Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 135257, 11 pages
http://dx.doi.org/10.1155/2014/135257

Research Article

Framework for a Cloud-Based Multimedia Surveillance System

M. Anwar Hossain

College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

Correspondence should be addressed to M. Anwar Hossain; mahossain@ksu.edu.sa

Received 3 November 2013; Accepted 27 February 2014; Published 18 May 2014

Academic Editor: Mohammad Mehedi Hassan

The new generation of multimedia surveillance systems integrates a large number of heterogeneous sensors to collect, process, and analyze multimedia data for identifying events of potential security threats. Some of the major concerns facing these systems are scalability, ubiquitous access to sensory data, event processing overhead, and massive storage requirements—all of which demand novel scalable approach. Cloud computing can provide a powerful and scalable infrastructure for large-scale storage, processing, and dissemination of sensor data. Furthermore, the integration of sensor technology and cloud computing offers new possibilities for efficient development and deployment of sensor-based systems. This paper proposes a framework for a cloud-based multimedia surveillance system and highlights several research and technical issues. A prototype surveillance system is also designed and analyzed in the context of the proposed surveillance framework. The paper finally reports that cloud-based multimedia surveillance system can effectively support the processing overload, storage requirements, ubiquitous access, security, and privacy in large-scale surveillance settings.

1. Introduction

Modern multimedia surveillance systems [1–3] are comprised of a large number of heterogeneous sensors distributed over multiple sites. These systems record, process, and analyze different sensor media streams to identify events of interest that are important to the decision makers. Despite significant benefit these systems provide, they tend to reach their limit in terms of scalability, resource utilization, ubiquitous access, searching, processing, and storage when large-scale surveillance support is required. In order to overcome this situation, a new breed of cloud-based surveillance systems has just started to emerge [4–7], which utilize the enormous processing capability, storage, and other resources provided by the cloud infrastructure.

However, significant research and technical challenges remain for developing a cloud-based multimedia surveillance system. Some of the challenges are, for instance, what is the best strategy for sensor data acquisition and storage to the cloud environment, how to dynamically allocate cloud resources for real-time processing of sensor data, what is the optimal approach for event notification and sharing, and so forth. Such challenges stem from the fact that diverse design decisions need to be made given the abundance of cloud resources and the specific requirements of a surveillance system. Existing work in this direction studies several aspects of cloud-based surveillance system design, for example, dependability characteristics [8], resource allocation [9], video recording [10], cloud storage mechanism [6], and cloud computing suitability for video surveillance [4, 11]. However, a holistic approach to develop a multimedia surveillance framework on cloud infrastructure addressing the aforementioned challenges is still missing, which we aim to propose in this paper.

As evident from the literature, existing research foresees significant potential for cloud-based multimedia surveillance systems. However, issues such as cost [4], privacy [12], and security [13] make some organizations wonder whether or not to opt for cloud-based solutions [14]. Some may also argue that a strong local control is needed on all surveillance data acquired, and a cloud approach may seem not needed. Nevertheless, with the availability of some commercial cloud-based video surveillance solutions (also known as video surveillance as a service or simply VSaaS) and strong research on cloud technology, the signs of its potential growth look bright.

This paper reports several distinctive issues of a cloud-based multimedia surveillance system and discusses the different design choices that come into play. It further proposes a general cloud-based surveillance system framework and analyzes it in light of the different design issues. As a proof of concept, a prototype surveillance system has been developed based on the proposed framework.

The remainder of this paper is organized as follows. Related works are described in Section 2, while the design issues of a cloud-based multimedia surveillance system are elaborated in Section 3. Section 4 introduces the proposed cloud-based surveillance system framework, and the prototype development is elaborated in Section 5. Experimental results are given in Section 6, followed by a discussion of concerns in Section 7. The conclusion and future work are in Section 8.

2. Related Work

Multimedia surveillance over cloud is an emerging research area. In traditional surveillance systems, a lot of resources related to infrastructure are required to conduct the surveillance operations. In cloud-based surveillance, the infrastructure is provided by the cloud vendor on a utility-like payment basis. Besides, cloud provides enormous resources on-demand, which is beneficial to many. However, such approach comes with several challenges as well. Literature review shows that there is a growing interest in addressing these challenges and adopting the cloud technology. The following section briefly comments on the existing literature.

A cloud-based video surveillance system is proposed in [6] with emphasis on storage. They analyzed the storage requirements of a traditional surveillance system and justified their choice of a cloud-based storage model as an alternative to that of traditional approach. This paper also addresses the optimization aspect of video transmission over to the cloud and investigated a secure and efficient cloud storage system. In another work, Zhao et al. also [5] studied the cloud storage mechanisms and identified its pros and cons with respect to video surveillance applications.

Karimaa [8] studies the dependability characteristics for the possible expansion of video surveillance technologies over the cloud infrastructure. More specifically the author reviewed availability, security, reliability, and maintainability attributes of the cloud-based video surveillance solutions and identified potential advantages in this technology.

Recently, Neal and Rahman [4] conducted a detailed analysis to explore whether cloud computing is suitable for high-resolution video surveillance management system (VMS). The authors identified that although cloud computing is a viable solution for VMS application, there are issues such as cost, legal issues, and other threats that need to be studied further. Similarly, the author in [11] conducted a suitability analysis of cloud-based multimedia surveillance solutions and reported positive experience with some reservation to security and privacy aspects.

Authors in [10] reported the design of a cloud-based scalable video recording system. Aside from video recording, their system also provided backup and monitoring features. They used Hadoop distributed file system for storing video recording. The authors consider cloud as a suitable platform to conduct video recording and analysis tasks. The authors in [15] reported their experience in designing video service as a service. Their work concentrated on the deployment of a software as a service platform for video surveillance and people reidentification in multicamera surveillance system.

A dynamic resource allocation mechanism for service composition in cloud is proposed in [9]. The authors suggested that for multiple surveillance services, a number of virtual machines need to be optimally utilized. They adopted a linear programming approach to demonstrate their proposal.

Overall, the above works demonstrate different aspects of cloud-based surveillance systems. However, the distinctive design issues and choices relevant to a cloud-based multimedia surveillance system and how these issues contribute to defining a surveillance system framework as a whole were missing. This paper concentrates on this gap.

3. Design Issues of a Cloud-Based Multimedia Surveillance System

From the point of view of a surveillance system, there are several distinctive issues that need exploration, especially when such a system is based on the cloud infrastructure. These are summarized as follows.

3.1. Deployment Architecture. Cloud-based surveillance system architecture can be designed to be deployed on public cloud, private cloud, or a combination of both, which is termed as hybrid cloud [16]. A brief discussion on them follows.

