Journal of Information Sciences and Computing Technologies(JISCT)
ISSN: 2394-9066

SCITECH
RESEARCH ORGANISATION|

Volume 3, Issue 2
April 21, 2015|

Journal of Information Sciences and Computing Technologies
www.scitecresearch.com

Video Forensics in Cloud Computing: The Challenges & Recommendations

Manal Al-Rawahi[1], E.A.Edirisinghe[2]
[1]Computer Science Department, Loughborough University, Loughborough, LE11 3TU, UK.
[2]Computer Science Department, Loughborough University, Loughborough, LE11 3TU, UK.

Abstract

Forensic analysis of large video surveillance datasets requires computationally demanding processing and significant storage space. The current standalone and often dedicated computing infrastructure used for the purpose is rather limited due to practical limits of hardware scalability and the associated cost. Recently Cloud Computing has emerged as a viable solution to computing resource limitations, taking full advantage of virtualisation capabilities and distributed computing technologies. Consequently the opportunities provided by cloud computing service to support the requirements of forensic video surveillance systems have been recently studied in literature. However such studies have been limited to very simple video analytic tasks carried out within a cloud based architecture. The requirements of a larger scale video forensic system are significantly more and demand an in-depth study. Especially there is a need to balance the benefits of cloud computing with the potential risks of security and privacy breaches of the video data. Understanding different legal issues involved in deploying video surveillance in cloud computing will help making the proposed security architecture affective against potential threats and hence lawful. In this work we conduct a literature review to understand the current regulations and guidelines behind establishing a trustworthy, cloud based video surveillance system. In particular we discuss the requirements of a legally acceptable video forensic system, study the current security and privacy challenges of cloud based computing systems and make recommendations for the design of a cloud based video forensic system.

Keywords: cloud computing; security; privacy; video surveillance; forensic analysis; Data Protection Act 1998; IaaS; hadoop; law.

1. Introduction

Present video surveillance systems that typically consist of a large number of distributed and networked CCTV cameras, collect significant quantities of digital evidence that can be used for crime forensics. The evolution of such systems have at present resulted in a significant proportion of the labour intensive video analytic and forensic tasks, usually carried out by trained CCTV operators, to be alternatively carried out by intelligent, automated, computer based analysis systems. Such systems use image processing, computer vision, pattern recognition and machine learning algorithms to detect and recognize objects of interest (e.g., people, vehicles etc.) and identify events of significance (e.g., person running, car speeding, people fighting etc.) enabling real-time alerts/warnings (i.e. video analytics) to be generated or objects/events to be indexed and stored in a database to allow off-line search to be carried out (e.g. search for a man wearing a red shirt who entered a specific named building between 1pm to 3pm on given week) for video forensic investigations (i.e. post incident analysis). However conducting efficient video forensics analysis on large datasets captured by distributed camera systems require high performance computing capabilities due to the complexities of computing algorithms to be utilized and the significant storage capacity required due to the sheer volume of data usually gathered/recorded. These two requirements increase the burden on the IT infrastructure to be used and introduce important challenges that need to be met to ensure practical viability. In response to meeting the above challenges at present there are initiatives to move video analytics/forensics, typically carried out using dedicated storage and computing infrastructure to the cloud to best utilize its potential benefits in providing on-demand resource pooling (both compute power and storage). Although cloud computing and related infrastructure can support the above mentioned critical requirements of modern intelligent, automated video surveillance systems it also introduces other technical and non-technical challenges. Security and privacy risks are the most cited challenges in the area of cloud computing[1] due to the customer's/user's lack of physical control and the multi-tenancy nature of the cloud. Yet this is of fundamental importance in video evidence analytics and forensics, given the potential legal use of the evidence stored and/or created. Since video evidence gathering and use is regulated by law, it is crucial to review the legal implications of deploying video surveillance in the cloud and determine the practicalities and challenges that need to be met to abide by the law. According to authors knowledge there has not been any previous attempt in studying the legal requirements of a video forensic system and investigating the viability of developing a cloud based system for video forensics, given the known security and privacy threats of cloud computing. This paper attempts to bridge this research gap and makes relevant recommendations for the design of a large-scale, cloud-based video forensic system. Figure 1, illustrates the key focus area of the research context of this paper which will be visited in the forthcoming sections of the paper.

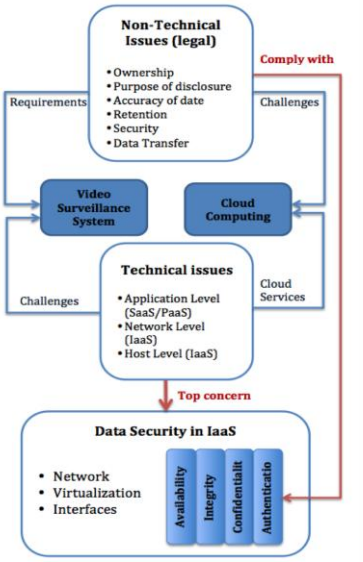

Fig 1: key focus areas of the research

For clarity of presentation the rest of this paper is organized as follows: Apart from this section which introduces the reader to the research context on this paper, section-2 introduces the reader to the existing work in conducting video surveillance within a cloud based system. Section-3 presents the architecture of a Forensic Video System previously developed by authors and implemented within a dedicated, stand-alone computing architecture which is used in this paper to make recommendations for upscaling towards a cloud based implementation. Section-4 presents the security and privacy requirements of a video surveillance system, given the laws and legislations governing the use of video as evidence in a legal prosecution. Section-5 provides a detailed review of security and privacy related issues in cloud computing and uses the knowledge gathered in section-4 provides recommendations for the design of a cloud based video forensic system based on that presented in section-3. Finally section-6 concludes with recommendations for further research and development.

2. Video surveillance in the cloud- A Survey

There are some recent initiatives that are underway that gathers video surveillance data from a system of distributed IP cameras and carry out some basic video analytic tasks such as, motion detection, object identication, etc., in the cloud, overcoming storage capacity and processing power limitations of traditional video analytic applications. One example is the releases of the commercial cloud-based video surveillance systems, "video surveillance as a service (VSaaS)", which is expected to grow by 17%annually[2]. VSaaS is software-as-a service (SaaS) powered by Microsoft Windows Azure cloud platform. It provides High dimension (HD) video quality, real-time alerts performing motion detection, through heterogeneous connected devices. However, VSaaS is used for alert based video analytic tasks and do not support an extensive range of algorithms that can work together to support large-scale post incidence (i.e. video forensic tasks) video surveillance. Hence the basic dataset stored is nothing beyond the original video data captured and the usage of the service is so far not to support evidence in courts, but just as an alert system that can be used for monitoring security of a locality. A further drawback of VSaaS is that the infrastructure is beyond the user's control, which raises security and privacy concerns. In addition the compatibility issue of integrating cameras to VSaaS software adds extra hardware costs [3].

