Recent ICT Advances Applied to Smart e-Government Systems in Life Sciences

Alexander B. Sideridis[1], Loucas Protopappas[2]

[1]Informatics Laboratory, Agricultural University of Athens, Greece, e-mail: as@aua.gr
[2]Informatics Laboratory, Agricultural University of Athens, Greece, e-mail: loucas.protopappas@aua.gr

Abstract. As Internet of Things and Cloud Computing are gaining momentum, smart e-government systems and applications to citizens and business, adopting these technologies, improve further our everyday lives and business frontiers. E-government systems are further expanding their range of application also, by reclaiming advances in electronic authentication and identification. These late developments make even possible the application of smart e-government systems not only to the areas of immense security like Public Health and Banking but also to Life Sciences mainly Agriculture, Food Sciences, Farming, Forestry and the Environmental Sciences. In this paper an attempt is made to describe the framework of designing smart e-government applications aiming to support advanced with no national frontier limitations systems on the above important application areas. The importance of these systems is becoming greater taking into account that the economic recession hits particularly countries with main income from exports of agricultural products.

Keywords: Internet of Things, Cloud Computing, Radio frequency identification (RFID), Smart e-Government Agricultural Applications.

1 Introduction

A couple of years ago we had observed the potentiality of new forms of e-Government applications as well as the necessity of adopting advanced e-Government services in both enhancing citizen's daily activities and creating the appropriate basis in public administrations for the development of knowledge based economies [17][13]. Emphasis was given to the need of fully exploiting Information and Communication technologies (ICT) and new forms of communication for the development of the appropriate structures aiming to support complex e-Government systems which should extend further their area of application beyond national boarders and economies [5]. This need is immense since globalization has strongly emerged and we now discussion about global economies, global health, global banking systems etc. [10] Global security, in all those systems of international cooperation and application, is the dominant aspect and as recession, downturn in the

Proceedings of the 7th International Conference on Information and Communication Technologies in Agriculture, Food and Environment (HAICTA 2015), Kavala, Greece, 17-20 September, 2015.

economy and international terrorism remain the main areas of exchange of information and methodologies between international organizations, governments and individuals, this aspect promotes continuous research in this area.

The implementation of secure, trustworthy and smart e-Government systems in order to support common standardized procedures within a country has been encouraged by national governments and federal agencies [6]. In particular, the progress of standardization and unification within the European Communities at the beginning and European Union (EU) soon after has pressed State agencies for the transformation of already developed procedures to cross-border e-Government applications [7]. The EU policy towards convergence of e-Government systems of member States was expressed through a series of incentive programs promoting interoperability of those systems by introducing new research developments on e-Signature (e-SIGN), e-Authentication and e-identification (European Commission, [8],[9]). The latest EU's initiatives were aiming to create an integrated and well established workplace for e-IDentification and AUthentication, [(eID) and (eAU)] respectively, within European States for both citizens and enterprises or legal entities of any form. Since the EU project STORK 2.0 [19] has just been successfully implemented, these recent developments and EU's directives are going to be gradually adopted by security sensitive systems on e-banking, e-health, e-Justice and customs export systems of the member States [15]. However, if not, the above systems could not be put in practice efficiently and the envisaged creation of a Digital Single Market in Europe could not be materialized.

The operation of interoperable eID environments was one of the key objectives of STORK 2. In fact, this objective was successfully tested by the operation of four cross-sectoral pilots [15]. This implies that e-Government systems making use of this capability can be designed not only to the benefit of important Government to Government (G2G) or Government to Citizen (G2C) systems, such as those of public administrations, public health, education etc but also Government to Business (G2B) or Business to Business (B2B). The latest G2B and B2B will operate mostly to the benefit of private sector and are considered to be very vital for boosting Small to Medium Enterprises (SMEs), particularly these days of economic recession during which SMEs have badly hit, and the creation of new jobs is the main scope of nearly all Governments in order to fight unemployment. Particularly, countries of south Europe have experienced very high figures of unemployment, mainly in young people, e.g. in Greece this figure exceeds 50%, so that expected benefit out of the growth of new SMEs, in a few remaining areas of the primary sector, like that of agricultural production, is also high. Unemployment in Europe has brought many young people abroad looking for jobs and new opportunities. Thus, G2C systems with cross-border capabilities are invalid for safe certification using eID.