(i) In the public cloud setting, the cloud infrastructure is open for general user. Also, as it remains on the premises of cloud provider, surveillance customers often have the fear of losing control on their data and are concerned for potential data loss. However, the current cloud providers, such as Amazon cloud, take utmost measures to ensure their customers of any such mishaps.

(ii) In the private cloud-based multimedia surveillance system, the cloud infrastructure is exclusively used by a single organization, where it may be hosted and it guarantees enhanced data security, privacy, and ownership.

(iii) The third design choice is a composition of the two, where an organization may decide to put critical surveillance data in private cloud while leveraging public cloud for ordinary and insensitive data.

It is finally up to the organization who would analyze the requirements of the surveillance systems they design and make a trade-off among the possible deployment choices they have.

3.2. Media Acquisition. It is important to choose a suitable strategy to capture sensor data streams and store it in the cloud storage. Several design choices exist in this case, for instance, push-only, pull-only, push-pull, event-driven, and so forth. A brief description of these is given below.

(i) Through push-only, the connected sensors may continuously push the sensor data stream to the cloud [17]. In this approach, the receiving end of cloud environment must adopt special mechanism to handle the continuous flow of received data streams.

(ii) Pull-only approach allows the cloud infrastructure to pull the data stream from the sensor in an on-demand fashion. This mechanism takes the burden of round-trip data query for each data request from the cloud [17]. However, if the data needs are minimal and intermittent, this mechanism has the potential of reducing the consumption of energy and bandwidth.

(iii) Push-pull mechanism is a hybrid approach to balance the trade-offs between push-only and pull-only mechanisms. The combination of push and pull mechanisms offers several benefits, such as reduced network traffic, minimized cost of sensor sampling, and reduced energy consumption. Figure 1, adapted from [17], shows a schematic view of push-pull mechanism. It reflects that the media acquisition process can use either push or pull in the same session depending on the situation.

(iv) Event-driven mechanism is a popular approach, where sensor data streams are only pushed to the cloud when some basic event (i.e., motion detection) is identified in the input data streams at the client side. This approach can significantly reduce energy consumption and bandwidth [18] due to minimal data transfer to the cloud environment as compared to continuous transfer.

Therefore, depending on the requirement of a surveillance application, any of the above data acquisition approaches can be adopted with varying performance impact on surveillance system.

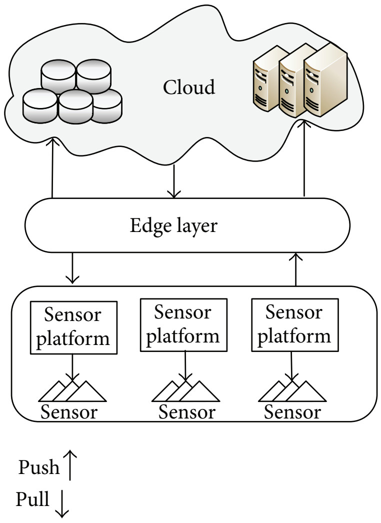


Figure 1: Push-pull mechanism among sensors, middle layer (edge), and cloud.

3.3. Cloud Storage. Typical surveillance systems have high demand for large storage to store huge amount of data coming from multiple sensors. These data are processed in real-time and often in an off-line fashion to detect safety events [6, 8]. However, typical surveillance systems cannot cope with the continuous demand for massive storage. A cloud storage comes as a rescue that can connect different types of network storage devices to meet specific requirements of surveillance systems, such as (a) record media streams in higher frame rate without dropping frames, (b) cost-effective storage for longer retention of media data, and (c) elastic storage capability for varying demand and future growth, among others [19]. Besides, the cloud storage is considered as highly available, always-on, and more reliable than the local storage [20]. As a result, it cannot only meet the needs for large surveillance systems, but also provide intelligent video analytic as a service on-demand to several customers. However, there are several key concerns that need design decisions when using cloud storage. Some of these concerns are as follows.

(i) Vendor lock-in [21] is an important issue that concerns surveillance customers. Because cloud storage service differs in performance, price, and often geographic distribution of data stores, it may become troublesome and expensive for customers to switch vendors. This is critical for the customers as it deals with sensitive surveillance data.

(ii) Disaster recovery capability [22] is an important factor to consider when choosing cloud storage due to the sensitive and often private data a surveillance system handles. A cloud storage provider that offers a solid disaster recovery mechanism will have less downtime and hence ensure continuous public safety and security.

(iii) Elasticity [21] of cloud storage is an important factor for surveillance customer, which ensures that cloud provider has the capability of dynamically mitigating the variability in storage demand. The performance of a surveillance system can be greatly influenced if flexible storage elasticity is not provided by the cloud provider.

(iv) Suitable security and privacy policy must be in place for cloud storage. There are different choices, such as enforcing public auditing [23] for ensuring data privacy and integrity.

(v) Payment and pricing structure [22, 24] drives the selection of cloud provider. A surveillance system that

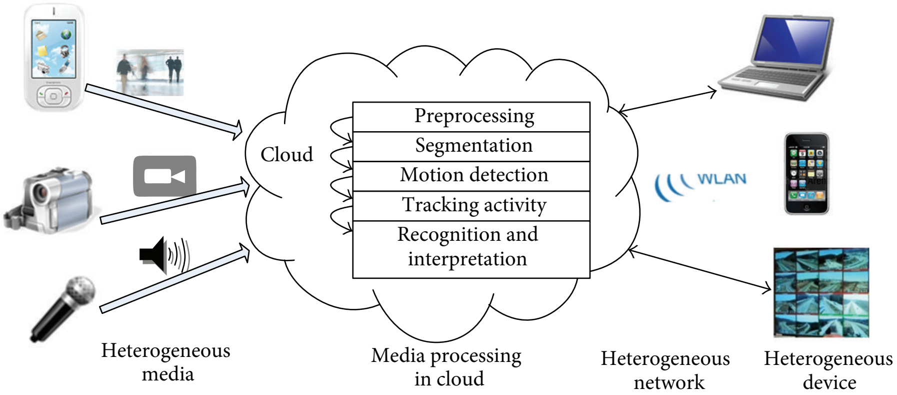


Figure 2: Media processing for event detection in the cloud.

requires massive storage support needs to agree on a pricing model before it can go for particular cloud vendor.

When designing and deploying a surveillance system, it is important to look into the above issues and adopt a suitable cloud storage mechanism that can serve the purpose.