Some recent efforts from academic research addressed the challenges in the context of a cloud-based video surveillance system. The following sections introduce some of these research findings:

Neal et al [3] investigated the capability of cloud services to support the requirements of hosting a high-resolution video surveillance management system and studied the cost in various cloud service models based on market pricing model. The author proposed cloud computing as a solution for VSM and highlighted issues to be considered such as the cost, legal requirements and compliance. These issues are considered and discussed in detail in this paper. Anwar Hussain has a number of contributions to video surveillance in the cloud. In 2012[4], he proposed a dynamic resource allocation scheme using a liner programming approach for composite video surveillance streams with cloud-based video surveillance system. A prototype of a system was implemented in Amazon AWS. In 2013[5], he analyzed the suitability of cloud solution by comparing video surveillance local infrastructure with his proposed cloud-based system in terms of performance, storage, scalability, reliability and collaborative sharing of media streams. The results demonstrated the capability of cloud computing to tackle the mentioned issues. In 2014 [6], a prototype design considering issues from his previous work was implemented and tested on Amazon EC2 platform. The author raised concerns in relation to the security and privacy factors and thus suggested a hybrid-cloud solution as an alternative. Yong-Hua et al[7] proposed a prototype design for cloud-based video surveillance implemented in a private campus network. The design was focused on exploring the interaction between system components: surveillance system, browse system and storage system. Rodriguez and Gonzalez[8] proposed a cloud-based video surveillance system and focused on scalability and reliability issues in comparison to a traditional surveillance system. The proposed system was operated by optimizing the transmission of video streams between the client and cloud server, depending on network conditions, to avoid data loss in case of cloud failure or excessive network traffic. In this work video data was received and processed in the cloud, attending to security and privacy consideration. This was done by using security mechanisms such as, data encryption and secure transmission. The authors of [6,7,8] utilized a cloud computing model to perform some basic image processing and computer vision algorithms. This work was limited with the design of fundamental video analytic tasks and no technical details were discussed.

Recently Hadoop framework [9] for processing video in cloud environment has become an active area of research with the key focus being parallelizing video analysis algorithm and thus reducing execution time. This approach utilizes Hadoop Distributed File System (HDFS)[10], MapReduce framework [11] and other open source tools to build and implement computer vision algorithms. Existing work has focused on solving the challenges faced by operating Hadoop with unstructured data (image, video) where video processing libraries need to be modified to work within a computing cluster as well as the associated changes required to video analytic algorithms. Heikkinen at al [12]evaluated the feasibility of using Hadoop for video analysis tasks. The authors demonstrated that splitting video into smaller files before inserting into hdfs gives better performance than extracting frames first. Ryu et al [13]also implemented a similar system using a basic computer vision algorithm for face detection and tracking. The authors modified the well-known ffmpeg [14] video coding library to access data in hdfs, which gives better performance than the common mounting approach called fused-hdfs. Chia-Feng and Shyan-Ming [15] proposed a framework for a scalable video recording system in the cloud to optimize video streams from hundreds of heterogeneous connected devices. This approach was implemented under IaaS service model with an integrated Hadoop based distributed file system, to store video data. H.Tan & L.Chen [16] have provided technical implementation details to handle large-scale video data within a Hadoop based cluster. All of the above work have focused on parallelizing video analytic algorithms using Hadoop, within a cloud like environment, but has not considered the virtualization environment and the legal or privacy issues. In section-6 we comment that for our future work in the implementation of the cloud based video forensic system, a Hadoop based system may be used.

As discussed above although some work has been presented in literature on cloud based video surveillance, this work has been limited to implementing simple video analytics tasks within cloud based architecture. The key focuses of such attempts have been to optimally use the available infrastructure and ensure security of video evidence gathered. The surveillance systems are not of a scale that requires the storage of metadata about the stored videos thus requiring the safeguard of such annotated data. Further the computing resource requirements were not sufficiently extensive to warrant considering the best use of a cloud based architecture. Further such work also did not discuss the legal requirements of a surveillance data gathering and investigatory system. Nevertheless such requirements warrant special features of both architectural and security requirements of a cloud based implementation. The key focus of the research presented in this paper is to bridge this research gap in making viable recommendations for a cloud based architecture for video forensics.

3. Video Forensic System

Figure 2, illustrates the high-level block diagram of a video forensic system that was developed by the authors as a part of a research and development project, CrimeVis [17]. This video forensic analysis tool is an example of a state-of-the-art, computer based, post-event forensic analysis and visualization system for CCTV video footage. It was designed and built as a stand-alone system that was implemented and operated on a dedicated hardware setup. A summary of its operational features can be described as follows: A typical video surveillance system consists of a distributed set of video cameras covering an area/space that requires monitoring 24/7 for security purposes. We assume that these cameras are connected to the Video Database (see figure-2) and store the input video with some high-level annotations information such as, camera number/location, time of day etc. The video annotations engine is a collection of image processing, computer vision, pattern recognition, machine learning and optimization algorithms that work collectively to identify the presence of known objects (e.g. humans and vehicles) and are able to articulate their detail/appearance (e.g. shirt colour, vehicle type, number plate details, carrying a bag etc.) The annotation engine is the key component of the forensic tool and is the location where most extensive computational tasks are carried out. The annotated data is stored in an annotation database, real-time. The accuracy and trust of the data stored in the annotation database are key to conducting a forensic investigation that has any legal validity. The annotation information (i.e. metadata) will be used in the search process for the detection and recognition of people (e.g. man wearing a red jumper, carrying a bag), vehicles (e.g. a red van, speeding) and activities (e.g. man walking away from a blue car). Any breach of security that could lead to potential intentional alteration of the metadata will result in objects not being found during a forensic search of the database. This is a serious security threat that will completely invalidate the use of forensic search evidence legally. The search is initiated by a human operator (user) through an interface and using a Search Tool (see figure-1). The search tool searches through the Annotation Database created by the Annotation Engine detailed above. Once the objects/events with given descriptions are located, going through the Metadata, this will be used to fetch the data from the stored, original video footage. The second security threat exists here. If the Video Storage Database can be tempered, the stored video content can be removed or altered making the process void, legally. Apart from providing a level of security for the Annotated Data/Metadata and the original video content, the communication between the human investigator and the stored data should be secured. Hence a level of security is needed within the communication channels/mediums. It is also noted that the Annotation Engine is made out of a large number of algorithms that are based on foundations of image processing, computer vision, pattern recognition and machine intelligence. Their algorithms are computationally extensive and will not typically operate real-time within the limited resources of infrastructure that can be offered by a dedicated, standalone hardware system/implementation. Hence a cloud-based architecture will help alleviate this problem. However the proposed use of cloud computing as a solution raises concerns to the confidentiality and integrity of video footage when video streams are processed and stored off-site in cloud infrastructure that is operated by a third party. In some cases cloud providers involve other third parties such as cloud brokers and cloud auditors, which makes security more complex[18]. Therefore for video surveillance systems to take advantage of cloud computing benefits, the potential security threats should be analyzed and solutions be found to protect video data in the cloud while data is in-transit and data is at-rest (stored). Further the integrity of the video processing algorithms should also be protected against threats of unlawful alterations. Before discussing the security and privacy related issues relevant to cloud computing, the next section presents the security and privacy requirements of a video surveillance system. This understanding is important before one study the associated risks when using cloud computing.

