Security-and-Privacy-Related Issues on IT Systems During Disasters

Shinsaku Kiyomoto, Kazuhide Fukushima, Yutaka Miyake

Security-and-Privacy-Related Issues on IT Systems During Disasters

Shinsaku Kiyomoto[1], Kazuhide Fukushima[1], and Yutaka Miyake[1]

KDDI R & D Laboratories Inc.
2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, Japan
kiyomoto@kddilabs.jp

Abstract. In this paper, we focus on security-and-privacy-related issues that confront IT systems during disasters. We summarize these security and privacy issues in the context of two major areas of operation: information gathering and system continuity management. Then we provide the results of a survey on techniques for solving these issues. Finally, we discuss outstanding issues facing these the systems.

1 Introduction

Developing emergency and disaster management systems is an important issue in our "computer society". The primary issue is how to share information about a current disaster and the status of resource allocation for emergency management. Atteih *et al.* presented a case study [3] on the implementation of an emergency management information system (EMIS) in support of emergency responders. The incident management system (IMS) [41] proposed by Perry is a tool for marshaling pre-identified and pre-assembled resources for responding to an emergency or disaster. Yao *et al.* built a system [56] that allowed virtual teams of experts to create and discuss the emergency scenario. Collabit [11] is a virtual dashboard that facilitates distributed asynchronous sharing of information in an emergency. Wickler *et al.* considered the use of new media technologies, including virtual worlds on the Internet, for collaboration in disasters [51]. Shklovski *et al.* presented evidence on ICT use [48] for reorientation toward the community and for the production of public goods in the form of information dissemination during disasters. Jang and Tsai proposed a MANET-based emergency communication and information system [29] that could support a large number of rescue volunteers during catastrophic natural disasters. Research [4] by Dilmaghani and Rao identified a set of potential network oriented problems in existing inter-organizational communication protocols incorporating the information collected from several drill exercises and after interviewing first responders. Applications of geospatial information [12, 7] during disaster response have been considered to use a knowledge that can be applied to action plans during future disasters.

Systems using mobile terminals for the management of a disaster must receive some consideration. Fajardo and Oppus proposed a disaster management system [14] that facilitates the logistics for rescue and relief operations. The system

provides the optimum route for rescuing people in a disaster. Zeng *et al.* proposed a mobile communication system [57] for evacuations during emergencies. Ohya *et al.* presented a disaster-information gathering system using mobile phones [37]. However, security-and-privacy-related issues on the systems have not been discussed so far.

System continuity management is another important issue on disaster-related issue. Cloud computing environments have been considered a cost-effective solution for ensuring system continuity. Wood *et al.* performed a pricing analysis to estimate the cost of running a public cloud-based disaster-recovery service and showed significant cost reductions compared to using privately owned resources [53]. Cloud computing environments are also robust in the context of wide-area disasters, and cloud services have been used for system contiunuity management. The Japanese Ministry of Internal Affairs and Communications has assembled a budget of 40 million dallar and has supported to develop cloud computing technologies for wide-area disasters.

In this paper, we focus on the security-and-privacy-related issues that confront IT systems during disasters. We summarize security and privacy issues for two major areas of operation: information gathering and system continuity management. Then we provide the results of a survey on techniques for solving these issues. Finally, we discuss outstanding issues facing these systems.

2 Security and Privacy Issues

In this section, we consider the security-and-privacy-related issues that confront information systems during disasters or other emergencies. Two major functions for IT systems during disasters are system continuity management and information gathering and broadcasting. These items are summarized as follows:

- System Continuity Management. To use a cloud service is a cost-effective solution for system continuity management. However, when a cloud service is used as a backup system, some security issues need to be solved.
- Information Gathering/Broadcasting. During a disaster, information gathering and broadcasting are major issues. In particular, govermental organizations that manage resources for disaster recovery need to gather information, and another organization has the responsibility of broadcasting informartion to users. Concerns about privacy breaches should be considered even during disasters.

We discuss security-and-privacy-related issues on the above two functions in the later subsections.