3.4. Media Processing. Different sensors in a multimedia surveillance system generate a massive amount of media data that often need to be processed in real time to detect timely events. Traditional surveillance systems, which include a finite set of processors and servers, can easily be overloaded by heavy media processing depending on the number of surveillance tasks. Therefore, the cloud-based processing of surveillance data seems promising due to the enormous processing capability that can be leveraged. However, media processing in cloud environment brings lot of challenges [20]. From a surveillance system context, these can be briefly stated as follows.

(i) Media processing for surveillance systems is usually performed to support a variety of multimedia analysis tasks, such as face detection, face recognition, motion detection, people tracking, and crowd density estimation. A surveillance system, while receiving different sensory media streams in the cloud, performs these tasks in order to identify hazardous security events and generates alarms when necessary. A high-level view of surveillance media processing architecture is given in Figure 2. The challenges in this configuration are that sensor media are of heterogeneous types and hence different media analysis tasks consume varying amount of time and resources. Like the different media types, challenges also remain to address the heterogeneity of QoS, network, and devices [20], such that surveillance content can be delivered to diverse client devices through different types of network links and maintaining QoS guarantee.

(ii) It is important to decide whether to develop a real-time surveillance system such that all the media streams are processed instantly in the cloud. Few factors in this respect are worth mentioning, such as the required frame rate at which the media is captured, the number of pixels, the speed of the media processing algorithm, and the dynamic provisioning of resources needed to support the processing. Besides real-time processing, major computation in cloud occurs for off-line processing of surveillance video feeds. Many evidences used for criminal investigation are discovered during off-line media processing. Although time is not critical for off-line media processing, it is important to reserve sufficient resources for different off-line tasks.

(iii) Special considerations need to be made when media processing meets mobile cloud computing [25], which is a highly dynamic environment that receives huge volume of mobile media contents.

Overall, media processing is central to cloud-based multimedia surveillance system. A system can either process media in real-time and/or off-line fashion; however, it also depends on the capability of the surveillance system, the algorithms, the number of frames processed per second, and the high-level requirements of the system. The design of a surveillance system should focus on these aspects for supporting large-scale media processing in cloud.

3.5. Resource Allocation. Due to the massive storage and processing resource requirements for surveillance applications, traditional surveillance systems encounter a limit on how many such resources are available and utilized. Therefore, when such resources move to cloud environment, the capability of surveillance systems grows rapidly. Cloud resources are computational resources in the form of virtual machines (VMs) that are utilized on-demand and are deployed in a cloud provider's data center [26]. Not only are cloud resources provisioned on-demand, but they can also be utilized on pay-as-you-go basis [27]. This option is particularly interesting to a multimedia surveillance system that needs on-off resources, depending on the event detection tasks at hand. In cloud-based multimedia surveillance context, the resource requests to handle different surveillance tasks are translated in the form of VM resource requests, which are then mapped to

VM resource allocation to reserve physical server resources hosting the VMs. The massive storage and processing of surveillance data streams demand for an efficient QoS-aware resource allocation mechanism [9] that should cope with dynamic changes in network conditions, resource connectivity or associated cost, online or offline changes of user requirements [28], and other factors. There are several design considerations when devising a suitable resource allocation model. These are as follows.

(i) The resource allocation mechanism is basically a task of optimizing resource selection on the cloud, which aims to satisfy an optimization goal, for example, maximizing the resource utilization while minimizing the response time and cost,, finding a balance between resource utilization, response time, or cost, making a trade-off between average service waiting time and long-term service cost, maximizing individual profit or minimizing loss, balancing the load distribution equitably across all resource possessing nodes, and so forth.

(ii) There exist many different resource allocation strategies for cloud resources to satisfy the optimization objectives, such as game-theoretic approach [29], dynamic programming model [30], and genetic algorithm [31].

(iii) A particular resource allocation model also depends on the various choices made for media acquisition, storage, processing, and sharing mechanism.

(iv) Due to dynamic event occurrences in surveillance context, a surveillance system needs to determine a suitable dynamic resource allocation model, rather than depending on a cloud provider's predefined solution.

Therefore, cloud-based multimedia surveillance systems need to investigate the above issues and accordingly develop a resource allocation model suitable for the application in context.

3.6. Notification and Sharing. Major issues driving multimedia surveillance systems are the timely notification of events and ubiquitous sharing of surveillance footage from anywhere and anytime by the authorized surveillance users. It is expected that a security manager, in case of an emergency incident, is able to share live video footage with police or other law enforcement agencies in order to receive immediate response. One way to facilitate this is to develop a publish-subscribe engine [32] through which the surveillance customers can publish the event information while the users can receive the published content based on some subscription. In a cloud-based multimedia surveillance system, the publish-subscribe mechanism is also deployed on cloud platform, enabling it to utilize cloud resources on-demand. Several design issues worth mentioning here are the following.

(i) Like typical publish-subscribe system, a cloud-based publish-subscribe system [33] needs to state how the subscriber expresses their interest (e.g., topic-based, content-based, type-based, and parametrized) and how matching is performed by the notification system.

(ii) It is important to determine how information is disseminated or propagated from publishers to subscribers. Usually it uses multicast approach to connect and deliver surveillance media streams to various surveillance users. Also, it is possible to utilize broker-level and P2P overlay network architecture.

(iii) Which event processing/matching algorithm is used is an important design consideration.

(iv) Also of concern is how much information is to be disseminated and shared, as in a multimedia surveillance system video evidences which often need to be shared with multiple stakeholders.

All the choices just mentioned will have an impact on the performance and usefulness of the particular publish-subscribe mechanism in cloud environment.

3.7. Crowd-Based Surveillance and Big Data Analytics. The emergence of smart phones, cameras, and social networking brought new opportunities to multimedia surveillance domain. Unlike traditional surveillance system, where data is only captured from the deployed sensors, today's surveillance capability extends to incorporate crowd-based incidents reporting, which are potential clues for crime investigation [34, 35]. Already, surveillance footage is the largest source of big data [36], and the new approach of crowd-supported surveillance is making things even bigger. Therefore, when cloud becomes the host of all these data, a cloud-based surveillance system can obtain the benefit of collective intelligence. However, several considerations are associated with these new phenomena, which are as follows.

(i) Big data brings data analysis and manipulation challenges in the cloud for surveillance purpose. The big question comes from whether it is useful, whether it improves the fidelity of information, or whether it improves the timeliness of response [37].

(ii) Big data comes with challenges related to data security and privacy. Hence, selecting the right mechanisms to protect data and safeguard privacy is a big choice that has a greater impact on surveillance activity.

As crowd-based surveillance and big data bring new opportunity, the challenges just mentioned need to be addressed to reap its benefit.

