A Survey on Security in Future Internet and Cloud

Fabio Sanvido, Daniel Díaz Sánchez, Florina Almenárez Mendoza, Andrés Marín López
Telematic Engineering Department, Carlos III University of Madrid, Spain
Email: {fsanvido, dds, florina, amarin}@it.uc3m.es

***Abstract*—The Internet was designed in the 1970s with limited scope and applications. It has been evolving during the last decades applying specific and ad-hoc solutions around the IP protocol to cover growing needs about security, mobility, interconnection, etc. Recent research has been increasingly focusing on the problem of Future Internet evolution; while one research line argues that a *clean-slate* approach is necessary to cover all future requirements, others maintain that Internet could continue to *evolve* adaptively, adopting new technologies as real requirements emerge. Increasing adoption of Cloud Computing paradigms could support the evolutionary approach. Beyond what would be the most valuable theory, security is one of the core issues future technologies must face. This paper gives an overview of Cloud Computing and Future Internet research issues and initiatives, oriented to security aspects. We analyze the common points regarding *Trust* and *Identity Management*, as well as identifying guidelines for future research.**

***Index Terms*—Future Internet, Cloud Computing, Security, Trust, Identity Management**

I. INTRODUCTION

Internet was designed in the 70's as a communication system between end-to-end machines targeting a community of users that could be considered experts. Thanks to the transparency of the design it has been quite easy to join new networks to the Internet's network-of-networks model. It permitted also the deployment of new services and applications leading to the well know hourglass model around the IP protocol.

Today's Internet scope is far from the original design. It has developed as a critical infrastructure for our society and economy and plays an active role in the daily life of millions of people. Internet has evolved from a limited academic scope to a mass phenomenon [1]. It has been taking more and more relevance in business and e-commerce since all processes have been significantly automated and improved through the usage of Internet technology. Concerning the user experience, Internet has influenced the evolution of computing paradigms from the mainframe to grid computing being the popularization of Personal Computers (PCs) an important milestone. Moreover, in the recent years we faced the popularization of service-oriented paradigms that have finally lead to the *Cloud Computing* approach that is envisaged to satisfy the constant demand of computing resource, data storage or software functionality [2]. Cloud computing brings to the Internet-of-services a high degree of flexibility and scalability.

This work was partially founded by the Spanish Ministry of Science and Innovation within the framework of the project TEC2010-20572-C02-01 CONSEQUENCE"

However, many aspects ave been traditionally deferred for later definition. Security is one of those aspects that were procrastinated. In fact, many early network protocols that are part of the Internet were designed without explicit security considerations [3], such as defining the security policies, managing and protecting identities, securing the interactions between heterogeneous systems, managing trust relationships between different administrative domains, monitoring and evolution of changing contexts, among others.

Thus it has become to agreement that a global re-design of the architecture may be needed pointing to the abstract concept of "Future Internet". The purpose of this paper is to summarize the most promising efforts concerning the definition of a reliable security framework for future Internet, since security is one of the tasks that are usually deferred during the definition of new architectures. Thus, we aim at bringing the reader a guide on security for the Future Internet that would help to bring robustness to the future network-of-networks.

The article is structured as follows. Some introducing notes on Future Internet evolution are given in Section III after the Section II, in which we define the basics of the cloud computing. In Section IV, we sketch out some proposals for Future Internet architecture. General security considerations and requirements are described in Section V. Finally, conclusions are given in Section VI.

II. CLOUD COMPUTING

Cloud Computing can be considered the prelude of Future Internet. Cloud computing is a new paradigm that offers scalability, reliability, availability when accessing resources across Internet. It is expected to abstract the details of the underlying infrastructure even when they are complex. Despite there is a lack of an accepted definition for this computing paradigm, Cloud Computing could be seen as the use of Internet-based technologies for the provision of services [2]. The term "Cloud" was originated from the way Internet is represented in diagrams. In general, the core concept behind Cloud Computing is Software as a Service (SaaS). Cloud Computing, and its complexity, born from squeezing or generalizing the SaaS concept to exhaustion. According to this, if in SaaS an application can be a service, also does the environment over which the application is executed, and even the hardware that executes the entire software. Following this reasoning, Cloud Computing is a resource aggregation of applications, components, frameworks that can be configured for serving several purposes.