2.1 System Continuity Management

There is always a risk that servers will be physically damaged in a disaster. To use open cloud architecture is an efficient and cost-effective solution [53] to

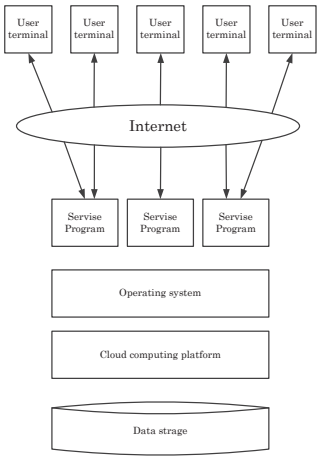

Fig. 1. Cloud Architecture

improve the availability of systems during a disaster. However, several security risks that could affect cloud computing services have been pointed out[36, 25]. It is impossible for users to verify the trustworthiness of all cloud computing environments, and the concern is that operations in cloud computing may be carried out in the absence of trusted environments. The dynamic and fluid nature of the environments will make it difficult to maintain consistent security and ensure the ability to audit records. Thus, moving critical programs and sensitive data to a public and shared cloud computing environment is a major concern for service providers [42]. Now, we consider a model for cloud computing. Figure 1 shows typical architecture of cloud computing. In PaaS services, the platform provider supplies a software development kit (SDK) and service providers develop service programs for the platform. Users can access the services by executing these programs from a user terminal via the Internet. The program can be executed by any server in the cloud environment; thus, system continuity is still maintained even when some cloud servers are damaged.

We discuss three security issues when cloud environments are used to ensure system continuity: secure computation, data backup, and user authentication.

Secure Computation A program that runs on its own servers has to be moved to a cloud environment in the event of a disaster. It is assumed that three kinds of entities try to attack the program on the cloud environment. External attackers can eavesdrop or modify Internet communications between a user terminal and service program. Malicious users try to attack other users to steal secret information or use a service without the correct permission. Furthermore, we have to consider malicious platform providers as an insider threat [24, 47, 30]. However, if the ability of the malicious platform provider is unlimited, we have to assume all possible attacks by the provider, which makes it a very difficult task

to realize secure cloud computing. We consider a reasonable adversary model as follows; the platform provider honestly executes user requests and cannot obtain any information from the execution environment such as physical memory. The platform provider may try to use the user's program maliciously or try to obtain information from data storage. This model is a reasonable model in the situation where we assume that the attacker is the system manager of the platform.

We should consider the following threats to secure cloud computing.

- Malicious users or malicious platform providers may access a service program and execute it on the platform.
- Malicious users or a malicious platform provider may steal user's information stored in the service program.
- External attacker may modify a communication between a user terminal and the platform, or steal user's information from communication data.

Security issues in disaster situations are considered to be security problems for cloud services. Thus, we should find a solution to protect the program against the above threats.

Secure Data Backup If we assume that a database is compromized by a disaster, data backup is another issue that IT systems need to resolve for ensuring system continuity. There are many backup services that allow outsourcing of data backups; however, security concerns should be considered. Chow *et al.* suggested that a major concern [9] for cloud computing is lack of control in the cloud and thus cloud users are for the most part putting only their less sensitive data in the cloud. If a database is compromized and data on an outsourced backup service are used as a temporary system for workflows, an access control mechanism should be prepared. For example, take a data backup service, which is one of the most common services provided by cloud environments, and consider a situation wherein a company backs up their data in the storage service on a cloud environment. If the cloud service is vulnerable or the cloud provider has a malicious/curious administrator, the private information of users and corporate confidential information may be leaked. Furthermore, where a database on acloud service is shared by users, a fine-grained access control mechanism is a mandatory function. Hence, how to realize data encryption and access control without additional implementation on the cloud environment should be considered.

Authentication of Users User authentication is a key component for IT systems in a disaster. In particular, the capacity to respond to a request from disaster victims, such as issuing disaster-victim certificates that is based on an authentication mechanism, has to be resumed as soon as possible. Generally, many IT systems have an authentication mechanism based on an authentication token, ID/PW, and biometric information. There are two serious situations regarding authentication mechanisms as follows;

– Users have lost their authentication tokens due to the disaster.
– Information such as the biometric templates of users has been lost due to the disaster.

If the above situations occur, the IT system cannot authenticate each user, even supposing that the IT system has resumed functioning by using a backup system. One possible solution is to backup all data and programs to a cloud environment and run the programs on the cloud environment. However, this solution may be accompanied by a new security risk and it violates security policy. Another solution is to use a fuzzy encryption [43] for a biometric authentication; The fuzzy encryption can generate a key from biometric information and authenitcate users using the key, but it requires a huge computational cost fo each authentication. It is not a realistic solution to delegate local authentication/identification of users to an outsourced cloud service. Thus, we restore a local authentication/identification system without help from cloud services.

2.2 Information Gathering /Broadcasting

Fraunhofer Gesellschaft conducted a study on disaster and emergency management systems and suggested that timeliness and updating of information is a major requirement for the systems [32]. Mobile terminals are key devices to gather timeliness information for planning emergency responses. There are two key issues for information gathering and broadcasting: privacy control and information accuracy. We discuss the two issses in the following subsections.

