A Feasibility Analysis of Emergency Management with Cloud Computing Integration

Dimiter Velev, *Member, IACSIT*, and Plamena Zlateva

***Abstract*—Recent emergency situations in the world show the tendency that the occurrence frequency of natural disasters is expected to increase in future. Therefore new approaches for emergency management need to be elaborated based on the latest ICT developments. Cloud computing is considered as a possible way to lower the cost and complexity of computing by providing applications running on the Internet. Many organizations are looking at cloud computing as a new form of emergency management which will keep business continuity. Cloud computing could contribute to emergency management since it could facilitate the sharing of information among private and government organizations. The current article tries to analyze the specific features and problems of cloud computing use as a possible integration component in the emergency management and to generate some basic recommendations for providing support for the business continuity regardless of the natural disaster occurrence.**

***Index Terms*—Cloud computing, emergency management, natural disasters, information system, integration.**

I. Introduction

Landslides, avalanches, earthquakes, tsunamis, volcanic eruptions and floods are some natural calamities that occur due to changes in weather patterns and soil erosion. Natural disasters come without warning and takes lives of tens, hundreds and thousands of people. Natural disasters can destruct entire cities if precaution is not taken. The types of natural calamities are earthquakes, floods, tornadoes, hurricanes, tsunamis, wildfires and thunderstorms. The effects of natural disasters are very serious and the destruction caused may take a very long time to recover. The damage caused by natural disaster is severe and may cause damage of billions of dollars. The natural disasters cause severe damage and after the disasters the destruction continues with outbreak of epidemic diseases, undernourishment, sickness and other diseases [1, 2].

With the increase of natural disasters that have occurred in the past years it is expected their frequency will continue to increase in the coming years. From a business point of view, the evaluation of the risk of a natural disaster occurring comes in when talking about investing in a large in-house infrastructure. However the idea of having everything at the same physical location is not reasonable since all could be destroyed in a flash [3].

Manuscript received January 20, 2012; revised February 27, 2012. This work was supported in part by the University of National and World Economy, Sofia, Bulgaria under Grant NI 1-8/2011.

D. Velev is with the University of National and World Economy, Sofia 1700, Bulgaria (e-mail: dvelev@unwe.acad.bg).

P. Zlateva is with the ISER, Bulgarian Academy of Sciences, Sofia 1113, Bl. 2, Bulgaria (e-mail:plamzlateva@abv.bg).

In order to find alternatives to this problem, a lot of technology experts turn to Cloud Computing in a hope to solve this issue. Cloud Computing permits to have redundancy spread across the world to make sure that even if a part of the world is touched by such disasters, that everything can stay in operating order.

The article attempts to perform an feasibility analysis of the integration of cloud computing technology in emergency management.

II. Cloud Computing

Cloud Computing is a model for providing on-demand Internet-based access to a shared pool of computing resources, including networks, storage and applications. The user of cloud services never has to buy or upgrade computing hardware, not to worry about disaster recovery and significantly simplifying business continuing planning.

The Cloud computing paradigm aims at supplying virtualized and dynamically scalable resources. It is a co-result of the convenience of Internet which lets people access even the distant computing sites. Web applications and tools which can be used easily from a Web browser is what it forms into. Internet is replaced by the metaphor “Cloud” relating it to the sketch which earlier used to depict the functioning of computer in a network.

The abstraction of computing, network and storage infrastructure is the foundation of cloud computing. The infrastructure is a service, and its components must be readily accessible and available to the immediate needs of the application stacks it supports. Cloud computing removes the traditional application silos within the data center and introduces a new level of flexibility and scalability to the IT organization. This flexibility helps address challenges facing enterprises and IT service providers that include rapidly changing IT landscapes, cost reduction pressures, and focus on time to market.

Cloud users are maybe identified as follows [4]:

- Individual consumers;
- Individual businesses;
- Start-ups;
- Small and medium-size businesses;
- Enterprise businesses.