 ISBN: 978-1-61208-148-9

When it comes to the user role, the interaction with Cloud Computing systems might be similar to already existing paradigms, in fact, Cloud computing can be seen as an evolution of the academia-oriented Grid Computing [4] or the next step in data center paradigm [2]. In a typical cloud infrastructure, a unique node, a huge "*black-box*" connection point, stays in the center of the configuration while a number of users connect with it to consume the services it offers. What really differentiates the cloud computing from traditional web service architecture is the type of services it provides. Three general types of services can be distinguished in the cloud:

a) Infrastructure as a Service (IaaS): At the basic level of abstraction there are providers who provide instantiation of virtual machines to their customers. These virtual machines are static configured and therefore have to be re-instantiated by the operator when the customer reach its limits.

b) Platform as a Service (PaaS): Moving up in the abstraction level, a provider can offer to its customers an entire environment, composed of virtual machines instantiated in the data center but invisible for the developer customers, where the programs are executed.

c) Software as a Service (SaaS): At the upper abstraction level, the providers offer entire applications to its customers. Those applications can be typically used as a desktop applications and offer storage and resources to the end user.

The combination of these services converge in three key factors for the success of the model: the illusion of infinite computing resources available on demand, eliminating the need for Cloud Computing users to plan far ahead for provisioning [5]; the possibility for companies to start small and increase hardware resources only when there is an increase in their needs; the ability to pay for use of computing resources when needed and release them when they are no longer useful.

III. What is Future Internet?

Besides Cloud Computing popularization could be considered the trigger for the definition of the Future Internet, the more Cloud Computing grows as operative technology, the more it disassociates from the definition of Future Internet becoming, as much, a component of it.

Nevertheless, at the time of writing this article, there is no "uniform" definition of what the Internet of the future will be. There exist several attempts all around the word that try to define it. The European Commission focused on research on Future Network in the Seventh Framework Programme (FP7) [6] while the US National Science Foundation launched the program Future InterNet Design (FIND) [7]. The National Institute of Information and Communications Technology of Japan launched in 2006 the AKARI project that aims to implement a new generation network by 2015.

Within a plethora of efforts and definitions, it is possible to recognize two different trends on Future Internet develop. On one hand we can find the EVOLUTIONARY approach. Followers of this trend found its view on the assumption that Internet is now a full commercial network and that the inertia introduced by operator investment and the lack of immediate gain for early adopters make the incremental enhance the only way of evolution. Some followers also point that most of the common problems, such as security, are not a problem of architecture.

On the other hand a more revolutionary idea can be found. In what is called the CLEAN-SLATE approach [8] the objective is to forget about the structural and commercial limitation imposed by the current Internet architecture in order to redefine network requirements and principles. Over them it would be designed a new architecture that would avoid known problems of IP in fields like QoS, security and mobility while provide best support for future applications.

IV. Prominent proposals

One of the key issues in the current Internet architecture has been identified in the use of IP addresses for both physically locate and identify hosts. Some proposals have been advanced to separate these concepts.

The Host Identity Protocol (HIP), defined in RFC4423, and the Accountable Internet Protocol (AIP) [9] use one public/private key pair to identify each host, where public key is used as public identifier or part of it while location is achieved through standard IP for HIP or, for AIP, through a hierarchical construction of Accountable Domains, which AIP addresses are concatenated with host address for routing purpose. Both rely on DNS services for address discovering. The Hierarchical Internet Mapping Architecture (HiiMap) [10] steps forward to redefine the DNS architecture for location. It divides Internet space in several regions, which was proposed to be real countries, and creates one mapping authority per region and one global authority to map region ones. Whit regard to the distribution of public keys HIP, AIP and HiiMap don't rely on a PKI infrastructure separated from the backbone Internet architecture but face the problem of the key distribution in different way. While AIP and HIP aim to integrate public keys in its address space through the use of self-certifying addresses, HiiMap integrates a PKI in its location system infrastructure [11], so that keys do not identify host but legal entities and solving the problem of key flexibility.