Privacy Control A special issue during a major disaster and/or emergency is how an organization responsible for disaster management gathers reliable and useful information. Internet search engines are not an effective means for searching for information about a disaster, and sometimes an information overflow occurs. There are several studies that have examined how to construct a disaster management system using computer networks. The main topic is how to support sharing of information about the current disaster and the status of resource allocation for emergency management. Currently, user-centric systems using mobile terminals are seen as new approaches to achieving a more efficient information-sharing system. It has been suggested that SNS and micro-blogs are effective systems for communication and sharing information during a major disaster. A simple solution for setting up an information-gathering system is to construct a server to which information is uploaded and published. However, such a centralized approach is not flexible and nor is it robust. For example, it is often difficult to find an appropriate system to which the user can upload information in a disaster, and the centralized server may be down because of overload or has been physically destroyed. We must consider a distributed and dynamic architecture for the platform.

How to control the privacy level is an important issue when gathering information during disasters. For example, where a rescue worker is searching for a

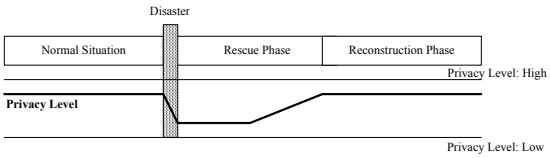

Fig. 2. Privacy Level

person who has a mobile phone, it is very helpful if that mobile phone is able to automatically distribute detailed information on the location of the terminal. On the other hand, privacy should be protected in the reconstruction phase; for example, detailed personal information should be kept secret but people can obtain personalized information that is customized to each person. Figure 2 shows variations in the privacy level according to the phase of the disaster. Thus, technology that flexibly changes privacy levels is required.

Information Accuracy False information may spread in a major disaster, and an attacker may try to confuse governmental organizations or users by broadcasting false or fake information to them. Furthermore, the information may be altered during communications and a masquerading entity may broadcast information to users. Thus, how to ensure the trustworthiness of the information sent from user terminals is an important issue. Generally, it is very difficult for an organization and users to judge whether the information is correct or not. A possible solution is to compare the information with other information; that is, the information is trusted where many messages from many users include the same information. The organization may be able to identify a person who sends a message by tracing logs. This fact may work as a deterrent against the dissemination of false information. However, it is still an open issue as to how to measure the reliability of gathered information.

In a disaster situation, a local and temporary broadcasting service is an effective way to convey emergency messages. It can be realized using a PC and small antennas mounted on a car. The problem is how to confirm that the broadcasting content is sent by an authorized organization. Appending a digital signature to data is a simple answer. A receiver of the data checks the validity of sender of information. However, how to compute a digital signature for content broadcast via a lossy channel is an important issue.

3 Solutions

In this section, we survey the current research aimed at solving security and privacy issues in a disaster situation. Especially, we focus on practical solutions for the issues.

3.1 Solution for System Continuity Management

We have three existing technologies for secure system continuity management.

Software protection Scheme for Cloud Computing There are several secure computation methods based on cryptographic primitives. Garbled circuits (GC) [54, 55] allow secure computation with encrypted functions, and a fully homomorphic encryption scheme [17] allows arbitrary functions to be computed over encrypted data without a decryption key. Bugiel *et al.* proposed an architecture [8] for secure computing, which uses GC as a primitive component. However, their scheme imposes a heavy computation load on cloud environments.

Fukushima *et al.* presented a practical software protection scheme [15] for cloud computing. Their scheme transforms a target program into a protected program and a user program. The protected program is executed on the platform and only handles encoded data. The program receives encoded input and sends back the encoded output to the user program. The user program is executed on the user terminal. This function encodes the input by the user and sends it to the protected program. After receiving the encoded output, the user program checks the validity of the output. If it is valid, the function returns the decoded execution result to the user. The user program encodes the input using encoding rules and checks the validity of the data received from the protected program using a non-trivial relation. Finally, it decodes the execution result of the whole program using a decoding rule.

Another approach to ensure secure computation is monitoring insider activities. Khorshed *et al.* presented evaluation results [26] of popular machine learning techniques, where the techniques are applied to the detection of insider threats.

Attribute-Based Encryption Attribute-based encryption (ABE) schemes are an efficient way to realize both encryption of data and fine-grained access control. Sensitive user data are encrypted under an access policy in ABE schemes, and a user who does not satisfy the access policy cannot decrypt the data. An access policy is described by a user's attributes; for example, appointments, departments, or work location etc.