3.8. Security and Privacy. Security and privacy are an important issue for sensor information management in cloud environment [38]. In the absence of proper security and privacy policy, the deployment of cloud-based multimedia surveillance system will hamper. This is relevant to several issues that need attention, such as the following.

(i) Surveillance footage must be secured and withstand various security threats. Different approaches are

Table 1: Summary of the issues and design choices related to a cloud-based multimedia surveillance system.

Distinctive issues	Design choices
Deployment architecture	Public, private, and hybrid
Media acquisition	Push-only, pull-only, push-pull, and event-driven
Cloud storage	Vendor lock-in, disaster recovery, elasticity, security and privacy, and payment and pricing
Media processing	Different media processing tasks, heterogeneity of QoS, network and devices, and mobile cloud considerations
Resource allocation	Different optimization goal (maximized resource utilization versus minimized response time and cost, trade-off between average service waiting time and long-term service cost, maximized profit versus minimized loss, and equal load distribution)
Notification and sharing	Publish-subscribe mechanisms (topic-based, content-based, type-based, parametrized), mode of information dissemination, event-matching algorithms, and volume of information
Crowd-based surveillance and big data analytics	Usefulness of big data, fidelity of information, timeliness of response, and data security and privacy
Security and privacy	Cryptographic approach, various authentication and identity management approaches, different access control policy (RBAC, TBAC, and ABAC), and security impact on cloud deployment choices
Performance issues	Several performance metrics (accuracy of event detection, response time, CPU and storage utilization, workload, cost trade-off, average task waiting time, QoS, QoI, and QoE)

adopted to ensure security at different levels, such as cryptographic approach for cloud storage security [39], to make sure customers are confident in the services provided by cloud vendor.

(ii) There are various authentication and identity management approaches, which can provide varying level of security for accessing cloud [40].

(iii) Privacy enforcement mechanism can influence many customers whether to choose cloud or not for multimedia surveillance infrastructure. Several access control policies exist that have varying level of acceptance, such as role-back access control (RBAC), threshold-based access control (TBAC), and activity-based access control (ABAC). A cloud-based surveillance system can leverage a suitable access control policy among the various choices.

(iv) Which cloud deployment architecture, such as private versus public, is chosen will have an impact on the security and privacy of the cloud-based surveillance systems.

It is thus important to identify the security and privacy leakage channels in cloud-based multimedia surveillance systems and take strong measure to mitigate any relevant threats.

3.9. Performance Issues. A cloud-based multimedia surveillance system can leverage huge storage and computing resources in exchange of certain cost. Therefore, it is important to measure performance implications of different surveillance-related tasks. Few factors related to performance are highlighted in the following.

(i) It is important to identify the quality parameters that need to be measured, for example, accuracy of event detection, response time, CPU and storage utilization, workload, cost trade-off, average task waiting time, and so forth.

(ii) Another important aspect is to determine whether the cloud-based processes and services provide QoS guarantee. Measuring quality of information (QoI) [41] and quality of experience (QoE) [42] is also needed due to the importance of event detection and sharing activities done by surveillance systems.

Depending on the choices of several factors concerning cloud storage, media processing, resource allocation, and so forth, the performance of the overall surveillance system will be determined. It may be worthwhile to develop a quality framework for measuring the overall performance of cloud-based surveillance systems.

A summary of the different issues and design choices is presented in Table 1.

4. Proposed Surveillance Framework

Figure 3 shows the architecture of the proposed cloud-based multimedia surveillance framework. It is motivated by several design aspects and issues that have just been described. The proposed design highlights the different content providers, surveillance users, and the internal core components and services of the system. An elaboration of these follows.

4.1. Surveillance Content Providers. Two types of content providers exist in this architecture. One is the heterogeneous sensor devices, such as fixed cameras, IP cameras, and PTZ cameras, while the other is the crowd that reports security incidents. The content from multiple sources is transmitted to the cloud through a publish-subscribe mechanism. Different media acquisition alternatives are considered here. A user with proper authentication can configure the connected device(s) and control the sampling rate by which the media

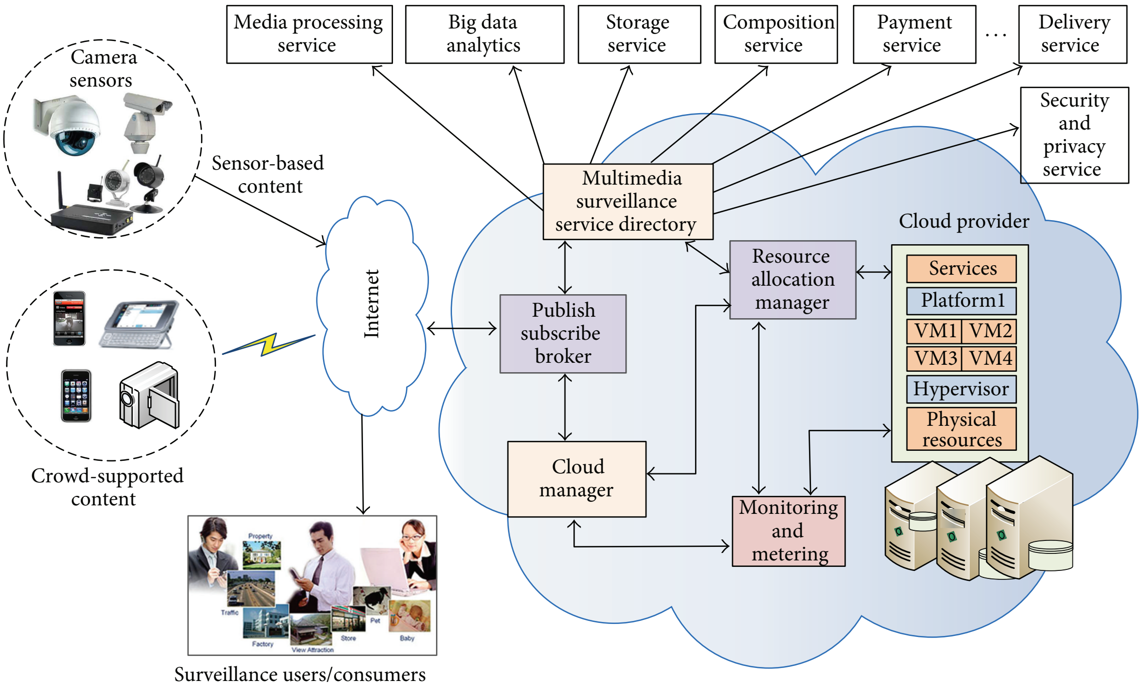


Figure 3: Proposed cloud-based multimedia surveillance framework.

is captured and delivered to the cloud. A user is also able to configure whether the media is captured continuously or event-driven.

