreements by their adaptable scale of shared responsibility between providers and end-users. For backing, Cloud provides SAAS (application), PAAS (platform) and IAAS (infrastructure) services. The infrastructure-as-a-service (IaaS) layer protects network, trusted computing and storage levels while sitting at the innermost implementation layer, stretched to form 2nd layer platform-as-a service (PaaS) protecting the resource-management with the support of OS and middleware which further stretched to from a 3rd layer software-as-a service (SaaS), stresses more on protection of functions at all levels with the implementation of applications on data using specific APIs.

V. FRAMEWORK - CASE STUDY

It is indispensable to get international standards implemented for NFC Mobile application via the Cloud based computing to restrict the damage and threat of consumer usability and service provider's applications security. Common Criteria is such an organisation imposes the international security certification standard involving national certification bodies. These service provider's work on mutual understanding to support secured IT applications. Common Criteria foundation ensures every single IT product or Electronic device must get evaluated, aligned as per the certification schemes, and shared agreement between bodies known as " Trusted Computer System Evaluation Criteria" . At a granular level, this is a structured and standardized process of Common Criteria, as the different branches,

- Common Criteria for Information Technology Security Evaluation (CC),
- Common Methodology for Information Technology Security Evaluation (CEM)
- Common Criteria Recognition Arrangement (CCRA)

puts the regulations in place for the fulfilment of security properties in licenced laboratories to the extent of assurance, certifying specific technologies and evaluation methods with international certifications of the products been used and implemented in a robust and skilled manner.

VI. CONCLUSION

NFC Mobile with Cloud based computing is an adventurous route of high end technology delivered to the customer with the collaboration of service providers together with high usability and cost-effective methods. The successful implementation of these technologies together will resolve many risks and issues for end-user and provides high standard as well easiest day-to-day life with a single tap-and-go process for many small to biggest routine activities. To deliver an interoperable service, require a standardised technology of NFC Mobile with Cloud based computing. The major problem in this solution, as many different organisations/industries with different core-competencies are involved i.e., a distributed standardization causing significant overhead, tough and time consuming process of adopting the benchmarks to enable highest cost-effective security zone while considering the many different views from each service provider. Any security breach will be discouraging adoption of this technology leaving devastating impact on the

industry. A non-profitable organisation co-ordinating with all service providers/stakeholders to form the agreed level of standardization will be able to address most of the risks involved.

Security, Reliability, Usability and low-Cost of NFC applications are perhaps the driving elements of the NFC technology and hence significant means of success. The proposed methodology of applying the cloud based computing to the NFC Mobile, while in comparison to alternative technologies, will be proved to be an excellent way of attaining NFC Mobile's boundless benefits. There has been tremendous work in progress in recent years, yielding several success stories in the real world with establishment of a small number of successful approaches.

The success stories reveal that, teamwork of key actors mentioned in the above sections of this paper, applications with reliability and security need to be circulated with a good knowledge transfer of the functionality to the consumers. The skilful amalgamation these two incredible technologies together, it is very likely that the NFC Mobile Cloud Computing Technology will change the visualisation of everyday life of end users making it more simpler and easier, in-turn it will play big role for entrepreneurs.

REFERENCES

[I] NFC enabled Mobile Phone or NFC Mobile and its Security by Vineela Malae, India, August 2017.

[2] Security Control System for the Integration of Mobile Agent and Web Services based on Certificateless Cryptography and Key Agreement Protocol by Ei Khaing Win*, Mie Mie Su Thwin

[3] Innovation Research and Technology (No Date), "NFC in real world: Turning the NFC promise into profitable, everyday applications" available at: http://innovation-group.com (Access date: May 27, 2011)

[4] B. Choudhary and 1. Risikko, Mobile Financial Services Business Ecosystem Scenarios & Consequences, Mobey Forum, c/o Nordea Bank,Satamaradankatu 3 B, 3rd floor, 00020 Nordea, Helsinki/Finland, April 2006.

[5] The Need for Integration in NFC Mobile Payments Pardis Pourghomi, Muhammad Qasim Saeed, Gheorghita Ghinea available at: https://www.researchgate.net/

[6] I. Kounelis, J. Loschner, D. Shaw, & S. Scheer. "Security of service requests for cloud based m-commerce". In Proceedings of the IEEE International Convention, pp. 1479- 1483. 2012.

[7] M. Rak, L. Liccardo, R. Aversa. "A SLA-based interface for Secure Authentication Negotiation in Cloud". Journal of Information Assurance & Security, 7(3), pp. 137-146, 2012.

[8] A. Dix, T. Rodden, N. Davies, J. Trevor, A. Friday, & K. Palfreyman. "Exploiting space and location as a design framework for interactive mobile systems", ACM journal of Transaction on Computer Human Interaction, 7(3), pp. 285 – 321. 2000.

[9] P. Pourghoumi and G. Ghinea. "Managing NFC Payments Applications through Cloud Computing". In Proceedings of the 7th IEEE International Conference for Internet Technology and Secured Transactions (ICITST), pp. 772–777, 2012.

[10] K. Markantonakis. "Practical relay attack on contactless transactions by using nfc mobile phones". In Radio Frequency Identification System Security: RFIDsec 12 (2012): 21.

VineelaMalae PhD Degree Scholar at Shri Venkateswara University Gajraula, U.P.,India.

Dr. G. Chenchu Krishnaiah Prof & VicePrincipal of Gokula Krishna College of Engineering, Sullurupet, A.P.,India.