RNA project [12] proposes a "single, flexible architecture based on the reuse of a metaprotocol over different regions", the stack of network protocols is thus dynamically composed by a particular instantiation of this protocol for each layer to avoid reimplementation. The metaprotocol composes capabilities currently dispersed in different layers providing services such as state management, congestion control and security association. The resulting service is thus configurable to mach the needs of the lower or the upper layer. The goal of RNA's metaprotocol is basically create a way to avoid the need of an ad-hoc service created adding a new ad-hoc layer between existing ones or virtualizing it over the current stack just to fit a particular context. RNA's metaprotocol provides security on the entire stack by reusing security features of existing protocols in different layers and coordinating them via a common metaprotocol module interface. Despite this is a very efficient solution, it does not specify any type of

 ISBN: 978-1-61208-148-9

recommendation or requisites for security. A release of the RNA's metaprotocol is available in [13] as a patch to Click Modular Router software.

4WARD project [14] covers several areas of interest such as: Business Innovation and Regulation, New Architecture Principles and Concepts, Network Virtualization, In-Network Management and Forwarding and Multiplexing. It proposes an *architecture framework* that make possible to derive and deploy families of interoperable networks. It uses the notion of virtualization and particularly network nodes, the *netlets* [15], which can be seen as containers that hide protocol details but provide a number of properties via interfaces. A specific network is build assembling or multiplexing different netlets, which accomplish runtime requirements. It archives to run multiply different networks architectures in parallel and select the more appropriated one on runtime [16]. Based on the concept of network selection, the security provided by a network typology is just a parameter of the network selection process. Moreover in a virtual multi-network environment, a single node can be part of several virtual networks at the same time, each one with a different predominant paradigm, for example high bandwidth instead of security. In [16] the security is reduced to the selection of the appropriate security protocol by using a selection algorithm that evaluates the effects of adding such a protocol on a TCP/IP stack.

SELF-NET project [17] aims to design a self-managed network, where the concept is enhanced to cover distinct self-management methods defined as: self-optimization, self-configuration, self-healing, self-protection, self-awareness and self-organization. The object is achieved by defining a three-part closed cycle process (Monitoring - Decision Making - Execution) composing a *Cognitive cycle* that each element of the network would implement. In this context an element is intend to be either a network element (e.g., router, base station, and mobile device), a network manager, or any software element that lies at the service layer [18]. Such a system will be able to recognize its operational context (Monitoring phase), analyze it to extract a set of possible action and select the most appropriated one in each case (Decision Making phase). The selected solution will be applied to the system in the Execution phase through processes like self-reconfiguration or replacement of software components. An important aspect of these architecture elements is the ability to learn from past decisions discerning if they target the desired objective and use this experience in future decisions. Thus Decision Making, Monitoring processes and algorithms are strictly correlated.

SELF-NET proposes an implementation of the system it designed adding new autonomic network elements that should be aware of their internal and environment state and also have the ability of planning, deciding and adapting their operation in a way that best fits the operator's goals and objectives. Because of its autonomy property and distributed nature, multi-agent system (MAS) paradigm is used to support the Self-NET requirements; thanks to its decentralized approach MAS would be able to solve difficult problems in complex environments.

Slightly less centered on defining new specific network architecture, other projects focuses more on security aspects.

ECRYPTII project [19] centers on the cryptology fundamentals in networking. Divided in tree virtual labs, the project aims to address issues in symmetric and asymmetric encryption primitives and protocols as well as efficient implementation techniques in hardware and software. Those techniques might be useful for Future Internet. The WOMBAT project [20] focus on monitoring and identifying malicious code and attacks in order to generate new security practice and tools against emerging security threats.