It's evident, up to now that federal strategies and policies, like those of the EU and the USA, towards the development of smart e-Government systems with capabilities as those described above, are acting as incentives and lead research [6] in the area of security and practically to innovative techniques e.g. on eID (with the prerequisite of e-SIGN) and eAU.

In the near past, not long before the EU's initiatives [8, 9, 19], just the opposite happened. ICTs and technological innovations used to provoke the policy makers to fully exploit them in designing their e-Government systems and applications tailored

made to their needs. Today, innovations such as those referred for e.g. to Big Data, Internet of Things (IoT) and Cloud Computing (CC), combined with more recent results on e-SIGN, eID, eAU, are leading us to design really smart e-Government applications applicable to many G2G and G2C applications, mainly in the area of our core interest in Agriculture, Forestry, the Environment and Food Technologies. Precisely, this is the focal of this paper and our ideas in designing such systems are analytically presented in section 5. For the completeness of these article innovations as those of IoT, CC, eAU and eID are presented in sections 2, 3 and 4 respectively. Finally, in section 6, are drown certain conclusions mostly based on the applicability of the proposed smart e-Government applications of section 5.

2 Internet of Things and its Expansion

The Internet of Things (IoT) is the upcoming evolution of the Internet services available today. It is a network that is not composed of computers but also of interconnected objects. These items will contain embedded electronic systems and may be of various household appliances, transportation, telecommunication means, books, cars, even foods. In this vision, each object will use radio frequency identification systems (known as RFID), a kind of sensor, etc. IoT will be the culmination of the effort to integrate and automate services that provide embedded systems of all kinds. All these are some applications that will radically change the current way of life in the next decades.

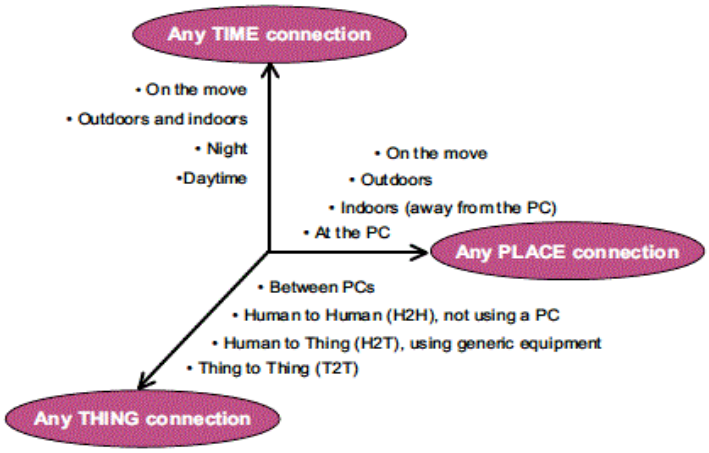

Fig. 1. A new dimension. Source: ITU adapted from Nomura Research Institute

Although, the sustainability of IoT is still being discussed, its usability seems to be very effective and efficient for citizen's daily activities as the connection of physical things to the Internet makes it possible to access management and operation of

remote devices [23]. Thanks to rapid advances in underlying ICT technologies, the IoT is opening enormous opportunities for many novel applications that citizens may improve the quality of their lives. International Telecommunications Union (ITU), in 2005, predicted that "the IoT will connect the world's objects both in a sensory and an intelligent manner", fact that, in our days, is verified. The technology of IoT, on the one hand, is a combination of 4 emerging promising technologies: RFID, Sensor technologies, Smart technologies and Nanotechnology and, on the other hand, it inherits the globality and interconnection of Internet and adds a new dimension to the world of ICTs: from anytime, any place connectivity for anyone, we will now have connectivity for anything (Figure 1).

The IoT has 3 major characteristics:

a. Integrated structure using RFID technology, sensors and two-dimensional code to collect information from objects anywhere and anytime.

b. Reliable transmission. Accurate and real-time information by the objects, involving various telecommunications networks and Internet.

c. Smart processing using smart ways such as cloud computing and fuzzy recognition (fuzzy identification) to analyze and process vast amounts of data and information, with a view to implementing intelligent control objects [25].