Attribute-based encryption (ABE) has been extensively researched as a cryptographic protocol [6, 50, 21]. In Ciphertext-Policy ABE (CP-ABE) systems [6], a user encrypts data with descriptions of an access policy. The access policy defines authorized users, their statements consisting of attributes and logical relationships such as **AND**, **OR**, or **M of N** (threshold gates); for example, users who have the attributes "*Project manager*" and "*Control department*" can access the data, where the access policy is defined as "*Project manager* $\wedge$ *Control department*". It is possible to prevent a cloud service provider or an adversary from accessing the secret information. Another type of ABE is a Key-Policy ABE (KP-ABE) [21]. In KP-ABE, a user's personal key is described as a combination of attributes "*Project manager* $\wedge$ *Control department*".

Generally, ABE schemes require a huge amount of computation such as numerous pairing computations. Some papers have dealt with the implementation

of pairing computation on different devices [46, 1]. As shown in these papers, one pairing computation can be completed in less than a few msec on a current PC. However, more computation time is required on other devices that have less computational power, such as smart phones. It is an essential issue for practical use that the computational power of ABE increases according to the increase in the number of attributes.

Delegated Authentication Delegated authentication is one possible way to solve the problem where a local authentication mechanism is lost. The delegated authentication uses other authentication mechanisms and receives an authentication result from other authentication mechanisms. For example, if a local authentication mechanism has been lost, an authentication mechanism of an internet service provider, which performs the duties of the local authentication, is used instead. A local IT system authenticates a user to receive the result from the Internet service provider. Single-Sign-On schemes lend themselves to delegated authentication, even though some existing protocols have been shown to have vulnerabilities by security analyses[2, 49]. Gomi *et al.* [20] introduced a delegation model for federated identity management systems and proposed a delegation framework that is an extension of Security Assertion Markup Language (SAML). Santos and Smith developed a Web-based delegated authentication system [44] using proxy certificates that empowers a user to unambiguously specify a limited subset of his/her privileges to pass to another user. This scheme is also applicable to delegated authentication between two entities, and there are similar existing schemes for delegated authentication.

We have realized a delegated authentication scheme based on existing techniques; however, how to ensure the same security level between two authentication schemes is an issue awaiting resolution.

3.2 Solution for Information Gathering/Broadcasting

We are pursuing several research directions for solving security and privacy issues in relation to information gathering and broadcasting in a disaster situation.

Location Data Management Obfuscation of location information is an effective way to protect user privacy. There are several approaches to obfuscating location information to provide *privacy-aware* location-based services [34, 45]: Kido *et. al.* proposed a *false dummy method* [27], where a user sends n different locations to a location database server, with only one of them being correct (the rest are "dummies" that mask the true location). Hong and Landay introduced an architecture based on *landmark objects* [23], where users refer to the location of a significant object (landmark) in their vicinity, rather than sending an exact location. This scheme makes it difficult to control the granularity of location information and thus may not be suitable for some types of location-based services. For many service providers it is sufficient to provide *approximate*, rather than *exact* location information. The objective of *location perturbation* is

to blur the exact location information. Various location perturbation techniques have been suggested for obfuscating location information. Gruteser and Grunwald [22] suggested "blurring" the user's location by subdividing space in such a way that each subdivision has at least $k-1$ other users. Gedik and Liu [16] adapted this to allow users to have personalized values of the masking parameter k. Mokbel *et. al.* presented a hierarchical partitioning method to improve the efficiency of location perturbation [35]; however it was shown in [18] that this fails to provide location anonymity under non-uniform distribution of user locations. Selection of optimal subdivision spaces was investigated in [31, 5]. Finally, in [18] a decentralized approach without an anonymizer was considered in order to realize good load balancing; however communication between users is required to calculate anonymized location information. Recent research [34] has focused on establishing location anonymity in a spatial domain. This approach uses a *location anonymizer*, which is a trusted server that anonymizes location information within a defined *anonymizing spatial region* (ASR). Location anonymity is provided to the extent that an attacker cannot determine precisely where a given user is in the ASR (although they do know that they are located in the ASR). Existing schemes can control granularity of location information by changing parameters for location anonymization.

Privacy Preserving Information Gathering System Kiyomoto *et al.* proposed the information gathering system [28] shown in Figure 3. They suggested that security and privacy concerns should be addressed when providing information from user's mobile terminals using their platform. If the identity of users can be kept anonymous from governmental organizations, users will find it acceptable to send information to such organizations. They summarize three security and privacy requirements for information gathering systems as follows. Messages on the mobile terminal should be encrypted to protect the privacy of communications. User consent is needed to transfer messages to a governmental organization; thus, the user is required to configure which information is acceptable to send to governmental organizations, so a tagging process should be executed on user terminals. Location information is important for choosing the appropriate governmental organization; however, location information is personal information that may be sensitive in terms of user privacy. Thus, attached location information should be anonymized.