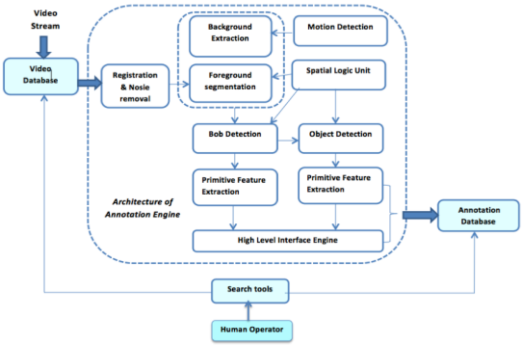

Fig 2: High-level block diagram of a video forensic system

4. Security and Privacy Requirements of a Video Surveillance System

Intelligent CCTV surveillance systems used in public areas are installed by international, national and local governments to help prevent/detect crimes. Therefore they should be operated in such a way to preserve confidentiality, integrity and personal privacy, by following appropriate laws and adopted codes of practice [19]. From country to country the legal requirements can differ in the details but the essence of the requirements would be the same. In this paper we focus our investigation on UK based legal and regulatory frameworks. It is noted that in the design, implementation and operation of a computer based, automated, CCTV video forensic system the legal and regulatory aspects would be taken into account. If not the practical use of such a system as a forensic evidence gathering and investigatory tool will be questionable. In this section we review and analyze the security and privacy requirements of video surveillance based on the following:

1. Legal frameworks: it should be clear how data protection act (DPA) applies to video data processed in cloud infrastructure[20]and also how it is accepted as evidence in court[21], and
2. Research publications: addresses current problems, solutions, and future trends for research.

4.2. Review of the current legal framework that governs video surveillance systems installed in the UK

In the UK, the operation of CCTV is regulated by Data Protection Act of 1998 and Human Rights Act of 1998. In 2008, the UK Information Commissioner's Office (ICO) issued guidance for the use of CCTV in the “CCTV code of practice”, which was subsequently updated in 2014 titled, “In the picture: A data protection code of practice for surveillance cameras and personal information” to cover the inevitable widespread use of CCTV systems and thus the essential need to focus on data protection. The document provides practical guidance to those involved in operating surveillance camera systems and provide recommendations on how the legal requirements of Data Protection Act (DPA) can be met when monitoring individuals and disclosing images for the investigation of crimes. The guidelines highlight important criteria that should be considered in line with the requirements of designing a video surveillance architecture. The criteria can be summarized as follows:

- Ensuring effective administration - An individual/organization (i.e. the Data Controller) should be taking the ownership of the data gathered. The Data Controller is legally responsible for maintaining compliance with the DPA([22]page 10).
- Storing and viewing surveillance system information - Recorded material should be stored in a way that maintains the confidentiality and integrity of an image. This can be accomplished by encryption. Some cases when Cloud computing is used the controller has to ensure that provider can ensure the security of the information following guidance from ICO [22], page 12).
- Disclosure - Video records must be secured and only accessed when there is a court order or information access right (freedom of information act 2012). This is to prevent the potential misuse of the system by operators who could spy on people, collect unauthorized copies, and manipulate data and marketing purpose which violate privacy and confidentiality of individuals. Disclosure of any image should be consistent with their purpose([22]page 14).
- Retention - The DPA does not prescribe specific minimum or maximum retention periods, which apply to all systems or footage. Rather retention should reflect the organization's own purposes for recording images ([22], page 19). Retention depends on the period of the investigation needs. After the retention period the data should be permanently deleted. However, recently UK government has introduced specific laws for dealing with data retention to protect public from criminals and terrorists [23].

A further guidance was published for the use of CCTV camera and Automatic Number Plate Recognition (ANPR) systems in the form of “Surveillance Camera Code of Practice” by Home Office and Lord Taylor of Holbeach CBE [24]. The guidelines include twelve principles that describe best practices to be followed in using surveillance camera systems and processing images and footage in public places. This code of practice came into effect in England and Wales in 2013[25]. The guiding principles can be categorized into two groups as follows:

1. The development or use of surveillance camera systems", addressed in principles 1-4 (chapter 3-page 12) - These principles are related to the purpose of using the surveillance camera system, consideration of privacy and location of individual cameras, transparency/signage of cameras and clear responsibilities and accountability of surveillance systems.
2. The use or processing of images or other information obtained by virtue of such systems", addressed in principles 5-12 (chapter 4-page 16).

The principles under category (2) are related to the way that the video feed is handled. These principles overlap with the requirements listed by the ICO's principles [22] listed above, including, video integrity and authorization access, retention and purpose of data disclosure. These principles are as follows:

- **Principle 5:** Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

- **Principle 6:** No more images and information should be stored than that is strictly required for the stated purpose of a surveillance camera system. Such images and information should be deleted once their purposes have been discharged.
- **Principle 7**: Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
- **Principle 8:** Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work, in order to meet and maintain those standards.
- **Principle 9:** Surveillance camera system images and information should be subjected to appropriate security measures to safeguard against unauthorized access and use.
- **Principle 10:** There should be effective review and audit mechanisms to ensure that legal requirements, policies and standards are complied with in practice, and regular reports published".
- **Principle 11:** When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
- **Principle 12:** Any information that is used to support a surveillance camera system, which compares against a reference database for matching purposes should be accurate and kept up to date".

A closer study of the above principles reveal that the annotation of stored video database (Principle 6) should be carried out only when there is a need for a forensic investigation (Principle 11). Therefore the data within the annotation database will only be created when it is necessary or for law enforcement purposes (Principle 7) and should be accurate and complete (Principle 12) at any given time.

4.3. Review of the legal framework governing video to be used as evidence

Video footage evidence, is defined as: "the presentation of visual facts about the crime or an individual that the prosecution presents to the court in support of their case"[26]. Once video evidence is collected from any type of storage media it must comply with legal requirements to ensure its admissibility in court procedures. In order for any digital evidence to be admissible in court, Nagel [27] listed a number of evidentiality rules required for any digital evidence to be relevant, authentic, original or an acceptable duplicate and hearsay. Other evidentiality rules found in literature [28] such as those that relate to preservation, completeness and reliability is considered by Nagel as simply methods of authenticating digital evidence. The work presented in [29] explained how the court addresses legal issues when video is presented as evidence and emphasizes that video should be authenticated by testifying what is on the video is an exact representation of what should be on the video footage. If no witness is able to authenticate the surveillance video, then under the silent witness theory a judge can determine if the video can be authenticated if the following requirements are met [29]:

- There is evidence establishing the time and date of the video, which can be found in the metadata files of the captured videos.
- There was no tampering with the video.
- The video equipment used was sound.
- There is testimony identifying the participants depicted in the video.