2.1 Architecture of Internet of Things and its Technologies

The IoT can be divided into three levels: the perception layer, the network layer and the application layer.

a. The perception layer consists of RFID tag and reader, camera, GPS, all kinds of sensors, sensor network, M2M terminals, and sensor gate (gateway), etc. The main function of perception layer is the perception and identification of objects and collecting information.

b. Network layer, also called as transport layer, is a convergent network that formed by all kinds of communication networks and the internet. The network layer has not only the ability of network operation, but should improve the ability of information operation. Also, it provides and processes information from the perception layers, like it is the nerve center and the brain structure, completing the transfer of information and data between perception layer and the application layer.

c. The application layer is mainly composed of types of application systems, with main functions the convergence, the transformation, the analysis and the exchange of data and the relevant support platform for users. Moreover, this layer also provides an interface for implementing IoT and the service's implementation for devices and user terminals.

The IoT is a technological revolution that represents the future of ICT and its development require support and collaboration with some innovative technologies. The major technologies that will dominate the IoT applications are wireless sensor networks (WSN), the radio frequency identification (RFID) and mobile communications with existing LAN / WAN networks.

2.1.1 Radio Frequency Identification (RFID)

The radio frequency identification is considered of the key drivers of growth of the IoT. The objects should be identified so that can be connected. RFID technology, which uses radio waves to determine the elements, can provide this function. The RFID system includes various frequency bands from 124 kHz as the 5.8 GHz, such as 124 kHz, 135 kHz, 13.56 MHz, 470 MHz, 900 MHz, 2.4 GHz and 5.8 GHz.

The technology composed of tags / transmitters, a reader and a computer support system. The tag has a unique identifier (ID) and an antenna for transmitting / receiving radio waves from the reader located nearby. The reader transmits the information that received from the tags in support system for validation and the backend system runs the applications, according to data received from the reader. Finally, RFID technology has been identified as the replacement of the bar code system, but the RFID system can do much more than that. In addition to the data identification, it can monitor the data in real time in order to get important information about their location and status.

2.1.2 Sensor Technologies

The sensors have the innovative ability to detect any change in the physical status of things and they provide a series of important data. In more details, the nodes collect and forward the data to the base station for the joint monitoring of physical objects or environmental conditions such as temperature, pressure and motion. In Wireless Sensor Networks (WSN) are usually one or more base stations and many sensor nodes. The base station acts as the trusted central authority and also serves as a data processor that connects the sensor network to the outside world.

2.1.3 Smart technologies

The objects that become smart after the implantation of intelligent technologies can communicate with the users by actively or passively way. Nowadays, smart technology is one of the most upcoming innovation as in combination with others technologies (Bluetooth, Wireless Networks, RFID), it gives, in physical things, an independent and dynamic role. Advances in smart buildings, in smart vehicles, in smart environment and personal robotics are some of the leading areas.

2.1.4 Nanotechnology

Nanotechnology is used to improve products in many industries and disciplines, including medicine, energy and transport. This kind of technology is growing and is connected with the capacity to observe and supervise the atoms and molecules. Meanwhile, it can have other various forms of use, such as to develop special sports equipment for therapeutic applications [12].

2.2 Applications

Nowadays, the emerging IoT has impacted many application domains (Fig 2.) and, according to the researchers, up to 2020, it is estimated more than 30 billion devices will be wirelessly connected to the IoT [11][1].

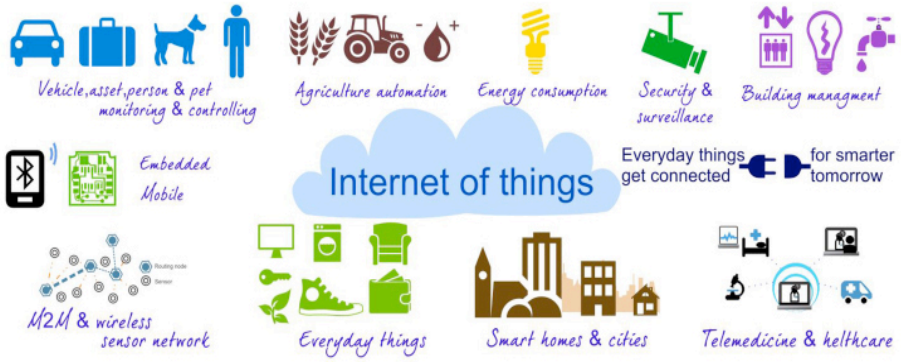

Fig. 2. Application of IoT. Source: datasciencebe.com

The IoT appends to physical objects both an interactive and dynamic task, providing them the capacity to interact with users via embedded systems. Ubiquitous computing and the IoT are become entwined with our everyday lives in many areas, such as health, transport, agriculture, public sector, almost without our noticing it. Although, it seems that the IoT will change future lifestyles, further work is required in safety and security.