Cloud computing architectures offer to its users numerous advantages that can be briefly summarized to [4], [5]:

- reduced cost since services are provided on demand with pay-as-you-use billing system;
- highly abstracted resources;
- instant scalability and flexibility;
- instantaneous provisioning;
- shared resources, such as hardware, database, etc.;

- programmatic management through API of Web services;
- increased mobility – information is accessed from any location.

Cloud computing turns the computer into a virtual software or application image, which resides on some physical server in the cloud hosting environment. The virtual software image can be diverted between hardware resources, breaking the hardware dependency associated with external hosting. With hardware dependency no longer an issue, a user system is insulated from hardware breakdowns.

If a hosting system fails or overloads, the cloud provider would automatically move the user software image to another piece of hardware while it fixes the original hardware.

If an application starts to demand more resources then what is assigned to it, more resources can easily be added to ensure the system does not suffer.

Cloud connects the hosts with the users though the web. This allows the user to be able to access the resources as long as they have access to the internet [6].

The cloud computing environment usually consists of the following components [7]:

- Servers - Hosting servers in the cloud using the corresponding services means operating those servers a safe distance from any disaster. Cloud hosting providers generally have more redundancy of network connections, mirrored sites and other precautions to ensure access under adverse conditions.
- Applications - People that use cloud-based applications like Google Apps or Microsoft Office 365 can log in and be productive from virtually anywhere and any mobile device.
- Online data - Users will tend to keep their data stored remotely in the cloud. It is available from everywhere, and like cloud applications and it can be accessed from any device capable of connecting to the web.
- Cloud backup - Many companies fail to backup critical systems on a periodic basis at all, but it is even more severe when an organization has taken the time to create the backups, but the backups end up getting destroyed at the same time as the servers and data their backing up. Using a cloud-based backup solution provides for rebuilding the systems and resuming normal operations.

Under some circumstances, virtual appliances or virtual machine images of existing workloads can be created in the data center and stored in a cloud data center. In the event of a failure of the former, the virtual machines serve as recovery mechanisms that can be reactivated in the cloud.

Cloud computing handles resource management in a better way since the user no longer needs to be responsible for identifying resources for storage. If a user wants to store more data they request it from the cloud provider and once they are finished they can either release the storage by simply stopping the use of it, or move the data to a long-term lower-cost storage resource. This further allows the user to effectively use more dynamic resources because they no longer need to concern themselves with storage and cost that accompany new and old resources.

The following cloud computing categories have been identified and defined [4], [8] in the process of cloud development:

- Infrastructure as Service (IaaS): provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service Application Programming Interface (API). IaaS includes the entire infrastructure resource stack from the facilities to the hardware platforms that reside in them. It incorporates the capability to abstract resources as well as deliver physical and logical connectivity to those resources. IaaS provides a set of APIs which allow management and other forms of interaction with the infrastructure by consumers.
- Platform as a Service (PaaS): allows customers to develop new applications using APIs, implemented and operated remotely. The platforms offered include development tools, configuration management and deployment platforms. PaaS is positioned over IaaS and adds an additional layer of integration with application development frameworks and functions such as database, messaging and queuing that allow developers to build applications for the platform with programming languages and tools are supported by the stack.
- Software as a Service (SaaS): is software offered by a third party provider, available on demand, usually through a Web browser, operating in a remote manner. Examples include online word processing and spreadsheet tools, CRM services and Web content delivery services. SaaS in turn is built upon the underlying IaaS and PaaS stacks and provides a self-contained operating environment used to deliver the entire user experience including the content, its presentation, the applications and management capabilities.
- Multi-Tenancy: the need for policy-driven enforcement, segmentation, isolation, governance, service levels and billing models for different consumer constituencies. Consumers might utilize a public cloud provider's service offerings or actually be from the same organization, but would still share infrastructure.