4.2. Surveillance Users or Consumers. Surveillance users are the ones who consume the content. Content in this case is the event information consisting of multimedia data and event highlights. The users are the typical surveillance operators such as CCTV operators, or they could be any security officials accessing media from anywhere. They usually subscribe to the surveillance events or sensor footage as per their interest and accordingly the matching events or streams are delivered to the client.

4.3. Core System Components. There are several core components in this framework. Their design considers the issues described earlier. The following paragraphs elaborate the components. Publish-subscribe broker is one of most vital components of the proposed framework that facilitates publishing and subscribing the media streams as well as disseminating the events of interest to the appropriate clients. It is located in the cloud side because of its higher performance in terms of bandwidth and capabilities. It is the main backbone to provide ubiquitous video surveillance service with scalability. It uses multicasting approach to connect and deliver surveillance video streams to various surveillance content providers and users [11].

Multimedia surveillance service directory: the proposed system adopts a service oriented architecture style and hence all its functionalists are exposed as services that are accessible over the internet. These services are registered in the multimedia surveillance service directory.

Cloud manager: the overall management of the cloud-based operations of the proposed framework is managed by this component. It acts as the bridge between the users and the cloud-based surveillance system components. It also manages the publish-subscribe broker, multimedia surveillance service directory, the resource allocation manager, and the monitoring and metering component.

Monitoring and metering: cloud computing adopts a utility-like resource usage and billing approach or a pay-as-you-go model. Hence the monitoring and metering component is responsible for performance monitoring and usage tracking of cloud virtual machine (VM) resources and provides statics of usage and billing.

Resource allocation manager: it manages and allocates various VM resources for running the surveillance system and associated services. Upon receiving the sensor media streams, new VMs instances are initiated as per demand. These VMs will function as the surveillance media processing servers, which will be communicating directly with the client device interface. It also configures VM capacities dynamically according to the current workload demands. It can facilitate migration of VMs between physical servers in order to (i) pull out physical servers from an overloaded state when the sum of VMs capacities mapped to a physical server becomes higher than its capacity and (ii) turn off a physical server when the VMs mapped to it can be moved to other physical servers. When new service joins or VM migration is needed, it uses a VM allocation algorithm to find proper physical server [11].

4.4. Services Stack. In order to accomplish the target surveillance tasks, various services are defined. These include the media processing service (e.g., face detection service, motion detection service, and event detection service), storage service, big data analytics service, payment service, composition service, media delivery service, and security and privacy service.

5. Prototype Development

A prototype system is developed to implement the different functionality of the proposed framework. The following is a description of the development process and the prototype.

(i) Amazon EC2 public cloud platform is used for deployment. For normal operation, two instances were launched—one to store the captured information (alerts info and queries info) and the other for different web services. The web services demonstrate pub-sub mechanisms that manage sharing/accessing process in a way such that the information can be accessed from heterogeneous devices from anywhere and anytime.

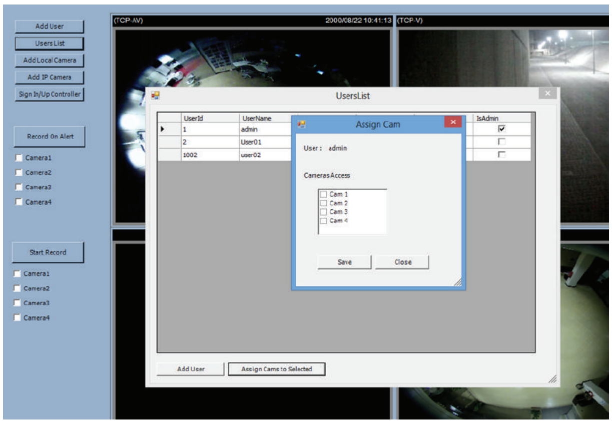
(ii) Several other web services have been developed, for example, face detection service, motion detection service, and media processing service.

(iii) VIVOTEK cameras were used to capture image and be connected to cloud.

(iv) The developed prototype allows the user to freely choose between continuous and event-driven data acquisition. The user can, for example, select a camera and put it in record mode based on event occurrence (e.g., when an object is detected, or an alert is generated that requires recording). The user can also put all/selected cameras in the record mode and accordingly the captured frames can be sent to the cloud.

(v) A sharing of information functionality has been implemented, which allows an admin user to assign cameras to the other users who can share their information with other users using queries based on SQL server 2012.

Figures 4 and 5 show two screen shots—the first one shows the admin adding new users in the system and adding camera for his view, while the second figure shows the generated alerts and corresponding responses.



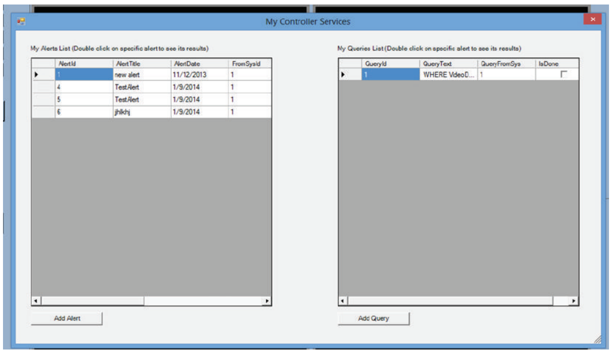
	UserId	UserName	IsAdmin
▶	1	admin	☑
	2	User01	□
	1002	user02	□

User : admin

Cameras Access

□ Cam 1
□ Cam 2
□ Cam 3
□ Cam 4

Figure 4: Admin adds the user in the system.



My Alerts List (Double click on specific alert to see its results)

	AlertId	AlertTitle	AlertDate	FromSysId
▶	1	new alert	11/12/2013	1
	4	TestAlert	1/9/2014	1
	5	TestAlert	1/9/2014	1
	6	jhlkhj	1/9/2014	1

My Queries List (Double click on specific alert to see its results)

	QueryId	QueryText	QueryFromSys	IsDone
▶	1	WHERE VideoD...	1	□

Figure 5: Alert list and corresponding reply.

6. Experiments

Few experiments are conducted on the developed prototype to investigate how cloud-based multimedia surveillance system performs. It is described in the following.

6.1. Workload Measure. To understand the characteristics of the surveillance system's workloads, we analyze the runtime statistics collected while running the applications on AMAZON cloud EC2. We rent a M1 small VM having 1 Intel Xeon E5430 @2.66 GHz CPU unit, 1 CPU core, 1.7 GiB memory, 1 Gbps bandwidth, and 30 G hard drive with Microsoft Server 2008 Base 64-bit. We use the performance monitor of Windows to record the resource utilization of CPU, memory, storage, and network bandwidth. We download videos from PETS and used open-source Open CV library for face detection. The video storage service is tested with windows file system.