Their system adds a label to messages sent from user mobile terminals and automatically transfers messages to an appropriate governmental organization. In a disaster, messages to a commercial SNS or micro-blog system are copied and transferred to systems of corresponding organizations, where the user accepts the responsibility of providing information to these organizations. The messages have a tag that describes the type of information, and the control server selects the appropriate system according to the tag. The organizations can gather information about the disaster and about people who need support. To improve usability, the tag for each message is selected automatically from among several categories in the mobile terminal. All message content is encrypted by the public key of

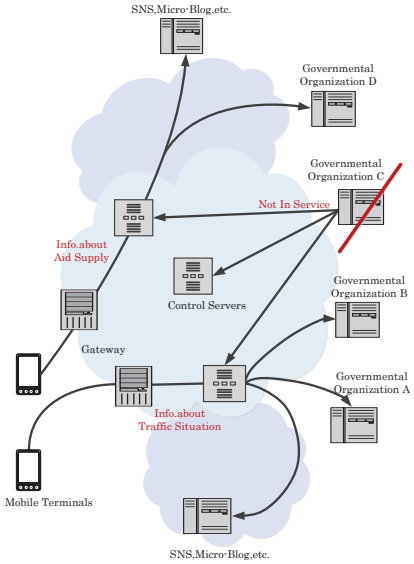

Fig. 3. Information Gathering System

the governmental organizations, thereby avoiding privacy leakage to intermediate entities. The control server is distributed in mobile networks and checks the current status of the systems by frequently accessing the system. If the system of a governmental organization is damaged by a disaster or the organization has insufficient human resources to help people, the control server automatically selects a system from another organization. Their system is designed in accordance with the following principles;

- Tag information is needed for each emergency message in order to deliver it. To avoid leakage of message contents, we execute a categorization mechanism that makes the tag on each mobile terminal.
- Messages should be kept secret from intermediate entities between users and governmental organizations. Thus, messages are encrypted on each mobile terminal.

They assumed the following scenarios as examples;

- **Scenario 1.** Users upload traffic information to the SNS or micro- blog services; for example, some trains have stopped running or stations are closed, there are traffic jams, or there are obstructions on the roads that make it hard to walk or drive. In this situation, the information is copied and transferred to the governmental organizations responsible for traffic control in order to provide support for evacuation of a disaster area.
- **Scenario 2.** A user updates information to SNS or micro-blog services about shortages of aid supplies. The information is copied and transferred to the

nearest governmental organization responsible for aid supplies. If the governmental organization does not have such supplies, the information is transferred to other governmental organizations near the location of the user.
– **Scenario 3.** If a user discovers an emergency involving the collapse of a house and gas leaks, the user would upload such information to the SNS or micro-blog services. In this case, the information is copied and transferred to the governmental organizations (rescuer or police) responsible for the area near the location.

Authenticated Broadcasting Various schemes have been proposed to achieve strong authentication of streaming data on a lossy channel. Wong and Lam proposed two approaches [52] for digital signature schemes tolerating arbitrary loss patterns on received data packets; a group of consecutive packets is signed in the star-chaining technique, and the digital signature is attached to each packet along with hashed values of all other packets in the group. The tree-chaining technique uses a balanced tree of hashed values of packets pertaining to a group. Each intermediate node contains a combination of all hashed values of the child nodes, and the hash value of the root node is signed and the digital signature is included in each packet. Piggy Backing [33] uses a group that is partitioned in a subgroup of packets. A generalization of the simple hash-chaining method has been presented by Golle and Modadugu [19]. Two efficient schemes [40], timed efficient stream loss-tolerant authentication (TESLA) and the efficient multichaining stream signature (EMSS) scheme have been proposed by Perrig *et al.*. The TESLA uses only symmetric cryptgraphic primitives and it is based on timed release of keys by the sender. In EMSS, each packet contains a fixed number of hash values of other packets and the final packet contains the digital signature. Park *et al.* adopted Rabin's information dispersal algorithm to construct a streaming authentication scheme that amortizes a group authentication data over all the group packets [39, 38]. Cucinotta *et al.* presented redundancy techniques [10] in order to avoid losses of packets including a digital signature. Eltaief and Youssef proposed a multi-layer connected chain structure [13] for streaming authentication. Lightweight streaming authentication schemes are ready for practical use; however, how to implement them to commercial products such as mobile phones should be addressed.