3 Cloud Computing and its Aggressiveness

Cloud Computing (CC) implies the use, through Internet technologies, of computers and their resources, like storage, system software, applications software, software packages, user applications and data, in a global scale. Obviously, access to unlimited resources permits among the others, flexibility in choosing the appropriate and most updated software, and collection of innovative applications and packages. At the same time, CC, by allowing the selection of low cost storage capacity of various computer systems and other computer devices income, provides immense scalability and reduces performance cost of CC systems considerably. An additional benefit to the end users of CC services is related to compatibility issues. Through CC, in most cases, end users can take advantage of advanced and updated versions of available software regardless of their platform specifications. But, "no pain no gain". The high benefits of CC cost high risks in inconsistency and security. And as

everybody knows how to efficiently deal with inconsistency, security remains in danger and presents the main issue for the CC system developers.

Cloud's source characterizes its deployment model. Therefore, in case of a private model, the owner of a cloud is an organization allowing its use to its own members. Quit often, these clouds are used for data and specific applications sharing. A public model of a cloud provider is usually offering services to customers. Examples of such providers are Yahoo, Google, Amazon etc. A model that provides applications and any kind of recourses to citizens of a community belongs to a community model. In such a case, an administrator or a number of community members are usually collectively operating the specific cloud. Finally, there is a hybrid model of cloud providers in case of any scheme combining more than one model of the above [22].

The large number of cloud users, the variety of platforms used and the unlimited number of physical devices operating under external protocols may result to cloud expose in various threats. For this reason, organizations are concerned of their data not being safe enough. This fear for corruption is intense in case of sensitive data. Fear intensifies more because users do not know the security measures taken by the provider's liability. Clearly enough, authorization, authentication, data confidentiality, privacy, trust, integrity and data availability in CC and cloud environments are opened research areas.

3.1 Authorization

Cloud providers are responsible for security measures of their system and specifics for identification of their clients whoever they will be (enterprises, staff, end users in general). In most of the cases clients, by providing their credentials (usually their name and password), are entering to the cloud and make use of their privileges which, in general, are, or should be, different from one user to another [22, 3]. If a user, in order to fully exploit an application available to a cloud, has to store his own data files on this cloud, he must be ensured that his file will not be modified without his authorization. Otherwise severe damage may be caused and this may be fatal, particularly in the case of systems using sensitive data. Therefore, authorization is necessary and it should be enforced by specific security precautions. As a conclusion, the structure of a CC system should be very well organized and provision of access to clients should follow restrictions according to their roles and needs.

3.2 Availability

Since unlimited clients may use a CC system, system's provider must be able to support it under a heavy network load. Varying protocols and bandwidths may also reconsidered. Also, in case of hardware failures operations should be not discontinued and alternative routes should be available. Failures may be also caused by external attacks of malicious users who are trying to bring down the system [22, 3, 14, 24]. Thus, availability is a critical issue and characterizes the quality of CC service.

3.3 Trust

In CC environments trust is an important issue since it has to do not only with the cloud provider and his precautions but also with the behavior of the rest of parties involved. Clients play a significant role since they may not always behave as they are expected. Users of this kind may cause damage to an unsuspecting client, his data files and expected outcome of his operation. Therefore, CC system providers must ensure their clients that all safety measures have been undertaken and trust should be their mutual feeling of minimized risks of the available cloud [22, 20].

3.4 Integrity

In CC environments data and hardware integrity refer to the system's protection by not allowing to unauthorized users to access or modify or make any modifications to the hardware used or its drivers. CC system' users may cause damages of this kind intentionally or unintentionally. In both cases unsuspected clients are victims of a malicious operation [22, 20].

4. e-Authentication - e-Identification: Ironing Computer Security

Currently, the complexity and multi-level architecture of computer systems pose risks to application security and integrity of citizens' personal data. Additionally, the developers make unremitting efforts to meet all the application security gaps but most of the time without success. The design of security in IT systems is closely linked to the techniques, procedures and administrative measures as well moral-social attitudes, principles and assumptions, sheltering from any threat of accidental or intentional. The most crucial point in the design process of safe policies is the identification and characterization as confidential data that are used and protected. In addition to, principles of Integrity of Information, Confidentiality and Availability Information security policies should incorporate besides the terms of authenticity, authentication and Identification. The new emerging technologies (IoT, CC), that we note above, facilitate greatly the daily life of citizens. However, security plays a key role in the sustainability of an application or that of a service. On the one hand, the system may defend information and data from unauthorized access and, on the other hand, people use and trust these services more easily because they have high levels of security.