The cloud services can be implemented in four deployment models [5]:

- Public Cloud. The cloud infrastructure is made available to the general public or large industry group and is owned by an organization selling cloud services.
- Private Cloud. The cloud infrastructure is operated entirely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off-premises.
- Community Cloud. The cloud infrastructure is shared by several organizations and supports a specific community. It may be managed by the organizations or a third party, and may exist on-premises or off-premises.
- Hybrid Cloud. The cloud infrastructure is a composition of two or more clouds (private, community or public) that are bound together by standardized or proprietary technology that enables portability of data and application.

Cloud computing has the potential to dramatically level the playing field for small and medium-sized businesses that cannot currently afford to own and operate the type of sophisticated Information Technology systems found in large corporations. Researchers, developers, and entrepreneurs in the world could use Cloud computing to collaborate with partners elsewhere, share their ideas, expand their horizons and dramatically improve their job prospects provided they can gain access to the Cloud. Telecommuters and workers who are on the road will also have access to the same software and data used by those in the office, provided that we increase broadband access in the home and over wireless connections.

As a result, development of the Cloud will increase pressure on governments to bridge the digital divide by providing subsidies or adopting policies that will promote investment in broadband networks in rural and other underserved areas.

Unfortunately, the main impact of many previous efforts to promote network deployment has been to distort the market or protect incumbent carriers from competition. As Cloud computing become critical for a large percentage of companies, governments will need to find cost-effective ways to ensure that homes and businesses have affordable access to the Cloud no matter where they are located [9].

Cloud computing could contribute to emergency preparedness and relief efforts since it could facilitate the sharing of information among central and local governments and make the emergency notification system much more accessible to the public [10]. Cloud computing would enable to build a sound and comprehensive system for disaster prevention and reduction, as well as relief and reconstruction.

III. Cloud Computing in Emergency Management

Emergency management is the generic name of an interdisciplinary field dealing with the strategic organizational management processes used to protect critical assets of an organization from hazard risks that can cause disasters or catastrophes, and to ensure the continuance of the organization within their planned lifetime [11].

Examples of an emergency alert implementation scenarios could be one or more of the following [12]:

- Individual Sensor systems or Building management systems generates alerts (smoke, fire, heat)
- Such alerts can be channelized to a cloud communication service that one implements.
- The cloud service processes the incoming request and initiates (communication) actions.
- The communication actions (alerts) can be such as:
  - Calling one or more Phone numbers (Telephonic call alerts across the world) and Playing a predefined voice message per incoming alerts
  - Calling and Connecting one or more people
  - Sending SMS Alerts
  - Sending MMS alerts
  - Sending Email alerts
  - Initiating safety controls based on remote actions.

Cloud computing offers capabilities to automate many services, to expedite the implementation of secure configurations to information devices, to reduce dependence on removable media due to broadband services, and to lower costs in disaster recovery and data storage.

Many companies and organizations typically store their business information in multiple data systems across many different servers located in different countries around the world. Trying to track down the information that is required and then accessing through some form of networked computer system can be difficult at the best of times. This is difficult if working remotely and there is a need to connect into a business system via a laptop computer. When losing the server architecture, the time needed to rebuild everything can cost a lot. If everything is in the cloud, the organizations can restart their operations as soon as they have access to the Internet.

In cloud operations, it is expected that multiple copies of a data set will be created and kept in sync.

It is important to consider data availability, backups and redundancy as component of the emergency management software selection process [13]. This is especially important in case of a natural disaster where there is a high risk of losing access to computers and data center. The data should be frequently backed up and stored in multiple locations separated by enough distance depending on the type of the disaster. Disasters such as fires, floods and earthquakes are more regional, while hurricanes can affect entire coast lines. It is important that the primary and backup sites are geographically separated in order to ensure that a single disaster will not impact both sites.

This geographic separation adds its own challenges since increased distance leads to higher bandwidth costs and will incur greater network latency. Increased round trip latency directly impacts application response time when using synchronous replication. Synchronous replication is feasible only when the backup site is within tens of kilometers of the primary. Asynchronous techniques can improve performance over longer distances, but can lead to greater data loss during a disaster. Distance can especially be a challenge in cloud services as a business might have only coarse control over where resources will be physically located.