The following are the observed results of our workload test in cloud environment. Figure 6 illustrates the resource utilization rates of the aforementioned workloads over the course of their execution. We only plot partial utilization traces that represent the key execution phases. The y-axis represents total resource utilization. The CPU utilization, memory utilization, disk space utilization, and network bandwidth in percentage form can be found in the figure. As we can see, a significant variation exists in the resource utilization across the workloads. Face detection tends to be a highly CPU intensive workload while video storage requires only large storage space during the execution time (Figure 7); the utilization of other resources is below 40%.

6.2. Trade-Off between Cost and Task Waiting Time. Using Figures 8 and 9, we present the trade-off between long term cost and allocation waiting time that has been observed by using a Min-Min [43] based heuristic allocation algorithm with delay tolerance. At each time slot, the allocation method repeats the following operations until the remaining allocation options do satisfy a given constraint: it selects and

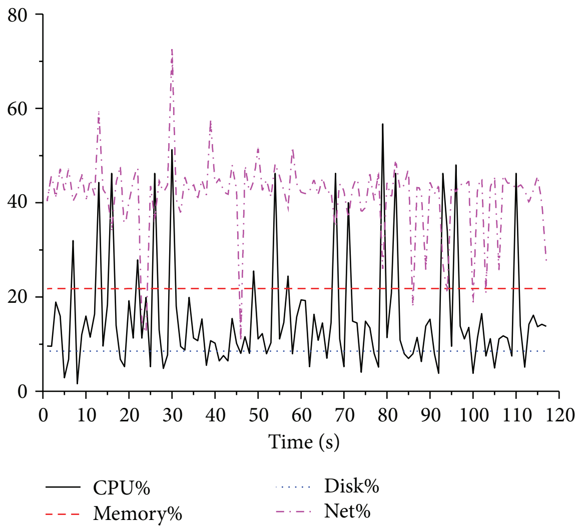


Figure 6: Workload for face detection task.

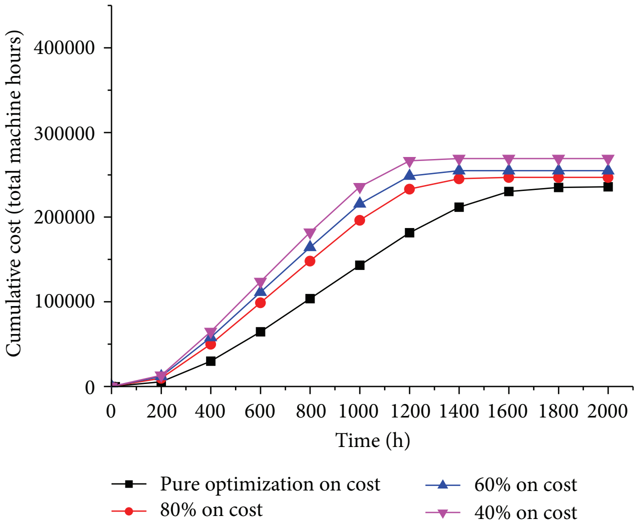


Figure 8: Total cost in different trade-off settings.

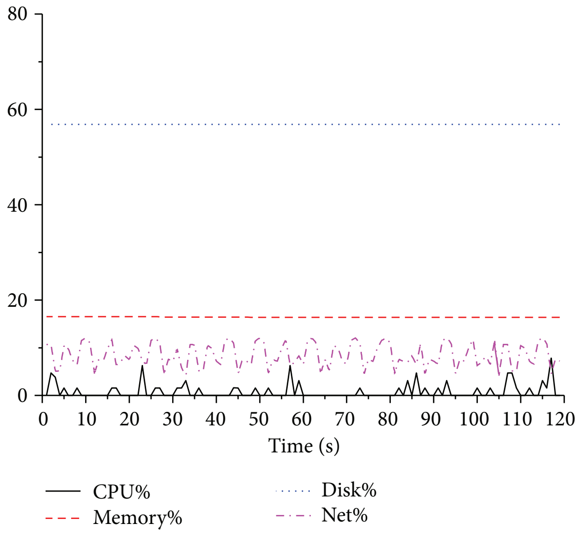


Figure 7: Workload for the storage task.

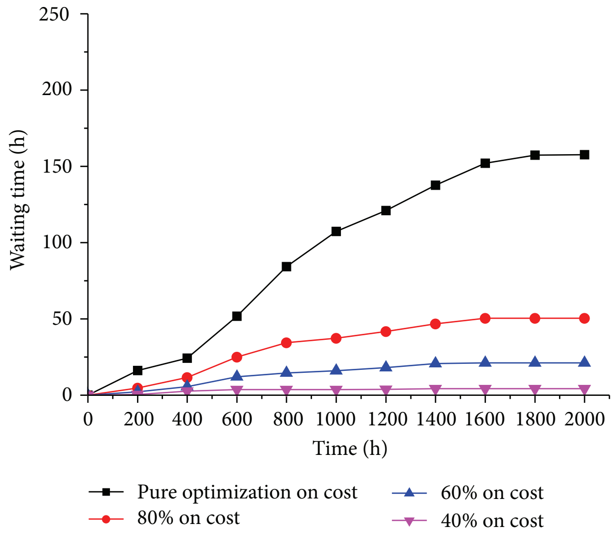


Figure 9: Average task waiting time in different trade-off settings.

enforces the global optimal allocation which produces the best metric value among all possible choices. A threshold value is adopted as the aforementioned constrain to control the trade-off between cost and waiting time. The simulations were conducted under dynamic workload setting where the arrival rate and service time are randomly generated. On the one hand, Figure 8 indicates that the total cost increases as we decrease the weight on cost optimization. On the other hand, the waiting time in Figure 9 is reduced when the total cost rises. The differences among several optimization settings are obvious and remarkable. When the optimization on cost is 80%, the waiting time is more than 50 hours in our simulation. However, this value is reduced to less than 5 hours if we set the optimization on cost as 40%.

Furthermore, we also conducted experiment on media acquisition time with different camera settings on frame rate, and network conditions. The frame loss was 5–7% under 30 frames/sec setting, which is not significant; given in actual scenario a little lower frame rate setting is also acceptable.