Furthermore, milestone are the cross-border services that allow increased citizens' mobility within the European states, as personal documentation and data are following citizens throughout Europe. STORK 2.0 that recently finished, launched by European Commission and presents a series of cross-border digital services that to (i) enable the Digital Single Market focusing on legal entities & attributes which is important for boosting SMEs & private sector, (ii) Facilitates cross-border eGovernment applications and (iii) Reduces administrative burdens of the companies & individuals wishing to provide services across borders. In this project, there are 58

partners from 26 participating countries, including Greece. EID, eAU and e-SIGN are the novel milestones for secure cross-border electronic transactions and foundation blocks of the Digital Single Market.

4.1 Security in Internet of Things

The widely usage of IoT is an indisputable fact and by 2020 it is estimated to reach 50 to 100 billion of devices [20]. In not-so futuristic world of IoT, security, privacy, and trust need to be considered as fundamental design parameters. Experts are trying to enhance the security of IoT framework, many security aspects must be covered in order to maximize the security, such as, secure booting of devices, role-based access controls, Firewalling and IPS and device authentication [21][18].

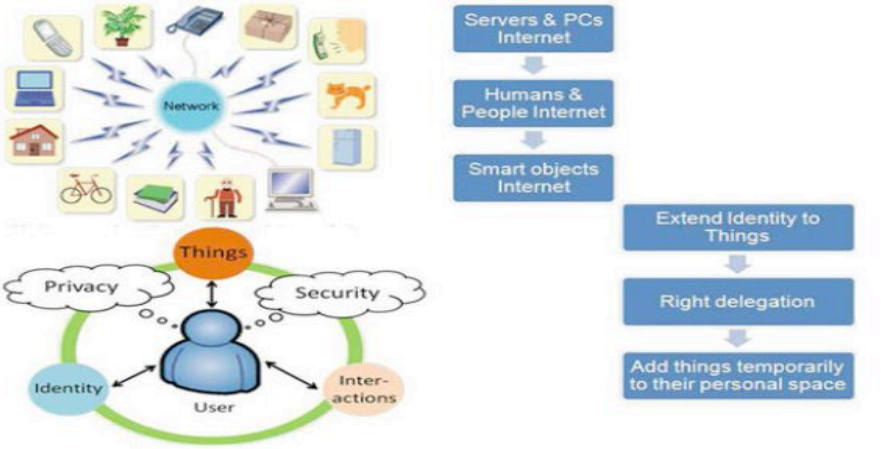

Fig. 3. Security in IoT. Source: http://link.springer.com/book/10.1007%2F978-3-319-06811-4

4.2 Security in Cloud Computing

The security of CC or just cloud security is a developing sub-domain of computer, network, and, information security roughly. It indicates an extensive set of policies, technologies, and controls that are used to secure data, applications, and the related infrastructure of CC. The CC security can be separated into two categories: security concerns encountered by cloud providers and security concerns encountered by their customers. Although, most of cloud providers are considered to be frontrunners in security issues, the last techniques that were used are: data encryption, data masking, authentication and privacy [2].

4.3 Security in cross-boarder Services

The goal of cross-border services is to eradicate the current digital barriers that citizens face, and the businesses' flexibility in the single market via e-gov services. In essence, they allow citizens to establish new e-relations across borders, just by presenting their national eID. EAU and eID, in combination with the e-Signatures are the key enablers for the interoperability and reliability of cross-boarder services [6][7][8]. The following figure shows the identification process and which the providers that are involved.