Traditionally data can be backup in three ways [13]:

- Hot Backup Site is a set of mirrored stand-by servers that are always available to run the application once a disaster occurs. Hot standbys typically use synchronous replication to prevent any data loss due to a disaster. This form of backup is the most expensive since fully powered servers must be available at all times to run the application, plus extra licensing fees may apply for some applications. It can also have the largest impact on normal application performance since network latency between the two sites increases response times.
- Warm Backup Site keeps its state up to date with either synchronous or asynchronous replication schemes. Standby servers to run the application after failure are available, but are only kept in a warm state where it may take minutes to bring them online. This slows recovery, but also reduces cost; the server resources to run the application need to be available at all times, but active

costs such as electricity and network bandwidth are lower during normal operation.

- Cold Backup Site - data is often only replicated on a periodic basis. Servers to run the application after failure are not readily available, and there may be a delay of hours or days as hardware is brought out of storage. It can be difficult to support business continuity with cold backup sites, but they are a very low cost option for applications that do not require strong protection or availability guarantees.

The on-demand nature of cloud computing means that it provides the greatest cost benefit when peak resource demands are much higher than average case demands. The cloud can be used to cheaply maintain the state of an application using low cost resources under ordinary operating conditions.

The practice of a business offering a free service to another in an area hit by natural disaster could become a new form of international aid. Under some circumstances virtual machine images of existing workloads can be created in the enterprise data center and stored in a cloud data center. In the event of a failure of the former, the virtual machines serve as recovery mechanisms that can be reactivated in the cloud.

Natural disasters may severely damage Internet access and communications which make it difficult to access cloud-based servers, applications and data storage. The interruption of network availability is usually temporary, while companies that relied purely on local infrastructure may find their servers completely destroyed and their backup totally lost [14].

When a disaster occurs, telephone lines in disaster areas are overloaded with calls. Using cloud computing for the emergency management could also improve the computer database by providing government agencies with detailed, real-time disaster information.

Several layers enable cloud computing to deliver solutions over the Internet: the Application Layer of SaaS applications (e.g. Gmail) and the Platform Layer (e.g. Force.com, Google App Engine) which is the cloud equivalent to an operating system [15].

A key feature of cloud computing is that information of the users is stored in multiple, geographically dispersed data centers that provide extensive backup, data archive and failover capabilities. This includes a multi-level backup strategy of disk-to-disk-to-tape data backups which ensure maximum recovery speed with minimum potential for data loss. Major suppliers of cloud computing infrastructure such as Salesforce.com provide very high levels of service availability through virtualized servers at multiple data centers. Users of web-based services have both their data and server availability protected in the event of a natural disaster.

Recovering data after a disaster costs typically twice as much as replacing compromised hardware and software. In the case of cloud computing, recovery costs are considerably lower since only local computers used to access the Internet are at risk and user data and cloud servers are protected far from the disaster site

In the case of a disaster striking a cloud computing data center, user data will not be lost since suppliers of cloud infrastructure replicate user data and cloud servers across multiple data centers.

If a city that uses cloud computing to manage its community development department had the misfortune to lose all its IT equipment in a hurricane or tornado, it could start the task of rebuilding the next day from any location using laptops and an Internet connection.

A common concern about using a cloud computing application is that data will be less secure. In practice, however, entrusting information assets to a recognized cloud computing provider generally increases the safety of those assets since on premise IT security practices are often sub-standard. Given that smaller IT departments struggle to design, fund and maintain secure systems while cloud computing providers deliver IT infrastructure as their primary business and competence, moving to cloud computing and SaaS will almost certainly increase security for the majority of IT users [7].