INTERSECTION project [21] aims to build a security framework for interoperable networks by dividing the framework in two different layers, in-network and off-network layer. The project focuses on monitoring and identifying new security threats and vulnerabilities, as well as good countermeasures, at the in-network layer, and on providing a decision support system in the off-network one. The framework uses knowledge-based approach, in the off-network layer, to efficiently cross-relate monitoring results from different networks through the VIO (Vulnerability Intersection Ontology [22]).

Several more projects in FP7, center on the analysis of security in well-defined fields such as emergency (PACE [23]), financial frameworks (COMIFIN [24], PARSIFAL [25]) or industrial control systems (VIKING [26]).

The core concept that is perceived as fundamental for the success of any architecture is *trust*. Trust between network entities or end users, either to allow a distributed management of the network or to dynamically ensure end to end transactions. COMIFIN "wants to deliver a composable software system for large scale infrastructures that meets non-functional properties, such as responsiveness, predictability, *security and trust* by design". As authors in [25] state: "A lack of *trust* between entities where information is being exchanged goes to the heart of many of the challenges facing the domain of critical infrastructure protection".

Trust comes with the inseparable concept of *Identity*. For humans, both concepts can be reduced to one following the paradigm: "If I know you, I trust you". In the digital environment this model can not be applied. For example, even if the network can securely authenticate the user who wants to connect his equipment to it, this does not mean that his equipment is free of third-party malware and therefore safe to connect. Moreover either in the human or in the digital context we have to take into account the level of the trust that has to be assigned to a specific user identity and how to handle them.

Several FP7 projects take into account Identity Management. The SWIFT project [27] is designing an overlay infrastructure where the identity of the user is managed through an element called Identity broker. In the SWIFT context user owns several different *virtual identities* all of them related to a single real identity. Each virtual identity represents a "*face*" of the user, maintained to separate roles or for privacy reasons.

In parallel the PrimeLife project, whitch focuses on providing a life-long protection to the user privacy in emerging Internet applications, has defined interesting requirements for ensuring users' privacy in [28]. The documents focus

 ISBN: 978-1-61208-148-9

on the analysis of social network sites and collaborative workspaces identifying several requirements for these kind of environments that can be easily dovetailed in a more general framework. The PrimeLife's work point out that: users should have control over contexts and be able to create different kinds of context relating to distinctions; A Management System (MS) should offer models for relationships, policies, etc., that mimic everyday's human social interactions; the MS should provide users with tools to inspect (and correct) the automated inferences made on the basis of their behavior in the network; the MS should offer users the option to terminate their identity which should result in deletion of all data pertaining to this user; the MS should provide a certain level of anonymity to its users and should provide features for creating, managing and deleting different partial identities in order to reduce linkability of all actions of the same user.

V. Security requirements

In this section, we analyze the efforts made in order to define high level indispensable requirements for research in Cloud and FI under the view of security, trust and identity.

A. Secure Cloud

Security aspects in cloud computing cover a large number of topics. To deal with that, the Cloud Security Alliance (CSA) was created as a non-profit organization to promote the use of best security practices. Within the *CSA domains* of work it is possible to find: application security, encryption and key management, identity and access management.

Identity and access management are among the most outstanding topics when defining a secure cloud. This is the domain of the Trusted Cloud Initiative (TCI). TCI published in 2009 the 2nd version of the research baseline for the CSA in order to define its certification criteria [29]. The same group is now working on version 3. The documents analyze what requirements have to be addressed in the fields of Identity Management (IdM), authentication and identity federation. In March 2010, CSA identified in [30] seven major security threats and proposed some directives for solving them. The threats described in the document can be summarized has follows:

a) Abuse and Nefarious Use of Cloud Computing: To overcome the problem, the CSA recommends to increase *accountability* degree, of services as PaaS or IaaS through stricter registration and monitoring processes.