This links to a reported court case in [27] which considered the use of hashing, metadata, and collection of data in its native format, as ways to authenticating evidence[21]. Even if evidence cleared the authentication process, additional evidential rules such as originality, preservation and hearsay will also apply[27]. An example of this is when a judge requests for a still-frame photo extracted from the video surveillance footage and compares it with the original video captured from the camera to ensure its originally and to avoid the possible misleading of the jury [30]. This confirms the importance of securing video surveillance data in-transit and at-rest, to preserve its integrity.

The process of investigating a crime via camera surveillance involves extracting the original video sequence and its associated meta-data files from recorded systems[31]. A given video files reliability to be used as evidence can be met by technical authenticity methods such as using an audit trail, encryption or watermarking [32]. Modern video surveillance systems such as that presented in section II, integrates various image processing, pattern recognition, machine vision and computer vision techniques for forensics video analysis. The operation of these algorithms affects the integrity of the resulting images but not their authenticity[26]. However, the use of processed images is not a problem in the law of England, Wales and Scotland as long as user (investigator) is able to perform an audit trail to give evidence of the procedures used for generating, processing and storing digital images that proves the image is an accurate copy of the original[32].

4.4. Research Publication

In addition to the information presented above based on various laws and codes of practice, a number of research papers have been published in literature that relates to the use of video footage as evidence. Qasim and Christian [33] summarised the current state of the security and privacy requirements of modern distributed video surveillance with respect of integrity, confidentiality and access authorization mechanisms and underlined limitations of the existing approaches in large scale video surveillance system. Real-time video encryption, key management, storage of video and its associated metadata, dynamic access controls are some research challenges identified by the authors. Winkler and Rinne[34] conducted a comprehensive survey of security and privacy protection related research work that have been published in the general area of visual sensor networks, which also relates to video surveillance systems. In this paper[34], security requirements to ensure data integrity, authenticity and confidentiality are classified into four areas, (see figure 3):

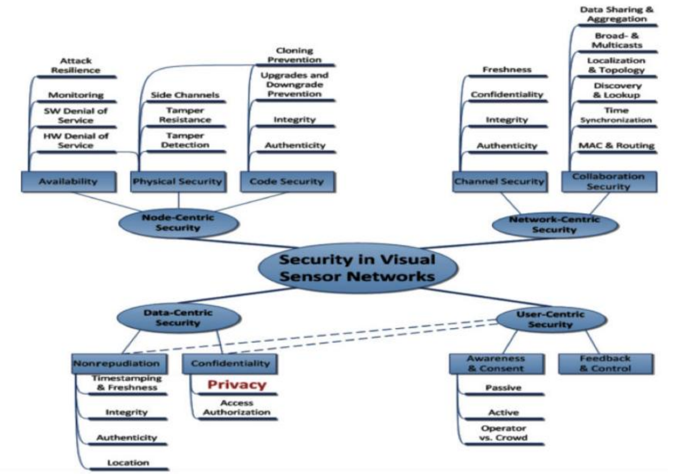

Fig 3: Security requirements in visual sensor networks, [34]

- Data-centric: include security of all data life cycles.
- Node-centric: include security of physical devices.
- Network-centric: include security of data transmission and communication.
- User-centric: related to awareness of how individual's personal data is protected.

As shown in figure 3, confidentiality, authenticity and integrity are needed in all security areas. The solutions adopted to achieve these requirements range from trusted computing, encryption to access control. Authors highlighted the need for the protection of security and privacy within the application layer where more research were traditionally focused but also within the underlying infrastructure, a concern that this paper demonstrates to be genuine.

4.5. The Legal Aspects: Summary & Conclusions

The regulations and guidelines discussed above require appropriate technical and security safeguards to ensure the confidentiality, integrity, availability and authenticity of video, in order to be accepted as evidence in court and also to prevent breaches of an individual's privacy. The following is a summary of typical technical security practices adopted to ensure legal compliance:

- Encrypt data in transit and at rest, to maintain integrity and confidentiality.
- Protect stored data from unauthorized access and tempering by implementing access control mechanisms.
- Implement a data backup plan to prevent data loss.

- Implement a mechanism to remove data from storage media after the retention period.
- Implement audit mechanism to monitor that published polices and legal requirements are met.

There is one principle listed in DPA about international restrictions of data transfer. This principle is not mentioned in any of the above discussed legal frameworks. Data transfer is relevant to how cloud computing handles data for better performance and resource utilization; this will be discussed in (section 1.2.11).

The implementation of the technical security practices mentioned above are based on common Information Technology (IT) practices presented in[33][34], However, there is no legislation that yet has specifically considers the use of cloud computing[35] and virtualization technology for CCTV video evidence gathering, processing and investigation. Therefore we consider security in cloud-based video surveillance as a research gap to be further explored.

5. Cloud Computing

Cloud Computing is a model that delivers Information Technology (IT) as services to users. The services can be classified into software, platform and infrastructure which are delivered on demand following a pay-per-use price model. The Cloud offers scalability and elasticity of resources, which reduces cost on hardware provisioning. This capability of Cloud computing is enabled by a collection of existing technologies including virtualization, internet technologies (web services, SOA, Web 2.0), distributed computing (cluster, grid), utility computing and system management (autonomic computing, data center automation)[36]. Cloud services can be deployed in different ways depending on who owns the infrastructure and the provisioning location, examples being the public, private, community and hybrid clouds. Each of these deployments introduces different risks. The following sections present security concerns and the associated technical and non-technical issues relevant to using cloud computing as a environment for video surveillance.

5.2. Cloud Computing Security Concerns

Migrating a video surveillance system and its associated metadata outside the limits of an organization requires the cloud provider to provide a level of security protection similar to that could be provided if the system is operated within a local data centre [37], in a manner consistent with policies [38]. In fact, hosting data, whether in a local data centre or in a public cloud, makes data exposed to the same risks and breaches. Hence existing security measures can be implemented [39]. Nevertheless, cloud computing inherits risks from the core enabling technologies such as multi-tenancy, web services, utility computing and the internet [40][41]. This combination of cloud technologies makes the existing security controls not applicable, thus requiring further research and appropriate modification [42]. Besides, the concept of security and privacy are different depending on the law of a given country or business requirements. This leads to different requirements and protection mechanisms for data [39]. The centralized nature of resources and data in the cloud presents a more attractive target to attackers [35], where one successful attack can make way to follow up attacks against the whole system. This show how severe is the potential for security breaches in the cloud. A number of real world security incidents have been reported in literature that proves possibilities of cloud attacks [41][43][44]. The main causes of these security incidents are customer's lack of physical control and the multi-tendency shared environment[18][35][44], which are vulnerabilities in cloud computing[45]. Surveys conducted by International Data Corporation (IDC)[1] in 2008 & 2009 shows that security is the top concern and barrier for cloud users, which reflects why the topic of security has been considered the primary research focus in the area of cloud computing [18][35]. The following sections refer to a review of literature that highlights the technical and non-technical issues that relates to the security and privacy of cloud computing.