4 Concluding Remarks

In this paper, we highlighted two important goals for IT systems operating in a disaster situation: system continuity management and information gathering/broadcasting, and discussed security and privacy techniques for approaching the goal. We can develop secure and privacy-aware IT systems based on existing technologies, but some open issues remain. We these remaining issues will be the subject of future research:

– *Feasibility study of a total cloud system.* We can solve a system continuity problem to use a cloud environment in a disaster, and existing technologies

are used as basic components for construction of a secure cloud environment. We implement all security components on a commercial cloud environment and evaluate the feasibility of the system.
- *Rebuilding of local authentication systems.* Delegated authentication is a temporary solution that can be used during an emergency. How to rebuild local authentication systems is an open issue. We also address peer-to-peer authentication that a person authenticates/authorizes other persons in an ad-hoc manner in a disaster.
- *Correctness of Information.* It is still an open question how we prevent fake information from being distributed during a disaster. Several alert systems are running on commercial network services; a message authentication mechanism should be implemented on client devices.

We hope that this survey is helpful for solving current issues on IT systems during disasters.

Acknowledgment. This work has been supported by the Japanese Ministry of Internal Affairs and Communications funded project, "Study of Security Architecture for Cloud Computing in Disasters."

References

1. D. Aranha, J. López, and D. Hankerson. High-speed parallel software implementation of the η_T pairing. In *Topics in Cryptology - CT-RSA 2010*, volume 5985 of *Lecture Notes in Computer Science*, pages 89–105. Springer, 2010.
2. Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuellar, and Llanos Tobarra. Formal analysis of saml 2.0 web browser single sign-on: breaking the saml-based single sign-on for google apps. In *Proc. of the 6th ACM workshop on Formal methods in security engineering*, FMSE '08, pages 1–10, 2008.
3. Ahmed Sobhi Atteih, Salman A. Algahtani, and Ayman Nazmy. Emergency management information system: Case study. In *GM, Unicom for Communication Technologies,* `http://www.unicomg.com/Home/`.
4. Dilmaghani R. B. and Rao R. R. A systematic approach to improve communication for emergency response. In *Proceedings of the 42nd Hawaii International Conference on System Sciences*, IEEE HICSS '09, pages 1–8, 2009.
5. B. Bamba, L. Liu, P. Pesti, and T. Wang. Supporting anonymous location queries in mobile environments with privacygrid. In *Proc. of 17th International World Wide Web Conference (WWW 2008)*, pages 237–246, 2008.
6. J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. *Security and Privacy, IEEE Symposium on*, 0:321–334, 2007.
7. B. Bhaduri, Bright E. A, and V. Vijayraj. Towards a geospatial knowledge discovery framework for disaster management. In *Proc. of ESA-EUSC 2008*, 2008.
8. Sven Bugiel, Stefan Nurnberger, Ahmad Sadeghi, and Thomas Schneider. Twin clouds: An architecture for secure cloud computing. In *Proc. of Workshop on Cryptography and Security in Clouds, ECRYPT-II*, 20011.
9. Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, and Jesus Molina. Controlling data in the cloud: outsourcing computation without outsourcing control. In *Proceedings of the 2009 ACM workshop on Cloud computing security*, CCSW '09, pages 85–90, 2009.