b) Insecure Interfaces and Application Programming Interfaces (APIs): The inappropriate and unauthorized use of those programming primitives should be avoided, for instance, enforcing cryptography in authentication and using fine grained access control models.

c) Malicious Insiders: The lack for provider of transparency in managing security over the entire service chain let malicious insiders to manipulate users' data. To overcome this, the CSA recommends active participation of the user in the entire security process.

d) Shared Technology Issues: a strong compartmentalization must be used together with the enforcement of Service Level Agreements (SLA) in order to overcome problems derived from sharing infrastructure among users and Cloud provider.

e) Data Loss or Leakage: As long as the number of iterations increase so does the risk of information leakage in a cloud environment. For that reason, the usage of strong encryption mechanisms and access control should be mandatory.

f) Account or Service Hijacking: If attackers gain access to users credentials, current and future activities, transactions and exchanged data will be compromised. To overcome this problem, besides implement stronger authentication methods, monitoring credentials is key for noticing hijacking.

g) Unknown Risk Profile: The risk of losing track of the security ramifications is a drawback of cloud deployments. Partial or full disclosure of provider's infrastructure details as well as security logs could overcome or mitigate the problem.

After analyzing the threats, stronger authentication and monitoring practices seems to be essential to solve cloud security threats. Nowadays the adoption of Cloud Computing solutions by real world industry is clearly driven by the size of the organization. In fact, while a small organization could find in public cloud computing services a perfect solution for a cheap start-up, medium to large organizations need to define more complex environments, with restrictively security constrains, in order to accomplish their business project in a secure way. Hybrid solution, mixing public and private clouds, are used to merge high level protection, enabled by private clouds, with the greater flexibility offered by public cloud services. Those trends could be eventually changed in the near future with the outcome of several efforts from organization as DARPA [31] and IARPA [32]. These efforts rely on homomorphic cryptography techniques that allow operating directly over encrypted data sets, producing an encrypted output without knowing data itself. Due to the complexity of the problem the first system using homomorphic encryption is quite recent. It was developed in 2009 by Craig Gentry [33]. Other prominent effort is [34], where a conceptual simplification using Integer based scheme instead of Ideal Lattices scheme was presented. Recently an important improvement to Gentry's fully homomorphic scheme based on ideal lattices has been presented by Stehle at al. in [35]. In this work, they describe a system that reduces the complexity of binary operations of Gentry's system form 2^{λ} to $quasi - \lambda^{3.5}$ where λ is the security parameter. If research on homomorphic encryption continues reducing the complexity while maintains the security, in a near future, public clouds might be no longer considered as dangerous as today.

B. Secure FI

Despite several projects aim at designing and defining Future Internet architecture, not all of them tackle security aspects.

In the scope of design a global trusted architecture one project takes particular relevance. The THINK-TRUST project

 ISBN: 978-1-61208-148-9

[36] wants to provide guidance on policy and research challenges in the field of security and trust in the Information Society. The project aims to model and define new intelligent and user-friendly ICT security environments that fit the requirements of the Information Society. THINK-TRUST final report [37] identifies challenges in different areas that depict a set of requirements that should be followed in order to provide trustworthy hardware and software:

a) Trust engineering: Trust is not absolute and will be quantified by the preferences and intuitive policies of users. Thus the need of a *trust framework* appears where trust relationships between entities are established and managed to encompass trust *preferences*, trust *policy* and trust *weighting*. Alternative approaches such as reputation, recommendation and frequentation should also be explored.

b) Architecture: Architectural support must be provided first with regard to transparency - security monitoring, observability and measurability - for data logging and log access and secondly, with regard to the ability to function across multiple layers and domain. The requirements for accountability illustrate that the user can be fully accountable in the local context but his privacy has to be protected by that local domain.

c) Cyber-security: Techniques and mechanisms to provide protection, assurance and integrity are required. These have to be platform-independent to allow interoperability of trusted entities and have to consider the growing in complexity, size, capacity, speed of the digital environment. At the same time both scarce resource devices, such as sensor networks, and self-awareness ubiquitous systems have to be considerate.