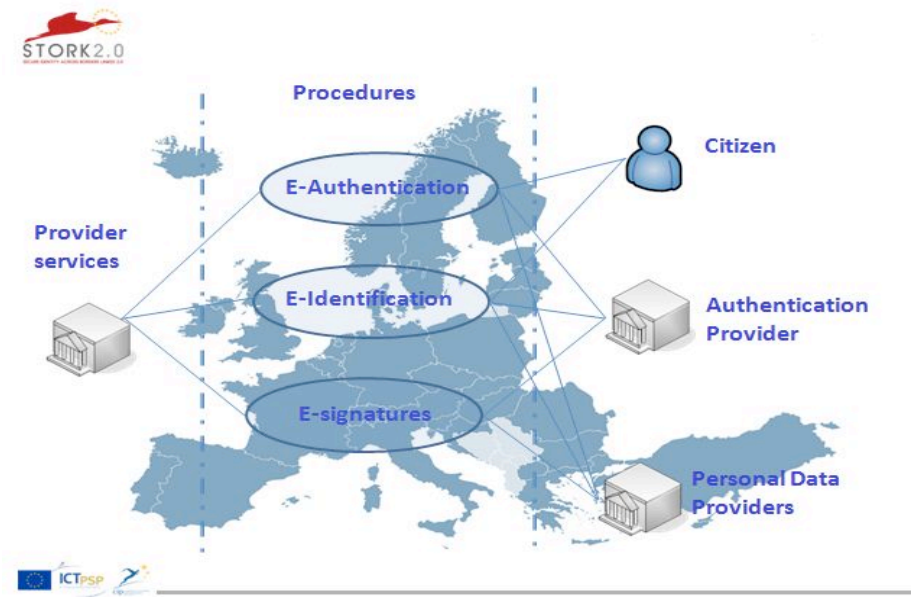

Fig. 4. Authentication Procedures. Source: https://www.eid-stork2.eu/

5 Smart e-Government Agricultural applications

Traditional e-Government systems, adopted by many countries for the last ten years or so, can be transform to Smart e-Government Systems (SeGSs) using last developments and plethora of applications of CC, Big Data and IoT technologies. This transformation, by the application or combined with recent research results, and actually readymade platforms, on eID, eAU and e-SIGN, is further extending their use and benefits to citizens, business or Government agencies. In the case of Agriculture, SeGSs present a special interest due to the global recession in economy which necessitates considerable reduction in production and distribution cost of the agricultural production.

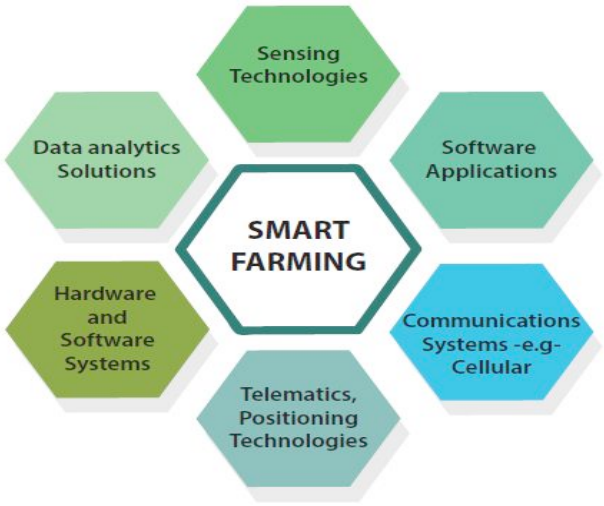

Fig. 5. Different Technologies in Smart Farming. Source: Beeocham Research Ltd

On e-Commerce, the decisive benefits in using e-Government systems of the mode G2B, B2B or B2C and their expected value for trust, time and money, are those enabling e-business to perform efficiently improving at the same time their security, accessibility and reliability. For example, let us consider a B2B application of import-export activity of agricultural products. The transformation of this application to the corresponding B2B smart e-Government system, by making full use of eID, eAU and eSIGN platforms, will further minimize bureaucracy, time and cost spent in ordinary transactions. E-transactions, through the above platforms, will lower burden in conducting business in person (physical or enterprise).

Exports and imports of agricultural products are important day-to-day activities and are usually supported so far by e-Government B2B systems conducted, in the name of farmers, by intermediaries and, in the best case, by their Unions. Small Medium Agricultural Enterprises (SMAEs) are paying heavy duties on this. Evidently in the cross-border environment, a SMAE cannot conduct business without guaranteed eID, eAU and eSIGN SeGSs. Therefore the use of SeGSs is of enormous significance for SMAEs in conducting business at least in cross-border environments (for example between the member States of the EU).

As we saw in previous sections, the IoT and the CC can work beneficially for every domain. Moreover, the perfect combination of them can "take off" and promote fast development in any sector. Agriculture is considered as a key driver of the economy in many countries, especially those of South Europe like Greece, which is in recession in economy. For this reason, there is an urgent need for transformation and upgrading of the agricultural sector and making full use of the benefits of Smart Agriculture.