One of the advantages using of SaaS applications is that the data is hosted externally, backed up frequently, and stored in multiple redundant locations. With a great probability both application and data will still be available in the case of a disaster. Some of the key considerations in evaluating SaaS applications for emergency management by Cloud Computing are [16]:

- Data Storage - The SaaS vendor should be hosting data in a remote location, and this location should provide secure access to your data. Some SaaS providers receive third-party certification for data and application security, ensuring that your data is stored in a secure location.
- Data Backups - In planning for disaster recovery, it is important that the SaaS vendor have a multi-tiered approach to backups. Data backups should at least occur daily, and there should be secondary backups in a secure offsite location. If data is physically stored in multiple secure locations, then the users will be confident that they will have access to their data and applicationa in the event of a natural disaster.
- Application Availability - SaaS providers should be able to ensure high availability for the user applications. The SaaS provider must be hosting their applications in an environment with reliable power and network infrastructure, a full high-availability infrastructure and redundancy.

All aspects of the service are redundant from the location, network, servers, storage devices, databases and backups. This ensures that users will have access to their applications and data at all times.

One of the benefits of cloud computing is that information and operations are hosted in well protected data centers. Top cloud providers keep information on thousands of systems and in numerous locations. Redundancy, availability and reliability are hallmarks of cloud computing, so that users can access your information quickly, no matter where they are located.

For example, Amazon and Microsoft have data centers all over the world, with tens of thousands of processing units and storage. They have miles of cables, generators and batteries to run these systems for days or even weeks in the event of power disruptions. Many are located in places less susceptible to harm from natural disasters. Some service

providers build data centers underground inside massive concrete buildings. All these precautions ensure that you have access to services and data 24 x 7.

The data involved in emergency management includes geographical data about the infected area, data about shelters and available transportation means, data about victims and relief personnel, available rescuing resources, and measurements from the field. The data may belong to multiple autonomous organizations, such as government organizations, non-governmental organizations, international non-governmental organizations, individuals, communities, and industries.

Therefore, besides integrating and manage data from these different organizations, there is a need to coordinate these organizations by enabling efficient communication and collaboration. Moreover, with the development of Web 2.0 technologies, such as Social Network Sites (SNS), blogs, wikis, and video-sharing, the general public is able to interact or collaborate with each other in a social media dialogue as creators of user-generated content in a virtual. the ubiquity of mobile wireless devices facilitates the general public's involvement in the generation, propagation, and consumption of information – the anywhere and anytime paradigm. Cloud computing can provide data-communication-as-a-service solution to emergency management [12], [17].

Another example is a cloud computing based disaster management system, the system core of which is a Web-based social network server that provides a platform to enable users (workers, first-responders, local disaster-related non-profit organizations, volunteers, and local residents) to access information, communicate, and collaborate in real-time from all types of computing devices, including mobile handheld devices, such as smart phones, PDAs and iPads. The system provides a community-based, effective and self-scalable cloud computing environment in which a diverse set of organizations and personnel can contribute their resources, such as data, knowledge, storage and computing platform to the cloud.

In this way, local communities, institutions/organizations and individuals can seamlessly interact with each other to achieve massive collaboration within the affected area. Future enhancement of the system envisages automatic information integration and improved interoperability between different information sources [18].

The location of a data center can have a significant impact on the performance of applications running in a cloud computing environment. If a cloud computing provider's primary data center is in country that is too far away from the current location of the natural disaster, the performance of that application will be adversely affected by the prorogated time needed for the messages to travel between the data center and the users in disaster condition.

However, there are certain requirements that must be imposed on the utilization of cloud computing in emergency management [19]:

- The cloud provider must be responsible for data confidentiality, integrity and availability. This accounting should not be a cursory exercise, but one that demonstrates complete detailed controllership and accountability at each point (and each vendor they use) within the cloud. Yes, this means during access, authentication, transmission, processing, storage, recovery and destruction.
- Specifications must be prepared regarding ways how the cloud provider will preserve and produce data from requests. Depending on the compliance and legal objectives, this can extend to a few more providers within the cloud and can impact systems that are shared with other cloud clients.
- Data encryption must be considered. The geographical and logical location of its use must be taken into account, the minimum and maximum levels required, laws that may impact use, and if encryption will block the ability to monitor and track the data and threats.
- The cloud provider must possess a crisis management process that will have the appropriate technical, organizational and procedural measures. This can include financial crisis such as vendor bankruptcies, mergers, acquisitions along with traditional areas like weather, geological disruptions, epidemics, etc.