d) Accountability: Faced to anonymity, represents a supposed dichotomy between security and privacy. Accountability is view as a priority if we consider that it allows traceability/identifability, making possible to establish responsibilities and liabilities. Two options are recommended: base the demand for traceability and accountability on global accountancy-type principles, which can encompass the whole network or reintroduce, on an intermediary network layer, a "territorialisation" of facts and participating parties. In both of them a certain degree of privacy have to be ensure and it is reflected in requirements for anonymous/pseudonymous charging and payment systems and requirements for anonymization or impersonation of heuristics to produce untraceable, but trustworthy, valid sources/channels for information; for example, for economic, social or health-related statistics.

e) Privacy: With nowadays data-recollection systems absolute anonymity may be neither possible nor applicable. [37] points out the need of a fine granularity access control to identity-related information, of tools and concepts for deleting data in the Internet (in order for it to "forget") and the need for standardized techniques to assure privacy across the various Internet layers, throughout to network level and maintaining consistent privacy across different environments. Common points can be easily recognized in the recommendations found in PrimeLife documentation [28] depicted in sec V.

f) Protection: The protection of data processing, storage and transmission, as well as the shielding of resources and assets (information, services, devices, communications) require the following: domains, partitioning, compartmentalization, leading to trusted zones (and therefore, intermediate, semi-trusted zones), and to the localization of damage; fine granularity access control based on multiple bases for authentication and authorization; mutual authentication, with multiple devices; new cryptographic techniques which are low cost but high performing, in preparation for the quantum/post-quantum age.

g) Usability: FI and generally new generation network trends focus the attention on the end user but two opposite viewpoint emerge: one where the user is surrounded by a system that monitors him and automatically configure itself in order to suit user's needs and requirements and one where the user actively influence and set his own environment. While in the second is the user who decides what and how much personal information provide to the system, in the first case the system "spy" the user in order to discover all kind of useful information. The trust of the user in both systems is a key factor in the analysis. The challenge consist in offer both possibilities to the user, solving trust issues in both scenario.

VI. Conclusion and Future Work

The concepts of Cloud Computing and Future Internet have been presented in this paper. Cloud, as an almost fully deployed infrastructure, has been introduced as the last paradigm before the Internet of the future, Sec. II. Future Internet is not a well-defined concept, instead several proposals have been used in order to give an overview of the fields concerned by the change, Sec. IV. Regarding security, several aspects for both Cloud Computing and Future Internet are still an open issue and Sec. V has been dedicated to summarize results of major efforts in defining guidelines for research and development of secure infrastructures. Analyzing threats pointed out in this section, an high degree of overlap can be found, in fact beyond the requirement for stronger authentication and cryptographic techniques, useful in every kind of environment, a transverse need of new trust and identity management frameworks arise from almost every Cloud threat, keeping included in the more extended vision presented by FI requirements. Assuming stronger authentication and encryption will be available, most Cloud security issues could be solved through fine monitoring techniques and a complete users accountability, ignoring users' privacy. Moreover FI requirements of *Architecture* and *Trust engineering* depict a scenario where multiple providers, of Cloud or new types of composable services, are required to interoperate ensuring trustworthy, dynamic and private transactions while Cloud security threats does not take into account interoperability.

Besides, some of the initiatives depicted in Sec. IV focus on aspects that can be directly mapped to requirements for a secure Future Internet: SWIFT and PrimeLife center on privacy and protection of users' identity, INTERSECTION on cyber security, HIP and AIP on user accountability but architectural aspects such as monitoring and observability are a common issue present in most of them. The lack of a uniform view for architectural reform of Internet infrastructure could

 ISBN: 978-1-61208-148-9

spread efforts in to many directions. At the same time, Cloud providers, whose infrastructures have already been deployed and are evolving to face security and privacy threats, could take advantage form research implementing solutions that fulfill the requirements for a secure Cloud. Being secure Cloud and secure FI somehow overlapped, this brings Cloud closer to the definition of FI strengthening the vision of the evolutionary approach at the expenses of the clean-slate one.