These days, farmers and breeders have new dynamic roles and challenges as utilizing the technology and many interactive tools to their smart phones or their tablets. So, based on key techniques of IoT, Big Data, GPS and CC, farmers have endless functions, such as environment monitoring and control systems, real-time weather forecasting reports, monitoring of food supply chain and soil and plant monitoring [3].

Smart Agriculture is now an unprecedented research area, which has numerous features, utilizing the sensors technology and ICTs. Among the benefits of innovative technologies are: improvement in the use efficiency of inputs, increased profitability, sustainability and food safety [3]. Additional, using RFID technology, farmers can monitor the plant's growth and monitor farm's important data (soil constituent, soil humidity, light, wind and air). Smart farms, now, aims to for making many agricultural works more autonomous and context-aware [14].

A concrete area of Smart Agriculture with a plethora of SeGSs is that of Precision Agriculture. Automation of farming procedures, climate monitoring, crops health data, diagnosis of farm machinery breakdown and early detection of natural disasters synthesize an upcoming Smart Farming era [24].

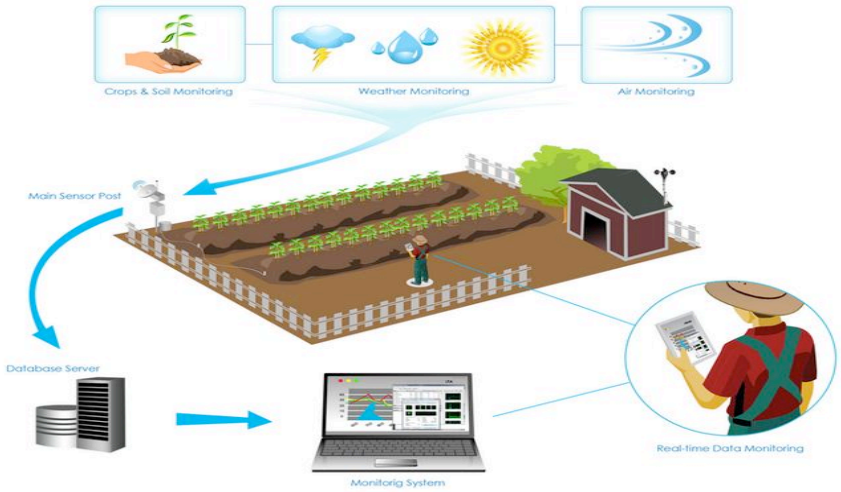

Fig. 6. Smart Farming. Source: http://www.iotphils.com/solutions/precision-agriculture/

6 Discussion

Under the World Wide Web (WWW) a new computing paradigm, with innovative applications and integrated e-government systems inspired by advances in CC, Big Data and IoT, is now prevailing. This computing paradigm dictates the extent, the applicability, the availability and reliability of the new e-government systems especially designed for unpredictable so far application areas in Agriculture,

Forestry, Food Science and the Environment. That is why the current technological epoch could be characterized as the epoch of Smart e-Government Systems (SeGS).

The main benefit of SeGSs is the combination of enormous quantities of data and information, available through the above mentioned technologies, with no or very low cost by the free usage of software and hardware globally available. The main shortcoming comes from the security aspect and its parameters. In this respect a lot of research effort is already producing useful results. Governmental organizations, realizing the importance of SeGS in sensitive and financially significant application areas, have announced political strategies, major programmes and specific projects. In particular, the European Union (EU), since the turn of the century, has put too much emphasis for the development of platforms by its member States enabling them to implement the EU's objectives. An important such EU's principle is that of free movement of its citizens with no cross-border obstacles. Other, no less significant objectives, are those of the financial sector, integrated banking system, e-health and e-justice systems. These systems have now developed and been applicable by advances in the latest EU's STORK2 project. This project is on line with launched seven priority areas in the "Europe 2020 Strategy". One of this areas should be dealt with “wider deployment and more effective use of digital technologies” as a way of preparing EU economy of the next decade [8]. Specific actions undertaken by member States form the Digital Agenda for Europe which, in turn, is leading to a Digital Single Market (DSM). Of course the main characteristic and prerequisite of DSM implementation should be the connectivity of all Europeans (citizens, businesses or administration staff) to high speed Internet though G2C, G2B, B2C and G2G mode [10, 21, 16].