5.2.1. The Cloud: Technical Issues

In literature several researchers have addressed cloud security and privacy from the perspective of industry, governmental and academia to find research gaps, propose solutions and provide guidelines on best practices. Gartner [46] was one of the first contributors to cloud computing. Their work titled "Assessing the Security Risks of Cloud Computing" published in 2008, warns organizations about the danger of migrating to the cloud, without performing a risk assessment in order to evaluate cloud specific risks, such as privileged user access, compliance, data location, data segregation, availability, recovery, investigative support and viability. Further the European Network and Information Security Agency (ENISA)[35] published a research article titled: “Cloud Computing: Benefits, Risks and Recommendations for Information Security” in November 2009. The document details a cloud computing risk assessment and provide guidelines on technical, organizational, and legal issues of cloud computing. It further introduced cloud vulnerabilities. Cloud Computing Security Alliance (CSA)[47] is another well-known organization that has conducted comprehensive research on cloud security, with a help of expert volunteers. They published their first report in December 2009 titled: “Security Guidance for critical Areas of Focus in Cloud Computing” [18] and updated it in November 2011 as version 3.0. The report provides analysis of cloud risks identified in thirteen domain areas considering the architecture, legal and operational aspects of the cloud, with recommendation on technical security controls. In 2010, CSA released another set of guidelines titled: “Top Threats to Cloud Computing V1.0”, which identifies seven top threats related to cloud computing. In 2013 this work was extended and updated as “The Notorious Nine, Cloud Computing Top Threats in 2013”, the threats ranked in order of severity [48] (see table 1). As comparing to the previous version of the guidelines, some shifts in ranking is noticeable, where data breaches have been moved from the 5th ranked in 2010 to the 1st ranked in 2013. This observation is not surprising due to the volume of data centralized in the cloud at present, which attract more attackers.

Table 1. Top Cloud Computing Threats, by CSA, [48]

Ranking	2010	2013
1	Abuse and Nefarious Use of Cloud Computing	Data Breaches
2	Insecure Interfaces and APIs	Data Loss
3	Malicious Insiders	Account Hijacking
4	Shared Technology Issues	Insecure APIs
5	Data Loss or Leakage	Denial of Service
6	Account or Service	Malicious Insiders
7	Unknown Risk Profile	Abuse of Cloud Services
8		Insufficient Due Diligence
9		Shared Technology Issues

In [18][35][46] a number of organisations identified the security risks in cloud aiming to provide recommendations and guidelines when using cloud computing. However, no technical details have been provided as how to secure the infrastructure or data and how to achieve compliance to data protection law[49].

In publications, the paper [50] conducted a quantitative analysis on cloud security challenges and identified seven cloud-specific issues that have been extensively received more attention in literature in terms of problems and solutions. The author classified them into a security model (considering network security, data security, interface, compliance, governance, legal issues, virtualization). The results showed that compliance, governance and legal issues received more solutions than problem citations, whereas the technical aspects such as virtualization, data leakage and isolation received less citation in terms of solutions. In [37][44][51], and the security and the protection of cloud infrastructure focused on trusted computing, cryptography and access control mechanisms. Similar mechanisms have been stated in video surveillance security[33]. Implementing any of the these mechanisms depends on the identified security metrics to quantify the improvement to system security and to compare security alternatives with similar functionalities [52][33].

Given above, an attack surface metric can be used to identify the access entry points that attackers exploit to target data integrity, confidentiality or availability and hence decide on security measures. Frank [49]presented cloud specific security attacks in a technical infrastructure as a service(IaaS) cloud environment as shown in figure 4. The author considered these risks as attack surfaces in IaaS caused by malicious insiders (i.e a rogue cloud provider or malicious tenant). The author classified attacks as either, traditional IT known risks (T) and specific-cloud risks

(C). Two scenarios of cloud infrastructure were illustrated and discussed, namely: multi-tenancy cloud host and single-tenant cloud host. In multi-tenancy scenario, multiple customers in a form of Virtual machines (VM) reside on the same physical machine and share resources. A single-tenant multiple virtual machine is only dedicated to a single customer, this concept is also called an off-private cloud. Both scenarios present security risks.

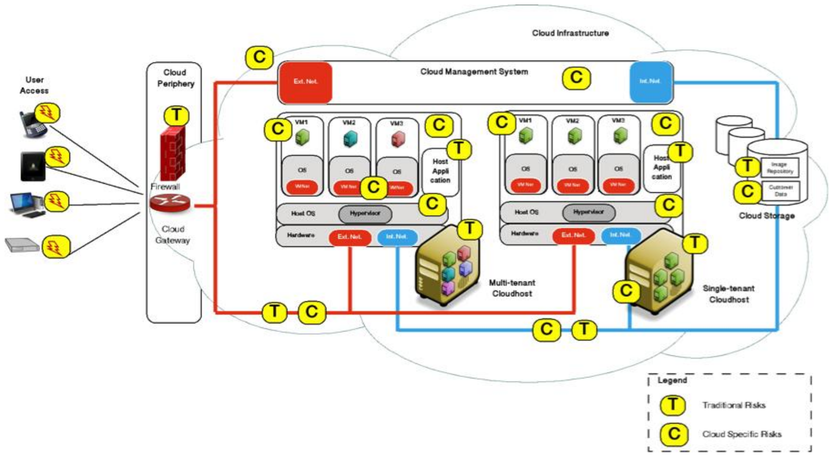

Fig 4: Security attacks in infrastructure as a service(IaaS) cloud environment, [49]

1.2.1. The Cloud: Non-Technical Issues

Legal issues and compliance have been recently addressed by researchers [53][21][54][55] analyzing the key issues outlined by ENISA. In relation to our research purpose we will discuss the legal issues related to data protection, data security and data location in the cloud, since they are considered main requirements for compliance with video surveillance laws. The following questions will be addressed in this section:

1. How data protection law applies and what are the responsibility roles for the data controller (owner) and the data processor (provider) in a cloud environment?
2. How data should be stored and operated?
3. Where data can be stored?
4. Who can access data?

1.2.1.1. Data Protection

In common pubic cloud computing scenarios, personal data is processed and stored in a virtualized infrastructure, where multiple customers can share same physical resources, and it can be transferred from one data center to another, without the knowledge of the next location of resources. This can violate data protection laws of organization's asset if no prior risk assessment was performed [45]. Two documents providing guidelines have been published on the use of cloud computing by the European regulator [56]and UK Information Commissioners Office (ICO) [20], which approves the use of cloud computing. The documents provide guidelines to protect personal data in the cloud, explaining the procedures to be considered prior to moving to cloud computing to protect personal data and lists the duties and obligations of data controller and data processors, in order to comply with the principles listed in EU Data Protection Directive 95/46EC and UK Data Protection Act 1998(DPA). Video data constitutes personal data thereby falls under DPA [57]. The following sections will discuss the main points in both ICO's and DPA's guidelines that are related to cloud computing.