Cloud providers might thus be identified as those early adopters which could lead the Future Internet implantation.

REFERENCES

[1] D. I. T. F. on the Future Internet Content, "Draft report of the task force on interdisciplinary research activities applicable to the future internet," July 2009, external Technical Experts: G. Camarillo, S. Dustdar, J. Magen, S. Paulus. [Online]. Available: http://www.future-internet.eu Accessed: Jun 2011

[2] T. R. Micro Focus, "Enterprise cloud services: Deriving business value from cloud computing," 2009, white Paper. [Online]. Available: http://cloudservices.microfocus.com, Accessed: Jun. 2011

[3] E. F. I. Assembly, "Security, privacy and trust in the future internet-issues for discussion." [Online]. Available: http://www.future-internet.eu/fileadmin/documents/bled_documents/Issues_TSD_Future_Internet_-_08_03_02.pdf Accessed: Jun 2011

[4] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in *Grid Computing Environments Workshop, 2008. GCE '08*, 12-16 2008, pp. 1 –10.

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, Feb 2009. [Online]. Available: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html Accessed: Jun 2011

[6] P. Stuckmann and R. Zimmermann, "Accepted from open call - toward ubiquitous and unlimited-capacity communication networks: European research in framework programme 7," *Communications Magazine, IEEE*, vol. 45, no. 5, pp. 148 –157, may 2007.

[7] "Future internet design," National Science of Foundation, the FIND Program is now part of the new NSF NetSE program (http://www.nets-find.net/netse.php). [Online]. Available: http://www.nets-find.net/index.php Accessed: Jun 2011

[8] J. Roberts, "The clean-slate approach to future internet design: a survey of research initiatives," *Annals of Telecommunications*, vol. 64, pp. 271–276, 2009, 10.1007/s12243-009-0109-y.

[9] D. G. Andersen, H. Balakrishnan, N. Feamster, T. Koponen, D. Moon, and S. Shenker, "Accountable internet protocol (aip)," *SIGCOMM Comput. Commun. Rev.*, vol. 38, pp. 339–350, August 2008.

[10] O. Hanka, G. Kunzmann, C. Spleiss, J. Eberspacher, and A. Bauer, "Hiimap: Hierarchical internet mapping architecture," in *Future Information Networks, 2009. ICFIN 2009. First International Conference on*, oct. 2009, pp. 17 –24.

[11] O. Hanka, M. Eichhorn, M. Pfannenstein, J. Eberspcher, and E. Steinbach, "A distributed public key infrastructure based on threshold cryptography for the hiimap next generation internet architecture," *Future Internet*, vol. 3, no. 1, pp. 14–30, 2011. [Online]. Available: http://www.mdpi.com/1999-5903/3/1/14/ Accessed: Jun 2011

[12] "Rna: A recursive network architecture," National Science Fundation, nSF NeTS FIND Initiative. [Online]. Available: http://www.isi.edu/rna Accessed: Jun 2011

[13] J. Touch and V. Pingali, "The rna metaprotocol," in *Computer Communications and Networks, 2008. ICCCN '08. Proceedings of 17th International Conference on*, 3-7 2008, pp. 1 –6.

[14] "4ward architecture and design for the future internet," European Commission, FP7. [Online]. Available: http://www.4ward-project.eu Accessed: Jun 2011

[15] L. Volker, D. Martin, I. El Khayaut, C. Werle, and M. Zitterbart, "A node architecture for 1000 future networks," in *Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference on*, 14-18 2009, pp. 1 –5.

[16] L. Volker, D. Martin, C. Werle, M. Zitterbart, and I. El Khayat, "Selecting concurrent network architectures at runtime," in *Communications, 2009. ICC '09. IEEE International Conference on*, 14-18 2009, pp. 1 –5.