Several additional objectives can be defined regarding cloud computing application in emergency management [20]:

- Using the computing cloud to rapidly converge geographically dispersed global experts at the start of an international incident, deploy a foundation of guidance in accordance with community leaders in a manner that empowers community members through education and smart technologies to support mitigation, response, recovery, and a resumption of societal normalcy at a level of functioning an order of magnitude higher than existed before.
- Using mobile communication devices for rapid threat/damage assessment of occurring events, as well as damage to critical infrastructure inland that necessitates mass sheltering of displaced community members.
- Using the power of non-governmental organizations, rapidly responding government and corporate groups, international groups, social networking communities and other resilient networks to locate and gather information, as well as to send help.

Clouds are secure and though adaptation of authenticity, encryption, and meeting security software regulation large concern about secure can be put aside. The cloud allows for large amounts of computing power over short periods of time, like during a disaster, so relief agencies can respond to anything in the world. The cloud platform allows resources to be used on an elastic basis. Furthermore, the cloud is not in one place, meaning the risk of systems failures substantially decreases. In the case of cloud computing, recovery costs are considerably lower since only local computers used to access the Internet are at risk and user data and cloud servers are protected far from the disaster site [21]. In the case of a disaster striking a cloud computing data center, user data will not be lost since suppliers of cloud infrastructure replicate user data and cloud servers across multiple data centers.

IV. Conclusion

Cloud computing is the best solution to the needs and

requirements of the government, organizations and individuals responding to catastrophic disasters. Cloud computing allows users to create resources on-demand and it can enable an ICT infrastructure that scales in response to the demands of disaster management The availability, scalability, cost, speed of communication and potential security offer solutions to current dilemmas within the emergency response and relief work community are considered. Cloud computing services are more readily available for a response to a catastrophic event. Since the cloud applications are hosted at geographically dispersed locations, they are not at risk of going down if one of the facilities fails. Cloud computing is effective because they can scale when user load dramatically increases. The Clouds allow for flexibility since they can expand quickly as the application demands increase. Cloud computing provides the ability for users to communicate between those in the field with those coordinating efforts outside the field. With cloud computing if one has access to the Internet, whether though cell phone or a computer they can connect with the cloud.

ACKNOWLEDGMENTS

The authors express their gratitude to the Science Fund of the University of National and World Economy, Sofia, Bulgaria for financial support under the Grant NI 21.03-44/2009, titled “Methodology for Business Information Support in the Conditions of Global Economic and Financial Crisis by the Cloud Computing Technology” and the Grant NI 1-8/2011, titled "Methodology for the Implementation of Web-Based Integrated Information System for Risk Assessment Due to Natural Hazards".