1- Roles of Data controller & Data processor:

“How the data protection law apply and the roles of data controller and data processor in cloud environment?”

The guidelines emphasized the need to identify the data controller (owner) and the data processor (operator) and their interaction to identify who is responsible to be compliant with data protection laws. This helps the cloud customer to understand their obligation and what data protection risks that cloud computing presents and similarly, for the cloud provider to understand data protection requirements to make their service more efficient to customers that are subject to DPA laws [20]. The guidelines defined the controller as the one who determines the purpose of processing personal data and has the highest responsibility for complying with the DPA.The processor is the one who processes personal data on behalf of the controller [20]. Applying these roles to our proposed cloud-based video surveillance model gives the following assumption:

(The organization is the operator of video surveillance system such as a local government council. They use a third party application for forensic video analysis to run in a cloud computing environment. The organization will be a data controller for the video data processed by the application since they are the one who determine the purpose for which video data is processed. Cloud computing platform will be acting as the data processor".)

Now by identifying the organization as the data controller, we understand that all the duties and obligations imposed by the Data Protection Act 1998 are upon the controller (data owner). This relates to the collection, storage, retention, access, and ensuring that security measures are adequately placed by the processor.

2- Data Security:

“How data should be stored and operated?”

The Seventh principle of the Data Protection Act states that: "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data" In accordance with this principle, the security requirement is only applied to the data processor by having to select the appropriate security measures taking into account the type of data being processed and the harm that might result from unauthorized access and misuse of the system. Putting this into the context of the cloud, the location of data in relation to the data controller is different for a public cloud. The data is stored remotely and the data control depends on the cloud service model. Compliance with the seventh principle requires that the cloud provider provides the basic security to data, and the customer (data controller) reviews the guaranteeing of availability, confidentiality and integrity of data through following an audit trail [20]. Figure 5, shows the relationship between the role of data controller and data processor.

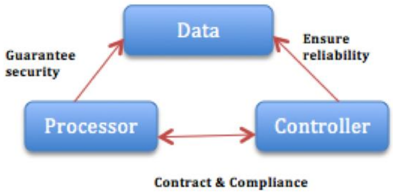

Fig 5: Relationship between the role of data controller & data processor

Given the above, The UK ICO guidance advices the data controller to assess and monitor the security measures by arranging an independent third party as a part of a standard certification to conduct a security audit of provider's services [58]. This will help a customer to monitor and check if the provider implements appropriate security and also to comply with its data protection obligation. It further reminds the customer to encrypt data in transit and at rest, to keep the encryption key at the customer premises, make sure all data copies made by the provider are completely deleted by the retention period. Data controller is not to be considered complying unless there is a written contract. Therefore, there should be a negotiation for SLA, including all requirements needed for data to be stored and processed in the cloud and to prevent the processor breaching the agreement.

3- Data Location:

“Where is the data stored?”

The Eighth principle of the Data Protection Act 1998 states that: "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data", Cloud provider may have data centers distributed across different geographical areas. This results in different laws and jurisdictions applying across countries. A consumer may specify the location of where data should be stored in their contract with the cloud provider (e.g. the Amazon cloud), However, determining which specific server or storage device will be used is difficult to verify due to the dynamic nature of cloud computing [59]. Even if they do, data may be subject to transfer without being informed [53]. This result in cross-jurisdiction by having to determine what law applies to which country and activity. Referring to the eighth principle, processing personal data is only restricted in EEA and to countries listed in the Safe Harbor Scheme[60] that can ensure an adequate level of protection to comply with all principles and the Act as a whole. There are some exceptional cases where data can be transferred to a non EEA country but this requires conducting a priori risk assessment. The cloud provider should guarantee lawfulness of cross-border data transfer and is included in a customer's contact agreement. Otherwise it could breach the eighth data protection principle.

4- Subpoena and E-discovery:

“Who can access data?”

When there is a subpoena by law enforcement agencies for investigation, they may have the power to require the cloud provider to give them access to personal data. However due to the shared multi-tenancy architecture, this may cause other customers who may reside on the same physical servers to be at risk of the disclosure of their data to undesirable agents. One solution that can solve this problem is to encrypt data to ensure data protection in case provision for such disclosure [35]. However, malicious insider is another threat. It can be employers working for cloud provider who has access to the system or an attacker's virtual machine resides on the same physical machine where data is stored.

It has been shown above that many security issues are found in cloud computing, whether technical or non technical, due to a customer's lack of control and multi-tenancy nature of cloud computing. The security and privacy laws that regulate video data does not take the virtualization environment into account, which present challenges for a cloud provider to comply with [61] within a cloud based video forensic system. For example Amazon AWS [62] states that its virtual infrastructure has been designed to provide high security and ensure complete customer privacy to promote compliance with for e.g. healthcare and other governments needs [63][64]. However, a question of trust still remains as a challenge, whether cloud providers would comply with what they have promised, and how transparent they are about security breaches. Therefore the potential use of clouds such as Amazon AWS for video forensics needs careful thought and trusted collaboration with the service provider.

6. Recommendation & Conclusion

In this paper we have investigated the security and privacy related legal requirements in deploying cloud-based video surveillance systems. In particular the study was conducted in relation to a video forensic system that requires data storage both in its original annotated formats, operating a number of video surveillance algorithms and conducting an effective search. Maintaining security at all levels of the video forensic system when deployed within a cloud is important. Table 2, summaries the key legal requirements that originate from the data protection act that governs the legal compliance of a video surveillance that can provide evidence that will be legally acceptable. The table further tabulates the challenges one must meet when using a cloud infrastructure to deploy a video forensic system.

Table 2. Summaries of the key legal requirements and the corresponding video surveillance system compliance and cloud computing challenges

Legal Requirement (Data Protection Act)	Video Surveillance System Compliance	Cloud Computing Challenge
Fair & Lawful	Controller is responsible to ensure that the law is obeyed	Provider's Level of transparency is not clear
Purpose	Annotation of stored video database is carried out only when there is a need for a forensic investigation	Possibility exists for malicious insider attacks
Accuracy	Ensure authenticity & integrity of video data	Possible data loss /leakage/manipulation
Retention	Retention requirements can depends on organization using the system	For a complete removal of data a device need to be destroyed which is not possible in cloud environment. Also Attackers may be able to recover data due to resource sharing
Security	Protect annotation engine (i.e. processing algorithms), video database & annotation database	Possible application, network, virtualization & interface attacks
International data transfer	Transfer data only within EEA & countries having similar data protection laws	Specific data location is unknown

Based on the information summarized in table-2, the following recommendations can be made:

- The controller of a video surveillance system is responsible for ensuring that the system complies with security and privacy requirements. When implemented within a cloud based environment the cloud provider's level of transparency is not always clear to the controller. Therefore the controller can outsource to a reputable third party auditor to monitor security and levels of disclosure of data.