In this paper has been pointed out, though reference to specific SeGSs, that to the above application areas should be added e-Agriculture, e-Forestry, e-Food Sciences and e-Environment. In the latest areas of our interest, security aspects are partly encountered by STORK's successful outcomes on eAU, eID and e-SIGN. The importance of these SeGSs, with the latest features, it becomes more eminent under the current economic recession on the economy of countries like Greece heavily dependent on export of agricultural products.

References

1. ABI Research, http://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne
2. Armbrust M. et al (2010) A View of Cloud Computing, Communications of the ACM.
3. Behl, A., Behl, K. (2012) Security paradigms for cloud computing. 4th International Conference on Computational Intelligence, Communication Systems and Networks, pp. 200–205. Thailand: IEEE.

4. Chaurasia R. (2014) Amity University A Review Paper On Security In Cloud Computing, International Journal Of Scientific Research And Education, Vol. 2, Issue 2, p. 896-902.
5. EUROPEAN COMMISSION (2005) I2010-A European Information Society for growth and employment. Brussels: EC publications.
6. EUROPEAN COMMISSION (2010) The European eGovernment Action Plan 2011-2015-Harnessing ICT to promote smart, sustainable & innovative Government in ICT for Government and Public Services2010. Brussels: EC publications.
7. EUROPEAN COMMISSION (2010) Towards interoperability for European public services. Brussels: T.C. Communication from the Commission to the European Parliament, the European Economic and Social Committee and the Committee of the Regions.
8. EUROPEAN COMMISSION. http://ec.europa.eu/information_society/apps/projects
9. EUROPEAN COMMISSION. http://ec.europa.eu/digital-agenda/en/ict-policy-support-programme
10. EUROPEAN UNION (2009) DECISION No 922/2009/EC of the European Parliament and of the Council on interoperability solutions for European public administrations (ISA). Strasbourg: Decisions adopted jointly by the European Parliament and the Council.
11. Gartner, http://www.gartner.com/newsroom/id/2636073
12. ITU (2005) The Internet of Things – ITU Internet Reports 2015. Geneva: ITU.
13. Karetsos S., Costopoulou C., Sideridis B. A. (2013) The use of Smartphones in Agricultural m-Government, Proceedings of Agricultural Informatics 2013: The past, the present and future of Agricultural Informatics. Debrecen: International Conference, p. 145.
14. Popovic, K., Hocenski, Z. (2010) Cloud computing security issues and challenges. In: 2010 Proceedings of the 33rd International Convention, MIPRO, pp. 344–349.
15. Protopappas L. and Sideridis A. B. (2013) The Strategy and the Progress Made on E-Government services in the EU, Athens: Proceedings of the 5th International Conference on E-Democracy, Security, Privacy and Trust in a Digital World, Springer CCIS series, Vol. 441, p. 192.
16. Sideridis A. B.(2013) E-Government research and services at an era of economic crisis. In Proceedings of the 6th International Conference on Information and Communication Technologies in Agriculture, Food and Environment. Vol. 8, pp.9-12, Corfu: HAICTA 2013.
17. Sideridis B. A. (2013) Present and future e-Government advances at the service of rural area citizens, Agricultural Informatics 2013: The past, the present and future of Agricultural Informatics. Debrecen: International Conference.
18. Song Y. (2013) Security in Internet of Things, KTH Information and Communication Technology, Stockholm: Master of Science Thesis Stockholm.

19. STORK 2.0. https://www.eid-stork2.eu
20. Sun, D., Chang, G., Sun, L., Wang, X. (2011) Surveying and analyzing security, privacy and trust issues in cloud computing environments. 2852–2856 (2011). Elsevier Ltd.
21. Tamara Almarabeh (2010) A General Framework for E-Government: definition maturity challenges, opportunities and success. European Journal of Scientific Research. pp. 29-42.
22. Vesyropoulos N,. Georgiadis K., Pimenidis E.(2013) Ensuring Cloud Security: Current Concerns and Research Challenges, Proceedings of the 5th International Conference on E-Democracy, Security, Privacy and Trust in a Digital World, Vol. 441, p. 3, Athens: Springer CCIS series.
23. Weber R., Weber R. (2010) The Internet of Things – Legal Perspectives. Springer.
24. Zissis, D., Lekkas, D. (2012) Addressing cloud computing security issues. Future Generation Computer Systems. Vol 28, p. 583–592 (2012). Amsterdam: Science Direct.
25. Zorzi M., Gluhak A., Lange S., Bassi A. (2010) The Internet of Things - From today's intranet of things to a future internet of things: a wireless- and mobility-related view. IEEE.