REFERENCES

[1] R. Arden, (Aug. 26th, 2011) Surviving a natural disaster with cloud computing. Available: http://edocumentsciences.com/
[2] Globalwarmingandu.com. (2010-b). What is the definition of natural disaster? Available: http://www.globalwarmingandu.com/ natural-disaster/What-Is-The-Definition-Of-Natural-Disaster.html
[3] Globalwarmingandu.com. (2010-a). Cloud computing vs. Natural disasters, Available: http://www.globalwarmingandu.com/natural -disaster/Cloud- Computing-And-Disaster - Recovery.html
[4] J. Rittinghouse and J. Ransome, *Cloud Computing: Implementation, Management and Security*, USA: CRC Press, 2009.
[5] G. Reese, *Cloud Application Architectures: Building Applications and Infrastructure in the Cloud*, USA: O’Reilly Media, Inc., 2009.
[6] S. Mallya. (2010). Crisis management in cloud = Courage under fire. Available: www.prudentcloud.com/cloud-computing-technology/.
[7] T. Bradley. (2011). Embrace the cloud for natural disaster recovery; *PC World*. [Online]. Available: http://www.computerworlduk.com
[8] C. Beukenkamp. (2011). Cloud computing – Demystifying IaaS, PaaS and SaaS. Available: http://www.scmtimes.com/it/ 3044-cloud-computing-demystifying-iaas,-paas-and-saas.html.
[9] R. Michal. (2009). The cloud, the crowd, and public policy, Available: http://www.issues.org/25.4/nelson.html.
[10] C. Babcock. (2011). Cloud becoming a major disaster recovery Strategy. *InformationWeek.* [Online]. Available: http://mobile.informationweek.com/10997.
[11] G. Haddow, J. Bullock, and D. Coppola, *Introduction to emergency management*, Elsevier Inc.: Butterworth-Heinemann, 2008.
[12] L. Juan, L. Qingrui, U. Samee, and G. Nasir. (2011). Community based cloud for emergency management. Available: http://ieeexplore.ieee.org/ xpl/freeabs_all.jsp?arnumber=5966573.
[13] T. Wood, E. Cecchet, K. Ramakrishnany, P. Shenoy, J. Merwey, and A. Venkataramani. (2011). Disaster recovery as a cloud Service: Economic Benefits and Deployment Challenges. Available: www.usenix.org/event/hotcloud10/tech/full_papers/Wood.pdf.
[14] C. Road. (2011). The natural disaster hard to predict makes the best of the disaster backup scheme in the high in the clouds. *Chip Road.* Available: http://www.ipreuse.org/?p=1011
[15] BasicGov. (2009). Cloud computing – Emergency preparedness for local government. Available: http://www.basicgov.com/ docs/White-Papers-Cloud-Computing-Emergency-Preparedness-for-Local-Government-2009.pdf.
[16] J. Wikkerink. (2009). 10 Things every local government should know about SaaS – Part 10: Data availability. Available: http://www.basicgov.com/blog/tag/natural-disaster.
[17] G. Xiaosan and W. Huilian. (2009). Cloud based service for big spatial data technology in emergency management. Available: http://www.isprs.org/proceedings/ XXVIII/7-C4/126_GSEM2009.pdf
[18] Homeland Security News Wire. (2012). New cloud computing based disaster management system. Available: http://www.homelandsecuritynewswire.com/dr20120106-new-cloud-computing-based-disaster-management-system
[19] R. Lawhorn. (2010). Tarantino-style approach to secure cloud computing. *Sec Techno.* Available: http://www.sectechno.com /2010/09/18/ tarantino-style-secure-cloud-computing/.
[20] J. Savageau. (2010). Social networking through disaster – Exercise 24. Available: http://john-savageau.com/2010/09/28/social-networking-through-disaster-exercise24/
[21] Sankar. (2011). Cloud computing for emergency alerts. *Communications and Pro-Active disaster prevention*, Available: http://cloudshoring.wordpress.com/2011/12/10/cloud-computing-for-emergency-alerts- communications-and-pro-active-disaster-prevention/.

Dimiter Velev, Dr. is Associate Professor in the Department of Information Technologies and Communications at the University of National and World Economy, Sofia, Bulgaria. He holds M.Sc. degree in Electroengineering from the Sofia Technical University, Bulgaria and Ph.D. degree in Engineering Sciences from the Institute of Modeling Problems in Power Engineering at the National Academy of Sciences of Ukraine, Kiev, Ukraine. His main areas of academic and research interest are Internet-Based Business Systems Modeling and Development, Service Oriented Architectures, Online Social Networks, Cloud Computing, Web Applications Development and Programming. His lectures cover such disciplines.

Plamena Zlateva, Dr. is currently Associate Professor at the Institute of System Engineering and Robotics at the Bulgarian Academy of Sciences, Sofia, Bulgaria. She hods M.Sc. degrees in Applied Mathematics from the Sofia Technical University and in Economics from the Sofia University St. Kl. Ohridski, and Ph.D. degree in Manufacturing Automation from the Institute of System Engineering and Robotics. Her main areas of academic and research interest are Control Theory, Mathematical Modeling and System Identification, Risk Theory, Risk Management.