- Data within the annotation database of the video forensic tool should only be created when it is necessary for law enforcement purposes. When implemented within a cloud based environment, as an alternative to having dedicated hard- ware idling, ready to store the large amounts of annotated data produced when an investigation needs to be carried out (i.e. when implemented within a non-cloud environment) the resource pooling characteristics of a cloud should be effectively utilized.
- Security measures must be put in place to prevent video data from unauthorized access and preserve accuracy, while in transit (network) and at rest (storage). Although various security measures are implemented by cloud providers, known real world examples exists of past, unpredicted breaches and outages. Although a definite solution does not exists as yet, on-going work by both academic and industry researchers should ensure improved levels of security in the future. Nevertheless, video surveillance data and its associated meta- data are very sensitive and not suitable to be stored in a public cloud. Using a private/hybrid cloud can be alternative solutions at present. Added levels of security to ensure that a cloud based architecture can be used for video forensics can greatly affect performance of the surveillance system due to the need of substantial operational/processing overhead to ensure security. It is vital that a trade-off between security and performance is considered[65].

Acknowledgements

This work is sponsored by the Ministry of Manpower, Oman. We would like to thank Dr.Olaf Maennel for providing helpful feedbacks and suggestions. We also want to thanks the authors who worked on the CrimeVis project and allowed using it as a case study in our research.

7. References

[1] Frank Gens, “IDC eXchange » Blog Archive » New IDC IT Cloud Services Survey: Top Benefits and Challenges,” 2009. [Online]. Available: http://blogs.idc.com/ie/?p=730. [Accessed: 26-Sep-2014].

[2] “VSaaS - Video Surveillance as a Service.” [Online]. Available: http://www.vsaas.com/. [Accessed: 24-Sep-2014].

[3] D. Neal and S. M. Rahman, “Video surveillance in the cloud-computing?,” in *2012 7th International Conference on Electrical and Computer Engineering*, 2012, pp. 58–61.

[4] M. S. Hossain, M. M. Hassan, M. Al Qurishi, and A. Alghamdi, “Resource Allocation for Service Composition in Cloud-based Video Surveillance Platform,” in *2012 IEEE International Conference on Multimedia and Expo Workshops*, 2012, pp. 408–412.

[5] M. A. Hossain, “Analyzing the Suitability of Cloud-Based Multimedia Surveillance Systems,” in *2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing*, 2013, pp. 644–650.

[6] M. A. Hossain, “Framework for a Cloud-Based Multimedia Surveillance System,” vol. 2014, 2014.

[7] Y. H. Xiong, S. Y. Wan, Y. He, and D. Su, “Design and implementation of a prototype cloud video surveillance system,” *J. Adv. Comput. Intell. Intell. Informatics*, vol. 18, no. 1, pp. 40–47, 2014.

[8] D. A. Rodriguez-Silva, L. Adkinson-Orellana, F. J. Gonz’lez-Castano, I. Armino-Franco, and D. Gonz’lez-Martinez, “Video Surveillance Based on Cloud Storage,” in *2012 IEEE Fifth International Conference on Cloud Computing*, 2012, pp. 991–992.

[9] “Welcome to Apache^{TM} Hadoop®!” [Online]. Available: http://hadoop.apache.org/. [Accessed: 24-Feb-2015].

[10] “HDFS Architecture Guide.” [Online]. Available: http://hadoop.apache.org/docs/r1.2.1/hdfs_design.html. [Accessed: 24-Feb-2015].

[11] J. Dean and S. Ghemawat, “MapReduce,” *Commun. ACM*, vol. 51, no. 1, p. 107, Jan. 2008.

[12] A. Heikkinen, J. Sarvanko, M. Rautiainen, and M. Ylianttila, “Distributed multimedia content analysis with MapReduce,” in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2013, pp. 3497–3501.

[13] C. Ryu, D. Lee, M. Jang, C. Kim, and E. Seo, “Extensible Video Processing Framework in Apache Hadoop,” in *2013 IEEE 5th International Conference on Cloud Computing Technology and Science*, 2013, vol. 2, pp. 305–310.

[14] “FFmpeg.” [Online]. Available: https://www.ffmpeg.org/. [Accessed: 01-Dec-2014].

[15] 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 *2012 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing*, 2012, pp. 655–660.

[16] H. Tan and L. Chen, “An approach for fast and parallel video processing on Apache Hadoop clusters,” in *2014 IEEE International Conference on Multimedia and Expo (ICME)*, 2014, pp. 1–6.

[17] “Digital Imaging Research Group :: Projects :: CrimeVis.” [Online]. Available: http://imaging.lboro.ac.uk/projects/CrimeVis/. [Accessed: 06-Oct-2014].

[18] Cloud Security Alliance, “Security Guidance for Critical Areas of Cloud Security in Cloud Computing.” [Online]. Available: https://cloudsecurityalliance.org/research/security-guidance/. [Accessed: 01-Mar-2014].

[19] “CCTV code of practice,” 2008. [Online]. Available: http://www.belb.org.uk/downloads/foi_cctv_code_of_practice.pdf. [Accessed: 15-Mar-2014].

[20] ICO, “Guidance on the use of cloud computing,” 2012. [Online]. Available: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf. [Accessed: 19-Mar-2014].

[21] T. V. Lillard, *Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data*. Syngress Publishing, 2010.

[22] ICO, “In the picture : A data protection code of practice for surveillance cameras and personal information.” [Online]. Available: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf. [Accessed: 01-Dec-2014].

[23] “BBC News - Emergency phone and internet data laws to be passed.” [Online]. Available: http://www.bbc.co.uk/news/uk-politics-28237111. [Accessed: 10-Jul-2014].

[24] “Surveillance Camera Code of Practice Surveillance Camera Code of Practice,” 2013. [Online]. Available: https://www.gov.uk/government/publications/surveillance-camera-code-of-practice. [Accessed: 15-Mar-2014].

[25] “BBC News - Surveillance camera code of practice comes into force.” [Online]. Available: http://www.bbc.co.uk/news/uk-23636462. [Accessed: 18-Mar-2014].

[26] N. Cohen and K. Maclennan-brown, “Digital Imaging Procedure,” 2007. .

[27] J. L. Nagel, G. P. C. Ibbons, and L. Jeffrey, “Getting ESI Evidence Admitted : Lorraine v . Markel American Insurance Co .,” 2007. [Online]. Available: http://www.metrocorpcounsel.com/articles/9210/getting-esi-evidence-admitted-lorraine-v-markel-american-insurance-co. [Accessed: 03-May-2014].

[28] M. Taylor, J. Haggerty, D. Gresty, and D. Lamb, “Forensic investigation of cloud computing systems,” *Netw. Secur.*, vol. 2011, no. 3, pp. 4–10, Mar. 2011.