[17] "Self-management of cognitive future internet elements - self-net," European Commission, FP7. [Online]. Available: http://cordis.europa.eu/ Accessed: Jun 2011

[18] T. Raptis, C. Polychronopoulos, A. Kousaridas, P. Spapis, V. Gazis, N. Alonistioti, and I. Chochliouros, "Technological enablers for self-manageable future internet elements," in *Future Computing, Service Computation, Cognitive, Adaptive, Content, Patterns, 2009. COMPUTATIONWORLD '09. Computation World:*, 15-20 2009, pp. 499 –504.

[19] "European network of excellence for cryptology ii - ecryptii," European Commission, FP7. [Online]. Available: http://www.ecrypt.eu.org Accessed: Jun 2011

[20] "Worldwide observatory of malicious behaviors and attack threats - wombat," European Commission, FP7. [Online]. Available: http://wombat-project.eu Accessed: Jun 2011

[21] "Intersection (infrastructure for heterogeneous, resilient, secure, complex, tightly inter-operating networks)," European Commission, FP7. [Online]. Available: http://www.intersection-project.eu Accessed: Jun 2011

[22] M. Choraś, R. Kozik, A. Flizikowski, R. Renk, and W. Holubowicz, "Ontology-based decision support for security management in heterogeneous networks," ser. ICIC'09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 920–927.

[23] "Ip-based emergency application and services for next generation networks - pace," European Commission, FP7. [Online]. Available: http://www.ict-peace.eu Accessed: Jun 2011

[24] "Communication middleware for monitoring financial critical infrastructure - comifin," European Commission, FP7. [Online]. Available: http://www.comifin.eu/ Accessed: Jun 2011

[25] "Presentation on identity management and protection in critical financial infrastructures topics," PARSIFAL project, deliverable D2.2. [Online]. Available: http://www.parsifal-project.eu Accessed: Jun 2011

[26] "Vital infrastructure, networks, information and control systems management -viking," European Commission, FP7. [Online]. Available: http://www.vikingproject.eu Accessed: Jun 2011

[27] "Secure widespread identities for federated telecommunications - swift," European Commission, FP7. [Online]. Available: http://www.ist-swift.org Accessed: Jun 2011

[28] M. Pekárek and S. Potzsch, "Requirements and concepts for privacy-enhancing access control in social networks and collaborative workspaces," PrimeLife - UE FP7, heartbeat. [Online]. Available: http://www.primelife.eu Accessed: Jun 2011

[29] C. S. Alliance, "Domain 12: Guidance for identity & access management v2.1," April 2010, trusted Cloud Initiative. [Online]. Available: http://www.cloudsecurityalliance.org/guidance/csaguide-dom12.pdf Accessed: Jun 2011

[30] CSA, "Top threats to cloud computing v1.0," March 2010, top Threats Research Working Group. [Online]. Available: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf Accessed: Jun 2011

[31] O. of Naval Research, "Catalyzing research initiatives in programming computation on encrypted data(proceed)," solicitation Number: DARPABAA10-81.

[32] O. of the Director of National Intelligencet, "Security and privacy assurance research (spar)," solicitation Number: IARPA-BAA-11-01.

[33] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009, crypto.stanford.edu/craig.

[34] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in *Advances in Cryptology EUROCRYPT 2010*, H. Gilbert, Ed. Springer Berlin / Heidelberg, 2010, vol. 6110, pp. 24–43.

[35] D. Stehl and R. Steinfeld, "Faster fully homomorphic encryption," in *Advances in Cryptology - ASIACRYPT 2010*, M. Abe, Ed. Springer Berlin / Heidelberg, 2010, vol. 6477, pp. 377–394.

[36] "Think tank for converging technical and non-technical consumer needs in ict trust, security and dependability - think-trust," European Commission, FP7. [Online]. Available: http://www.think-trust.eu Accessed: Jun 2011

[37] THINK-TRUST, "D1.7 project final report," FP7. [Online]. Available: http://www.think-trust.eu/public-documentation/think-trust-documents.html Accessed: Jun 2011

 ISBN: 978-1-61208-148-9