10. T. Cucinotta, G. Cecchetti, and G. Ferraro. Adopting redundancy techniques for multicast stream authentication. In *Proc. of the The Ninth IEEE Workshop on Future Trends of Distributed Computing Systems*, FTDCS '03, 2003.
11. T. R. de Lanerolle, W. Anderson, S. DeFabbia-Kane, E. Fox-Epstein, D. Gochev, and R. Morelli. Development of a virtual dashboard for event coordination between multipul groups. In *Proc. of 7th International Conference on Information Systems for Crisis Response and Management, ISCRAM 2010*, 2010.
12. Chelsea DeCapua and Budhendra Bhaduri. Applications of geospatial technology in international disasters and during hurricane katrina. In *available at the Project Site of "Capturing Hurricane Katrina Data For Analysis and Lessons-Learned Research"*, 2007.
13. H. Eltaief and H. Youssef. Efficient sender authentication and signing of multicast streams over lossy channels. In *Proc. of 2010 IEEE/ACS International Conference on Computer Systems and Applications (AICCSA)*, pages 1 –7, 2010.
14. JJovilyn Therese B. Fajardo and Carlos M. Oppus. A mobile disaster management system using the android technology. In *INternational Journal of Communications*, volume 3, pages 77–86, 2009.
15. Kazuhide Fukushima, Shinsaku Kiyomoto, and Yutaka Miyake. Towards secure cloud computing architecture - a solution based on software protection mechanism -. *Journal of Internet Services and Information Security (JISIS)*, 1(1):4–17, 5 2011.
16. M. Gedik and L. Liu. A customizable k-anonymity model for protecting location privacy. In *Proc. of the 25th International Conference on Distributed Computing Systems (ICDCS 2005)*, pages 620–629, 2005.
17. C. Gentry. Fully homomorphic encryption using ideal lattices. In *Proc. of the 41st annual ACM symposium on Theory of computing*, STOC '09, pages 169–178, 2009.
18. G. Ghinita, P. Kalnis, and S. Skiadopoulos. PRIVÉ: Anonymous location-based queries in distributed mobile systems. In *Proc. of 16th International World Wide Web Conference (WWW 2007)*, pages 371–380, 2007.
19. Philippe Golle and Nagendra Modadugu. Authenticating streamed data in the presence of random packet loss (extended abstract). In *ISOC Network and Distributed System Security Symposium*, pages 13–22, 2001.
20. Hidehito Gomi, Makoto Hatakeyama, Shigeru Hosono, and Satoru Fujita. A delegation framework for federated identity management. In *Proc. of the 2005 workshop on Digital identity management*, DIM '05, pages 94–103, 2005.
21. V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security*, CCS '06, pages 89–98. Algorithms and Computation in Mathematics, 2006.
22. M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proc. of the 1st International Conference on Mobile Systems, Applications, and Services (MobiSys 2003)*, pages 163–168, 2003.
23. J. I. Hong and J. A. Landay. An architecture for privacy-sensitive ubiquitous computing. In *Proc. of the 2nd International Conference on Mobile Systems, Applications, and Services (MobiSys 2004)*, pages 177–189, 2004.
24. W.A. Jansen. Cloud hooks: Security and privacy issues in cloud computing. In *Proc. of 44th Hawaii International Conference on System Sciences (HICSS)*, pages 1 –10, 2011.
25. Hamlen K., Kantarcioglu M., Khan L., and Thuraisingham B. Security issues for cloud computing. *International Journal of Information Security and Privacy*, 4(2):39–51, 2010.

26. M.T. Khorshed, A.S. Ali, and S.A. Wasimi. Monitoring insiders activities in cloud computing using rule based learning. In *Proc. of 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 757 –764, 2011.
27. H. Kido, Y. Yanagisawa, and T. Satoh. An anonymous communication technique using dummies for location-based services. In *Proc. of IEEE International Conference on Pervasive Services 2005 (ICPS 2005)*, pages 88–97, 2005.
28. Shinsaku Kiyomoto, Yutaka Miyake, and Toshiaki Tanaka. On designing privacy-aware data upload mechanism - towards information-gathering system for disasters -. In *Proc. of The 11th IEEE International Conference on Ubiquitous Computing and Communications (IUCC-2012)*, 2012.
29. Yao-Nan Lien, Hung-Chin Jang, and Tzu-Chieh Tsai. A manet based emergency communication and information system for catastrophic natural disasters. In *Distributed Computing Systems Workshops, 2009. ICDCS Workshops '09. 29th IEEE International Conference on*, pages 412–417, 2009.
30. Yanbin Lu and Gene Tsudik. Privacy-preserving cloud database querying. *Journal of Internet Services and Information Security (JISIS)*, 1(4):5–25, 11 2011.
31. S. Mascetti and C. Bettini. A comparison of spatial generalization algorithms for lbs privacy preservation. In *Proc. of the 1st International Workshop on Privacy-Aware Location-Based Mobile Services (PALMS 2007)*, pages 258–262, 2007.
32. Andreas Meissner, Thomas Luckenbach, Thomas Risse, Thomas Kirste, and Holger Kirchner. Design challenges for an integrated disaster management communication and information system. In *Proc. of DIREN 2002 (co-located with IEEE INFOCOM 2002*, 2002.
33. S. Miner and J. Staddon. Graph-based authentication of digital streams. In *Proc. of 2001 IEEE Symposium on Security and Privacy*, pages 232 –246, 2001.
34. M. F. Mokbel. Towards privacy-aware location-based database servers. In *Proc. of the 22nd Internationl Conference on Sata Engineering Workshops (ICDEW 2006)*, pages 93–102, 2006.
35. M. F. Mokbel, C. Y. Chow, and W. G. Aref. The new casper: Query processing for location services without compromising privacy. In *Proc. of the 32nd International Conference on Very Large Data Bases (VLDB 2006)*, pages 763–774, 2006.
36. National Institute of Standard Technology (NIST). Us government cloud computing technology roadmap, volume ii, release 1.0 (draft). *NIST SP500-293*, 2011.
37. Makoto Ohya, Junsaku Asada, Naoaki Harada, Ryo Matsubayashi, Motoshi Hara, Ryuichi Takata, Masahiko Naito, Masamitsu Waga, and Toshitaka Katada. Disaster information-gathering system using cellular phone with a global positioning system. In *Proc. of The International Symposium on Management System for Disaster Prevention 2006*, 2006.
38. Jung Min Park, Edwin K. P. Chong, and Howard Jay Siegel. Efficient multicast stream authentication using erasure codes. *ACM Trans. Inf. Syst. Secur.*, 6(2):258–285, 2003.
39. Jung Min Park, E.K.P. Chong, and H.J. Siegel. Efficient multicast packet authentication using signature amortization. In *Proc. of 2002 IEEE Symposium on Security and Privacy*, pages 227 – 240, 2002.
40. A. Perrig, R. Canetti, J.D. Tygar, and Dawn Song. Efficient authentication and signing of multicast streams over lossy channels. In *Proc. of 2000 IEEE Symposium on Security and Privacy*, pages 56 –73, 2000.
41. R. W. Perry. Incident management systems in disaster management. In *Journal of Disaster Prevention and Management*, volume 12, No.5, pages 405–412, 2003.