[29] R. I. Rubin and M. J. Stempler, “Video Surveillance in Personal Injury Cases,” 2010.

[30] D. Neal, “Video Surveillance in the Cloud?,” *Int. J. Cryptogr. Inf. Secur.*, vol. 2, no. 3, pp. 1–19, Sep. 2012.

[31] “Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0.” [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/378448/66-08_Retrieval_of_Video_Ev12835.pdf. [Accessed: 24-Sep-2014].

[32] “Digital Images as Evidence - CCTV Information.” [Online]. Available: http://www.cctv-information.co.uk/i/Digital_Images_as_Evidence. [Accessed: 24-Sep-2014].

[33] Q. Mahmood Rajpoot and C. D. Jensen, “Security and Privacy in Video Surveillance: Requirements and Challenges,” in *ICT Systems Security and Privacy Protection*, vol. 428, N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, and T. Sans, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. p. 169–184.

[34] T. Winkler and B. Rinner, “Security and Privacy Protection in Visual Sensor Networks,” *ACM Comput. Surv.*, vol. 47, no. 1, pp. 1–42, Jul. 2014.

[35] D. Catteddu and G. Hogben, “Cloud Computing: Benefits, risks and recommendation for information security,” 2009.

[36] R. Buyya, J. Broberg, and A. M. Goscinski, “Cloud Computing Principles and Paradigms,” Mar. 2011.

[37] E. J. Schweitzer, “Reconciliation of the cloud computing model with US federal electronic health record regulations.,” *J. Am. Med. Inform. Assoc.*, vol. 19, no. 2, pp. 161–5, 2011.

[38] W. a Jansen, “Cloud Hooks: Security and Privacy Issues in Cloud Computing,” *2011 44th Hawaii Int. Conf. Syst. Sci.*, pp. 1–10, Jan. 2011.

[39] D. Chen and H. Zhao, “Data Security and Privacy Protection Issues in Cloud Computing,” *2012 Int. Conf. Comput. Sci. Electron. Eng.*, no. 973, pp. 647–651, Mar. 2012.

[40] B. Grobauer, T. Walloschek, and E. Stocker, “Understanding Cloud Computing Vulnerabilities,” *IEEE Secur. Priv. Mag.*, vol. 9, no. 2, pp. 50–57, Mar. 2011.

[41] K. Dahbur, B. Mohammad, and A. B. Tarakji, “A survey of risks, threats and vulnerabilities in cloud computing,” in *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications - ISWSA ’11*, 2011, pp. 1–6.

[42] F. Rocha and M. Correia, “Lucy in the sky without diamonds: Stealing confidential data in the cloud,” in *2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W)*, 2011, pp. 129–134.

[43] M. T. Khorshed, A. B. M. S. Ali, and S. A. Wasimi, “A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing,” *Futur. Gener. Comput. Syst.*, vol. 28, no. 6, pp. 833–851, Jun. 2012.

[44] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey, you, get off of my cloud,” in *Proceedings of the 16th ACM conference on Computer and communications security - CCS ’09*, 2009, p. 199.

[45] Z. Xiao and Y. Xiao, “Security and Privacy in Cloud Computing,” *IEEE Commun. Surv. Tutorials*, vol. 15, no. 2, pp. 843–859, 2013.

[46] B. J. Brodkin, N. W. Cloud, S. Risks, C. Computing, and G. A. Engine, “Gartner : Seven cloud-computing security risks,” pp. 2–3, 2008.

[47] “Cloud Security Alliance.” [Online]. Available: https://cloudsecurityalliance.org/. [Accessed: 21-Mar-2014].

[48] CSA, “The Notorious Nine Cloud Computing Top Threats in 2013,” 2013. .

[49] F. Doelitzscher, “Security Audit Compliance For Cloud Computing,” Plymouth University, 2014.

[50] N. Gonzalez, C. Miers, F. Redígolo, M. Simplício, T. Carvalho, M. Näslund, and M. Pourzandi, “A quantitative analysis of current security concerns and solutions for cloud computing,” *J. Cloud Comput. Adv. Syst. Appl.*, vol. 1, no. 1, p. 11, 2012.

[51] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,” *J. Internet Serv. Appl.*, vol. 4, no. 1, p. 5, 2013.

[52] P. K. Manadhata and J. M. Wing, “An Attack Surface Metric,” *IEEE Trans. Softw. Eng.*, vol. 37, no. 3, pp. 371–386, May 2011.

[53] P. Balboni, V. Mascheroni, A. Paolo, and B. Law, “Data Protection and Data Security Issues Related to Cloud Computing in the EU,” *Soc. Sci. Res.*, vol. 022, no. 022, pp. 1–12, 2010.

[54] M. L. Kemp, S. Robb, and P. C. Deans, “The Legal Implications of Cloud Computing,” in *Cloud Computing Service and Deployment Models*, A. Bento and A. K. Aggarwal, Eds. IGI Global, 2012.

[55] S. De Silva, “Key Legal Issues with Cloud Computing: A UK Law Perspective,” in *Cloud Computing Service and Deployment Models*, A. Bento and A. K. Aggarwal, Eds. IGI Global, 2012.

[56] “ARTICLE 29 DATA PROTECTION WORKING PARTY,” 2012. [Online]. Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf. [Accessed: 01-Jun-2014].

[57] “Determining what is personal data,” 1998. [Online]. Available: https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf.

[58] R. Marchini, *Cloud Computing: A Practical Introduction to the Legal Issues*. BSI, 2010.

[59] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. “O’Reilly Media, Inc.,” 2009.

[60] “FREQUENTLY ASKED QUESTIONS RELATING TO TRANSFERS OF PERSONAL DATA FROM THE EU / EEA.” [Online]. Available: FREQUENTLY A SKED Q UESTIONS RELATING TO TRANSFERS OF PERSONAL DATA FROM THE EU / EEA.

[61] F. Doelitzscher, C. Reich, and A. Sulistio, “Designing Cloud Services Adhering to Government Privacy Laws,” in *2010 10th IEEE International Conference on Computer and Information Technology*, 2010, pp. 930–935.

[62] “AWS Security Center.” [Online]. Available: http://aws.amazon.com/security/. [Accessed: 04-Dec-2014].

[63] “Amazon Health care complience.” [Online]. Available: http://media.amazonwebservices.com/AWS_HIPAA_Whitepaper_Final.pdf. [Accessed: 04-Dec-2014].

[64] “AWS GovCloud (US) Region Overview – Government Cloud Computing.” [Online]. Available: http://aws.amazon.com/govcloud-us/. [Accessed: 04-Dec-2014].

[65] L. M. Vaquero, L. Rodero-Merino, and D. Morán, “Locking the sky: a survey on IaaS cloud security,” *Computing*, vol. 91, no. 1, pp. 93–118, Nov. 2010.