7. Discussions

Through some basic evaluation, we were able to monitor some important parameters in the cloud-based multimedia system, which showed motivating results. However, thorough investigation is needed to measure all the different aspects of the system. At some stage it will come to the point where the overall cost and privacy and security issues will be the decisive factor. For new installations, the apparent cost of cloud-based surveillance system is low, due to the fact that no investment on infrastructure is needed. However, this situation may change when the system will run 24/7 on the cloud, which will incur cost of usage of the cloud resources by time. For the existing surveillance infrastructure, the cloud solution might not seem cost-effective as the investment on local infrastructure has already been made [4]. However, in many cases the benefits that a cloud-based surveillance system offers may outweigh the cost and other concerns.

As for the security and privacy, many organizations are still not comfortable to put surveillance content over the cloud due to the potential of privacy leakage and security vulnerabilities. This is especially true for some government organizations, such as military. More research is needed to minimize the risk of privacy loss and design strong security mechanism for the cloud-based surveillance environment before these organizations change their mind. The private or hybrid cloud solutions may be a way to go for these organizations, where they can adopt a blend of private and public cloud infrastructure. This will allow them to schedule what remains in private and what goes to public infrastructure. More research is needed in this direction.

8. Conclusion

This paper describes the different design issues relevant to a cloud-based multimedia surveillance system. The significant issues are related to cloud deployment architecture, media acquisition strategy, cloud storage, media processing, resource allocation, notification and sharing, big data analytics, security and privacy, and cloud-based system performance. Based on these design issues, a cloud-based multimedia surveillance framework has been proposed and a prototype system has been developed. We report some results related to dynamic workload, cost trade-off, and average task waiting time. The result shows the suitability of the cloud-based multimedia surveillance framework. However, the cost, security, and privacy will remain a decisive factor to embrace the deployment of cloud-based surveillance solution. Therefore, the future work may be directed to these issues, along with some other important factors including resource allocation, media processing, and big data analytics on the cloud for multimedia surveillance application.

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The author extends his appreciation to the Deanship of Scientific Research at King Saud University for funding this work through the research group Project no. RGP-VPP-049.

References

[1] R. Cucchiara, “Multimedia surveillance systems,” in *Proceedings of the 3rd ACM international workshop on Video surveillance & sensor networks*, pp. 3–10, 2005.

[2] T. D. Räty, “Survey on contemporary remote surveillance systems for public safety,” *IEEE Transactions on Systems, Man and Cybernetics C: Applications and Reviews*, vol. 40, no. 5, pp. 493–515, 2010.

[3] I. S. Kim, H. S. Choi, K. M. Yi, J. Y. Choi, and S. G. Kong, “Intelligent visual surveillance—a survey,” *International Journal of Control, Automation and Systems*, vol. 8, no. 5, pp. 926–939, 2010.

[4] D. Neal and S. Rahman, “Video surveillance in the cloud?” *The International Journal of Cryptography and Information Security*, vol. 2, no. 3, 2012.

[5] Z. F. Zhao, X. J. Cui, and H. Q. Zhang, “Cloud storage technology in video surveillance,” *Advanced Materials Research*, vol. 532, pp. 1334–1338, 2012.

[6] D. A. Rodríguez-Silva, L. Adkinson-Orellana, F. J. González-Castano, I. Armino-Franco, and D. González-Martinez, “Video surveillance based on cloud storage,” in *Proceedings of the IEEE 5th International Conference on in Cloud Computing (CLOUD ’12)*, pp. 991–992, 2012.

[7] R. I. Chang, T. C. Wang, C. H. Wang, J. C. Liu, and J. M. Ho, “Effective distributed service architecture for ubiquitous video surveillance,” *Information Systems Frontiers*, vol. 14, no. 3, pp. 499–515, 2012.

[8] A. Karimaa, “Video surveillance in the cloud: Dependability analysis,” in *Proceedings of the the 4th International Conference on Dependability (DEPEND ’11)*, pp. 92–95, 2011.

[9] M. S. Hossain, M. M. Hassan, M. Al Qurishi, and A. Alghamdi, “Resource allocation for service composition in cloud-based video surveillance platform,” in *Proceedings of the IEEE International Conference on Multimedia and Expo Workshops (ICMEW ’12)*, pp. 408–412, 2012.

[10] C. F. Lin, S. M. Yuan, M. C. Leu, and C. T. Tsai, “A framework for scalable cloud video recorder system in surveillance environment,” in *Proceedings of the 9th International Conference on Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC ’12)*, pp. 655–660, 2012.

[11] M. Anwar Hossain, “Analyzing the suitability of cloudbased multimedia surveillance systems,” in *Proceedings of the 15th IEEE International Conference on High Performance Computing and Communications (HPCC ’13)*, 2013.

[12] S. Pearson, “Taking account of privacy when designing cloud computing services,” in *Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing (CLOUD ’09)*, pp. 44–52, May 2009.

[13] F. Sabahi, “Cloud computing security threats and responses,” in *Proceedings of the IEEE 3rd International Conference on Communication Software and Networks (ICCSN ’11)*, pp. 245–249, May 2011.

[14] W. Venters and E. A. Whitley, “A critical review of cloud computing: researching desires and realities,” *Journal of Information Technology*, vol. 27, no. 3, pp. 179–197, 2012.

[15] R. Cucchiara, A. Prati, and R. Vezzani, “Designing video surveillance systems as services,” in *Proceedings of the 2nd Workshop on Video Surveillance Projects in Italy (VISIT ’11)*, May 2011.

[16] P. Mell and T. Grance, “The NIST definition of cloud computing,” *National Institute of Standards and Technology*, vol. 53, no. 6, p. 50, 2009.

[17] Y. Xu, S. Helal, M. T. Thai, and M. Schmalz, “Optimizing push/pull envelopes for energy-efficient cloud-sensor systems,” in *Proceedings of the 14th ACM International Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWiM ’11)*, pp. 17–26, usa, November 2011.

[18] Y. Tsividis, "Event-driven data acquisition and digital signal processing-A tutorial," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 57, no. 8, pp. 577–581, 2010.

[19] R. Shen, "Building a cloud-enabled file storage infrastructure," TechRepublic White Paper, F5 Network, 2013, http://www.techrepublic.com/whitepapers/buildinga-cloud-enabled-file-storage-infrastructure/2941141.

[20] W. Zhu, C. Luo, J. Wang, and S. Li, "Multimedia cloud computing," *IEEE Signal Processing Magazine*, vol. 28, no. 3, pp. 59–69, 2011.

[21] H. Abu-Libdeh, L. Princehouse, and H. Weatherspoon, "Racs: a case for cloud storage diversity," in *Proceedings of the 1st ACM Symposium on Cloud Computing*, pp. 229–239, June 2010.