42. Kresimir Popovic and Zeljko Hocenski. Cloud computing security issues and challenges. In *MIPRO, 2010 Proceedings of the 33rd International Convention*, pages 344 –349, 2010.
43. A. Sahai and B. Waters. Fuzzy identity-based encryption. In *Proc. of EUROCRYPT 2005, LNCS*, volume 3494, pages 457–473, 2005.
44. N. Santos and S. W. Smith. Limited delegation for client-side ssl. In *Proc. of the 6th Annual PKI R & D Workshop*, pages 76–90, 2007.
45. Marcello Paolo Scipioni and Marc Langheinrich. Towards a new privacy-aware location sharing platform. *Journal of Internet Services and Information Security (JISIS)*, 1(4):47–59, 11 2011.
46. M. Scott. On the efficient implementation of pairing-based protocols. Cryptology ePrint Archive, Report 2011/334, 2011. `http://eprint.iacr.org/`.
47. S. Sengupta, V. Kaulgud, and V.S. Sharma. Cloud computing security–trends and research directions. In *Proc. of 2011 IEEE World Congress on Services (SERVICES)*, pages 524 –531, 2011.
48. Irina Shklovski, Leysia Palen, and Jeannette Sutton. Finding community through information and communication technology in disaster response. In *Proceedings of the 2008 ACM conference on Computer supported cooperative work*, CSCW '08, pages 127–136, 2008.
49. Rui Wang, Shuo Chen, and XiaoFeng Wang. Signing me onto your accounts through facebook and google: a traffic-guided security study of commercially deployed single-sign-on web services. In *Proc. of 2012 IEEE Symposium on Security and Privacy, to appear*, 2012.
50. B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Public Key Cryptography - PKC 2011*, volume 6571 of *Lecture Notes in Computer Science*, pages 53–70. Springer, 2011.
51. G. Wickler, S. Potter, A. Tate, and J. Hansberger. The virtual collaboration environment: New media for crisis response. In *Proc. of 8th International Conference on Information Systems for Crisis Response and Management, ISCRAM 2011*, 2011.
52. Chung Kei Wong and S.S. Lam. Digital signatures for flows and multicasts. *IEEE/ACM Transactions on Networking*, 7(4):502 –513, 1999.
53. Timothy Wood, Emmanuel Cecchet, K. K. Ramakrishnan, Prashant Shenoy, Jacobus van der Merwe, and Arun Venkataramani. Disaster recovery as a cloud service: economic benefits & deployment challenges. In *Proceedings of the 2nd USENIX conference on Hot topics in cloud computing*, HotCloud'10, 2010.
54. Andrew C. Yao. Protocols for secure computations. In *23rd Annual Symposium on Foundations of Computer Science*, pages 160 –164, 1982.
55. Andrew Chi-Chih Yao. How to generate and exchange secrets. In *27th Annual Symposium onFoundations of Computer Science*, pages 162 –167, 1986.
56. X. Yao, M. Turoff, and R. Hiltz. A field trial of a collaborative online scenario creation system for emergency management. In *Proc. of 7th International Conference on Information Systems for Crisis Response and Management, ISCRAM 2010*, 2010.
57. Qing-An Zeng, Heng Wei, and V. Joshi. An efficient communication system for disaster detection and coordinated emergency evacuation. In *Proc. of Wireless Telecommunications Symposium, WTS 2008*, pages 329–333, 2008.