[22] Y. Zhao, K. Ou, W. Zeng, and W. Song, "Research on cloud storage architecture and key technologies," in *Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human*, pp. 1044–1048, November 2009.

[23] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362–375, 2013.

[24] A. Greenberg, J. Hamilton, D. A. Maltz, and P. Patel, "The cost of a cloud: research problems in data center networks," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 68–73, 2008.

[25] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: a survey," *Future Generation Computer Systems*, vol. 29, no. 1, pp. 84–106, 2013.

[26] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. Foster, "Virtual infrastructure management in private and hybrid clouds," *IEEE Internet Computing*, vol. 13, no. 5, pp. 14–22, 2009.

[27] A. Beloglazov and R. Buyya, "Energy efficient resource management in virtualized cloud data centers," in *Proceedings of the 10th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing*, pp. 826–831, May 2010.

[28] M. Asad Arfeen, K. Pawlikowski, and A. Willig, "A framework for resource allocation strategies in cloud computing environment," in *Proceedings of the 35th Annual IEEE International Computer Software and Applications Conference Workshops (COMPSACW '11)*, pp. 261–266, deu, July 2011.

[29] G. Wei, A. V. Vasilakos, Y. Zheng, and N. Xiong, "A game-theoretic method of fair resource allocation for cloud computing services," *Journal of Supercomputing*, vol. 54, no. 2, pp. 252–269, 2010.

[30] H. Goudarzi and M. Pedram, "Maximizing profit in cloud computing system via resource allocation," in *Proceedings of the 31st International Conference on Distributed Computing Systems Workshops (ICDCSW '11)*, pp. 1–6, June 2011.

[31] J. Gu, J. Hu, T. Zhao, and G. Sun, "A new resource scheduling strategy based on genetic algorithm in cloud computing environment," *Journal of Computers*, vol. 7, no. 1, p. 42, 2012.

[32] P. T. Eugster, P. A. Felber, R. Guerraoui, and A.-M. Kermarrec, "The many faces of publish/subscribe," *ACM Computing Surveys*, vol. 35, no. 2, pp. 114–131, 2003.

[33] J. Hoffert, D. C. Schmidt, and A. Gokhale, "Adapting distributed real-time and embedded pub/sub middleware for cloud computing environments," in *Middleware 2010*, vol. 6452 of *Lecture Notes in Computer Science*, pp. 21–41, Springer, Berlin, Germany, 2010.

[34] J. Han, N. Choi, T. Chung, Ted Taekyoung Kwon, and Yanghee Choi, "A targetcentric surveillance system based on localization and social networking," *Multimedia Tools and Applications*, pp. 1–25, 2012.

[35] D. Trottier, "Crowdsourcing CCTV surveillance on the internet," *Information, Communication & Society*, vol. 17, no. 5, pp. 609–626, 2013.

[36] T. Huang, "Surveillance video: the biggest big data," *Computing Now*, vol. 7, no. 2, 2014, http://www.computer.org/portal/web/computingnow/archive/february2014.

[37] R. L. Villars, C. W. Olofson, and M. Eastwood, "Big data: what it is and why you should care," White Paper, IDC, 2011.

[38] P. You and Z. Huang, "Towards an extensible and secure cloud architecture model for sensor information system," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 823418, 12 pages, 2013.

[39] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography and Data Security*, vol. 6054 of *Lecture Notes in Computer Science*, pp. 136–149, Springer, Berlin, Germany, 2010.

[40] H. Takabi, J. B. D. Joshi, and G. J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security and Privacy*, vol. 8, no. 6, pp. 24–31, 2010.

[41] M. A. Hossain, P. K. Atrey, and A. El Saddik, "Modeling and assessing quality of information in multisensor multimedia monitoring systems," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 7, no. 1, article 3, 2011.

[42] M. Leszczuk, P. Romaniak, and L. Janowski, "Quality assessment in video surveillance," *InTech*, chapter 4, 2012.

[43] R. F. Freund, M. Gherrity, S. Ambrosius et al., "Scheduling resources in multi-user, heterogeneous, computing environments with smartnet," in *Proceedings of the 7th Heterogeneous Computing Workshop (HCW '98)*, pp. 184–199, 1998.

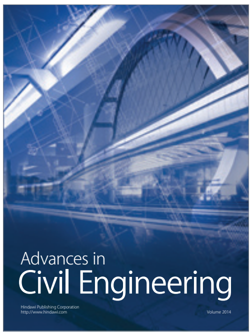
Journal of
Engineering

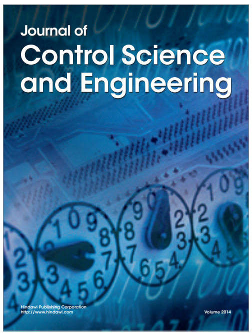
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

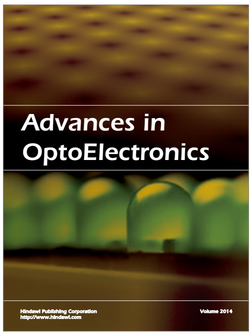
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

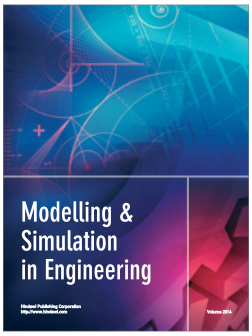
Journal of
Robotics

Journal of
Electrical and Computer Engineering

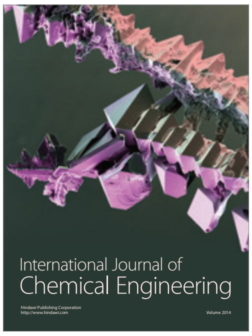

Advances in
OptoElectronics

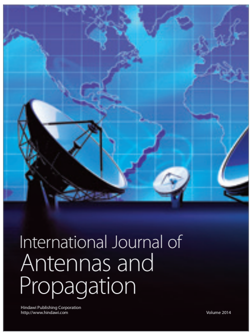
VLSI Design

International Journal of
Navigation and Observation

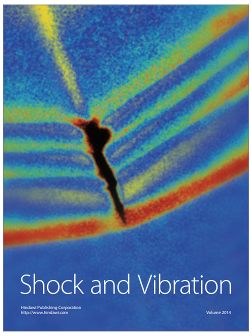

Modelling & Simulation in Engineering

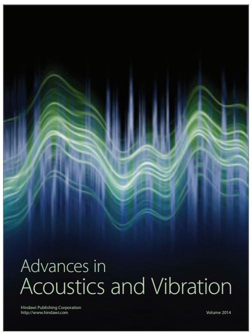
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration