

# Privacy-preserving Measures in Smart City Video Surveillance Systems

Shizra Sultan<sup>a</sup> and Christian D. Jensen<sup>b</sup>

*Department of Mathematics and Computer Science, Technical University of Denmark, DK-2800 Kgs. Lyngby, Denmark*

**Keywords:** Mass-scale Video Surveillance Systems, Smart City, Privacy, Information Security.

**Abstract:** Smart city video surveillance systems collect data from all around the city, and this aggregated data is used by several entities for achieving different city administrative tasks such as ensuring public safety and traffic management, to provide citizens with better services. This data, when combined with other smart city data sources, can reveal sensitive information about individuals, which if not used carefully can spawn grave privacy breach. In order to extract useful information from surveillance data without causing privacy invasion, it is important to see how, where and what information is collected about individuals, and how it is further used for said purposes.

## 1 INTRODUCTION

Smart cities (SC) signify the concept of information convergence from diverse data sources to provide well-informed services for both city administration and citizens. One of the key SC data contributors is mass-scale Video Surveillance Systems (VSS), which record public activities via video cameras, deployed all over the city. Major countries around the globe are investing heavily in SC video surveillance systems for accomplishing several administrative tasks such as ensuring public safety, traffic and infrastructure management, weather monitoring, etc. (Thom, 2018).

During the past two decades, VSS has evolved from simple video acquisition and display systems into intelligent (semi)autonomous systems. The development of digital video CCTV cameras and recorders have led to the latest generation of sophisticated video surveillance systems, with wide-area surveillance, reliable network-centric transmission, and enriched data analysis (Banu, 2017). Traditionally, humans (designated observers) viewed this data to observe events of interest, however, in past few years, due to the drastic increase in surveillance data; it has become a challenging and cumbersome job. Modern VSS can integrate some of the most sophisticated image and video analysis

algorithms to investigate the recorded data. These systems can perform various tasks such as object detection and tracking, face recognition, event detection, and prediction, behavior recognition, video summarization, etc., effectively. This is helpful in understanding the content of the surveillance data so that observers can take appropriate actions.

SC-VSS can process huge volumes of data, and retrieve the finest and meticulous information from it. The point of concern is the nature of the information that can be derived from it. On the one hand, it can provide valuable information in performing different administrative tasks of local authorities with greater efficiency and less response time. On the other hand, personal information about citizens can be obtained from it, which can be used to hurt them, personally and socially, by invading their privacy. The extracted information not being used for the purpose it is collected for is a privacy breach. The right to privacy is protected by different legislations in several parts of the world. According to recent European legislation, the General Data Protection Regulation (GDPR), surveillance data should be used for targeted purposes thus minimizing the collection and analysis of irrelevant personal data. It also states that poorly designed VSS not only portray a false sense of security but also violates the fundamental privacy right of individuals (GDPR, 2016). If smart cities fail

<sup>a</sup> <https://orcid.org/0000-0003-4201-9503>

<sup>b</sup> <https://orcid.org/0000-0002-0921-7148>

to preserve the privacy of their citizens then it will become a smart Panopticon rather than a (technology-equipped) user-centric city.

Smart cities require an efficient but privacy-aware VSS, which allows access to essential information for authorized observers without violating the privacy of individuals. Therefore, it is important to know who collects and owns the VSS data, what kind of information can be extracted from it, who has the authority to designate its access rights, and how it will be used. In order to achieve that, we will look at different aspects and modules of SC-VSS with the help of a general model in the first section, and the next section will discuss the privacy-preserving measures to implement a secure and privacy-aware VSS.

## 2 VIDEO SURVEILLANCE SYSTEM MODEL

In this section, we use a general model to represent the different functional units that make up a traditional VSS. This model has four basic modules: Capture, Transport, Monitoring, and Storage, as shown in Figure 1. In the first module, depending upon the purpose of surveillance, one or multiple cameras are deployed at different locations to cover the desired area. Each camera is assigned a unique identity in order to be recognized and generates a recording (video stream/file) of activities in a designated location. In the transport module, these recordings are transported to the monitoring room, or directly sent to the storage servers for archiving. In the monitoring module, humans or (semi)automated systems observe the live recordings/streams for events of interest. The storage module manages long-term storage of all the recorded video files. Each recording is of a particular duration and is archived so it can be retrieved later. The archived files and live streams can be requested from the monitoring room, where designated observers (human or systems) can view them. Monitoring room can be either a specific place where different stream/recordings can be viewed or it can be distributed to different rooms/observation-points (including hand-held devices) (Zhang, 2013). The recordings captured by VSS are called surveillance data and a lot of information can be extracted from its content, such as different types of objects, activities, physical location, time of the day, nearby objects and landmarks, etc. Generally, the surveillance data is accessible to the VSS owners, and they can further assign access rights

to different observers. These recordings can also be given as input to an intelligent system for automatic alert generation based on pre-defined events.

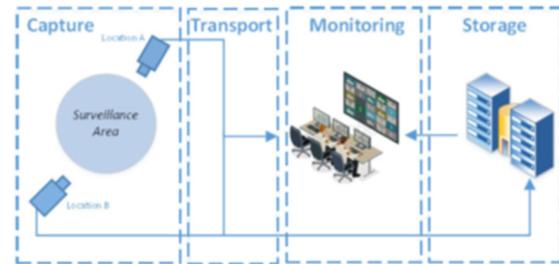


Figure 1: Video Surveillance System Model.

The model described above can be extended to any scale given the right hardware and software infrastructure. Conventionally, the VSS is centralized, and data from all the cameras is analyzed at a central processing and storage server. However, in mass-scale and real-time environments, many VSS are now deployed as a distributed network architecture, i.e. different functional units perform independent computational operations on given/assigned data and either take a decision upon it or forward it to the central node for further processing.

A smart city VSS is built on the traditional model and is deployed in a large environment, managed by the local administration. Thousands of video cameras may be deployed all around the city at various public places roads, parks, stations, town squares, etc. for several purposes. These cameras (Capture) are then connected via different wired and wireless networks (Transport) with several distributed storage and computational servers (Storage), and different observers can access any of the cameras live (Monitoring) or an archived recording (via Storage), from anywhere given they are connected to the system network (Perera, 2014). The objective of this paper is to understand how data is collected (Capture) and used (Monitoring) in SC-VSS in order to preserve the privacy of people recorded in data; therefore, we will focus more on three relevant data aspects:

- **Surveillance Data** (What is it, and what type of information it contain)
- **Data Owners** (Who (entities/systems) has the authority to collect, access, and distribute data)
- **Data Observers** (Who can access this data, and what are they supposed to do with it)

### 2.1 Surveillance Data

The most critical asset of any video surveillance sys-

tem (irrespective of its scale) is its data, mostly obtained from its primary data source i.e. video camera. Surveillance video cameras have different types such as unidirectional or omnidirectional field of vision, low light vision, or high-definition vision, infrared, etc. Choosing what type of cameras to be used at any location is dependent upon the purpose of surveillance (Limna, 2015). The surveillance data may also include other auxiliary data, such as the location of the camera, camera type, lens resolution, timestamp, and data from other sensors (microphone, GPS, etc.). Video data, combined with any other supporting data, increase the validity of the combined data with different contextual information and help observers make informed decisions.

In SC-VSS, surveillance data coming from all over the city is being collectively processed and evaluated with data from various public information systems that generate a lot of value. For example, cameras deployed over a highway may record the license plate of vehicles going too fast, which may then be compared against the vehicle registration database to issue a speeding fine to the vehicle owner. Conversely, data aggregation at such a large scale will also increase the privacy invasion threat as it contains sensitive information about citizens and if not managed properly raises serious concerns. For example, video surveillance data of informal public gatherings can be used to extract human faces, which can then be recognized from the national citizen database and can be used against the choice of the individual i.e. for racial profiling, or illegal surveillance, or spying on their personal life, etc. The use of surveillance data containing personal information in any way (without the consent of the individual) is a privacy breach. Though mass-scale VSS cannot obtain the explicit consent of every person being recorded all the time, general acceptance by the public must be ensured, i.e. that recordings will be used for public safety and law enforcement. In a real-world scenario, mass-scale surveillance data is used for multiple purposes that are often not explicitly consented by the public.

## 2.2 Data Owners

A data owner is an entity that has a legal authority to collect data at a certain location, store it or delegate its access to other observers (of choice). In city-scale surveillance systems, many data owners are collecting data, all around the city, for different purposes. Most countries have laws that require data owners to inform individuals that they are under video surveillance (e.g. through a display sign).

Based on their contribution to city surveillance data, VSS owners are categorized into four categories as shown in the Surveillance Area v/s Ownership matrix in Figure 2. There are several possibilities based on the nature of the surveillance area (private or public) and ownership of the surveillance area. Public owners can only collect data from public areas, while private owners can deploy VSS in private areas for property protection, as well as privately owned areas that are accessible to the public. VSS deployed in private areas cannot have public ownership, because this would be considered a violation of the citizen's privacy. The main three categories are:

- **Public-Public Ownership:** public area surveillance under public ownership
- **Public-Private Ownership:** public area surveillance under private ownership
- **Private-Private Ownership:** private area surveillance under private ownership

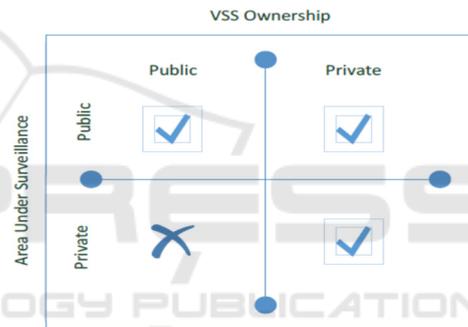


Figure 2: Surveillance Area v/s Ownership matrix.  
 1st Quadrant: Public area-Public Ownership  
 2nd Quadrant: Public area-Private Ownership  
 3rd Quadrant: Private area-Public Ownership  
 4th Quadrant: Private area-Private Ownership

### 2.2.1 Public-public Ownership

Public places such as parks, streets, bus stops, railway stations, airports, public offices, hospitals, etc. are generally under surveillance by public owners, i.e. national or local governments, and the VSS is managed in compliance with domestic surveillance policies. This includes both large open-space VSS by Law Enforcement Agencies (LEAs) and small-scale indoor VSS managed by other local departments. The main deployment purpose at these places is to monitor suspicious people, objects and activities to protect individuals, property and other personal or public belongings at those locations, to avoid crimes, harassment, vandalism, etc.

### 2.2.2 Public-private Ownership

The second most common VSS ownership is semi-public i.e. privately owned spaces concerning public areas such as banks, hotels, shops, malls, etc. The common purpose of surveillance here is property protection and facility management. Every owner has his own set of policies about cameras specifications, access and storage devices, etc., which generally complies with local surveillance guidelines, as they are recording citizens at a semi-public place.

### 2.2.3 Private-private Ownership

Third VSS ownership is private; individuals have deployed cameras inside their houses or private offices/property, to have proof if there was an outside intrusion. Footage from this surveillance is only of interest to the private owner, as it does not concern any other entity. Some of the privately-owned cameras are deployed (in private premises) in a way that records outside activities, e.g. public space, such as a nearby alley or road. The video recording of these places is owned by the owner/s of the property, but should not be used for any other purpose or else it would be voyeurism and against the law.

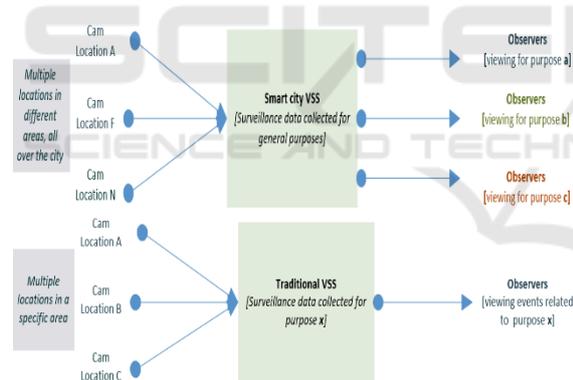


Figure 3: Traditional and SC-VSS model comparison.

Traditionally, each owner (public or private) uses his own data for a particular purpose and does not share or use data of any other owner. While in SC-VSS the data is being contributed by different owners (from different locations), which is aggregated and processed together, and then it is made available for all authorized applications and observers which can retrieve information relevant to their purposes as shown in figure 3. For example, earlier, the VSS deployed for ensuring public safety used the data to look for events that were related to human safety. In SC-VSS, various owners can retrieve different information from the same data, i.e. surveillance data

regarding human safety will be used by law enforcement authorities, data regarding traffic patterns by the traffic management department, and data about occupancy may be used by street sweepers and waste management services.

### 2.3 Data Observers

Once different owners record data at various places, the next step is to use that (aggregated) data for different purposes so they authorize usage rights to different observers. Data observers are authorized to extract information from surveillance data manually or via some application, i.e. they can be human or automated systems. Different local departments, such as LEAs, various emergency services, infrastructure & planning departments are interested in information that is relevant or helpful to their business operations. To achieve that, they designate skilled observers with different roles/responsibilities that they need to perform; based on the information they obtain from this data. Once it is decided who the observer is, the next step is to decide what type of information and how much of that information should be made available to them. In traditional and small-scale VSS, observers are mostly humans (guards or other employees) that monitor the real-time data to look for unusual activities. In the SC-VSS, there are a large number of observers, both humans, and semi-automated systems to observe data for unusual events as well as pre-defined activities (Khan, 2018). Data observers have a legal, social, and moral responsibility not to use data in any way that invades the privacy of an individual.

Access to all the required information in a timely manner help observers performs their duties in an efficient manner. Long-term analysis of such data can also prove to be very useful to make future decisions about city resources. For example, if the traffic management department is using the surveillance data, it can obtain information about mobility patterns, such as how many people travel from Point A to Point B, at what time of the day, and how long they spend on their commute. This information helps to decide which routes are busiest, which areas are visited most, but also the source and destination location of different citizens, which allows them to infer the location of their homes and work. The data can be used with another perspective to know how many people from a certain area visit certain places such as a bar, rehabilitation center, church, etc., or who are they going with (other humans), what are they carrying (objects), etc. The surveillance data of a rally in protest against a government can be used to

link protestors with their other routine activities, in order to intimidate them, or if the local authorities are using personal information (color, ethnicity, religious or gender bias) to stop them from certain activities. From the above example, it is evident that every piece of data, when seen with specific background information, reveals certain information to an observer (about an individual or a group of individuals). Data observers with the right intentions can use this information to provide better services, while biased observers can use this to harm or profile people. In order to preserve data privacy while offering utility in SC-VSS, we use our model presented to identify privacy requirements.

### 3 DATA PRIVACY

Video cameras capture everything happening in its line of sight, without any bias or prejudice (usually). It records the activities of the general public (passing the road, entering a building, boarding a train, etc.), objects associated with them (other people, vehicle, and luggage) and all the visible information present in the surroundings. Data collected at such a large-scale contains substantial information about any individual, so it is becoming critical to preserving an individual’s privacy in mass-scale video surveillance, where several data sources are gathering and using surveillance data for multiple purposes (Farooq, 2015). Personal data needs to be protected from unauthorized use and privacy-preserving measures must be proactive instead of reactive, i.e. privacy issues must be anticipated in advance before it affects an individual.

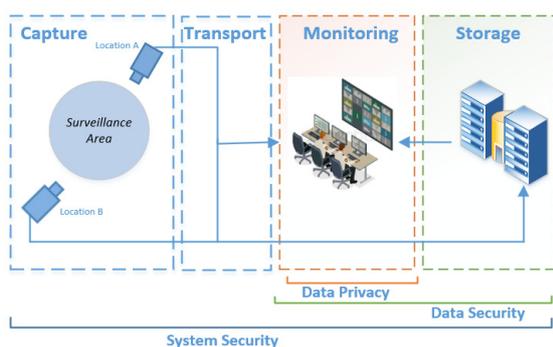


Figure 4: Security Aspects of SC-VSS.

When it comes to privacy-preserving measures, it is not an independent concept, rather a specific notion that involves (mostly) the personal information extracted from data. Privacy is a subset of data

security, while data security is a subset of system security (Kandah, 2013).

To explain it, let us look at Figure 4, as discussed earlier, VSS has four basic modules. The first two modules (Capture & Transport) do not process data (at least to a large extent) and only capture and transfer it, hence these have the least idea about the content of the data. These modules focus more on physical infrastructure rather than software components, i.e. cameras, recorders, wires, networks, monitoring and storage devices, etc. Therefore, the outermost layer to ensure data privacy is system security, which deals with ways to protect the basic infrastructure and operations/processes of the system irrespective of the nature of the data.

The central module of VSS is Storage with all the archived (processed) data. Different external and internal attacks (due to system and protocols vulnerabilities) tend to compromise the CIA triad (Confidentiality, Integrity, and Availability) of data. Hence, the middle layer to data privacy is data security, which refers to the preservation of received data (from Transport module) and should only be allowed to authorized observers (via Monitoring module) so the CIA of data is not compromised.

The module specifically related to data privacy is Monitoring. It deals with what can be made available to the observers. Here observers have the choice to search for a particular recording as information (content) from either directly from Transport or from Storage. Data privacy measures ensure that information or content available to authorized observers complies with access control policies, which should be in accordance with the legal data protection regulations.

#### 3.1 Privacy-preserving Measures

Any system or service that involves personal data should have built-in essential privacy features and not be left as an add-on. In the smart city VSS, privacy by design refers to the implementation of all the required system security, data security and privacy-preserving measures at applicable modules. Every process such as data collection, aggregation, distribution, access, should be carefully checked for vulnerabilities and leakage. All system and data requirements must be transparent and documented, observable and independently verifiable i.e. what data is being recorded, where and how it is stored, for which purposes will it be used and how will it be presented to observers (Hynes, 2010). If all the information about the individuals is kept private then it defies the purpose of surveillance, and if all is made public, it

will be a privacy invasion catastrophe. For example, in case a camera captured a violent attack and the identity of the perpetrator is not being revealed (to preserve his privacy), then it negates the purpose of surveillance i.e. public safety. Alternatively, if the employees (working for local authorities) are accessing the surveillance data to view the personal activities of individuals, which has nothing to do with the said purpose, then it is a privacy breach. The owners collecting all this data and designating access rights to different observers are responsible for preserving data privacy and keeping it out of harm's way. Some of the important privacy-preserving measures in SC-VSS are:

### 3.1.1 Privacy and Utility Trade-off

The balance between utility and privacy is key to an efficient and secure SC-VSS. Observers need to access different types of information from the aggregated surveillance data to perform their duties. Often the information they require contains personal data (location or identity of people involved in an event, or present around an event, etc.), and it is important for a system to evaluate their requirements suitably such as whether an observer really needs to access that part of data or not. Does the required observer need all the information that may be extracted from the data? Does revealing personal information to the observer conform to the requirements of the observer's responsibilities? If the information is not provided, will it cause any inconvenience for the observers in completing their assigned task etc? Answers to these questions for a data access request will help to maintain a balance between utility and privacy (Jensen, 2014). For example, if strict privacy measures do not let emergency services obtain surveillance data of a person who needs medical attention, then it is an interruption in service provision. On the other hand, if anyone with slight knowledge about SC-VSS can create a scenario in which personal information is made accessible to them, then it is not so good either. There should be a balance between privacy and utility based on careful situation evaluation.

### 3.1.2 Public Consensus and Information Disclosure

Public consensus about disclosing personal information (in given scenarios) should be ensured before access to resources (recordings) is authorized. The public should be notified in detail about all the possible use cases in which surveillance data will be observed by any application or observer, either

independently or in collaboration with other data sources. There should be a feedback platform to register complaints from individuals if they have a case of a privacy breach when the data is being used for other than the mentioned use-cases. For example, in case a speeding violation is caught on camera; this and similar type of events are categorized as a 'traffic violation' by the system and will be shared with traffic management observers (a system in this particular case). The traffic observer can detect the vehicle's license plate (particular information about an object) and via that information, it can know about the vehicle owner and issue a ticket to that individual. This is often acceptable to the public, but if the same system tries to extract information about individuals for profiling and advertisement purposes, then it is a privacy breach, as the system is obtaining information from surveillance data that is not used for predefined purposes or use-cases (Ambrosin, 2018). There may be authorized observers that have permission to access a part of personal data, but how they use that data is important.

### 3.1.3 Situation-aware Access Control

Privacy requirements vary dynamically with the observer's demands and situational changes in the data content (Wagner, 2015). Ideally, SC-VSS should adequately control information flow based on the requirements of the observer and the situation of the individuals. For example, in case of an emergency, if an individual's situation requires a particular service (say a fire engine), and observers (of the fire department) request access to the data at the location where the event happened. The data will have personal information that is related to that event (number of affected people, gender and estimated age of the people, the extent of the injuries of each individual, etc.) and should be made available to the observers so they can evaluate the situation clearly. In ordinary scenarios, it will be preferred that an observer does not have access to any data that has personal information about any individual (S.Oni, 2019).

An access control mechanism is a necessary tool for SC-VSS applications. Any observer should only be allowed to obtain personal information in case of precise conditions or events, which are defined in terms of quantifiable attributes of observers, recordings and real-time situations. Once all (observer's, recording's and situational) attributes are satisfied, only then can the observer access the data (Rajpoot, 2015). Each owner/stakeholder must clearly state all the potential observers who will have

access to their information and in what role. Different levels of privacy should be available for different roles i.e. personal information (faces, identities, associated information such as vehicles, current location, residential area, and work area) should not be made visible to the observer if it is not required by the offered SC-VSS service, specifically related to his role. Data transformations like sanitization, generalization, anonymization, etc. must be properly assessed and observers should be allowed to access personal information at a minimum level of requirement. Situation-aware access control mechanisms will provide robust yet flexible control in information flow to the observers.

### 3.1.4 Metadata and Digital Rights Management

The large-scale systems have huge data volume and variety (content and supporting data), which is categorized under different labels and is called metadata. Metadata describes data; it categorizes information (extracted from data) into different classifications, by arranging them in a structured and organized manner, which makes it easier to index and search for observers (Eckhoff, 2011). VSS metadata management enables to store semantic information (data content) with its related non-semantic information (device and network data) such as the location of the camera, timestamp of the recording, assigned observer, etc. In many cases, observers do not have access to the whole data but a certain part of it, i.e. auxiliary data or less-sensitive metadata, can still infer useful information without looking at the actual content (data that is not available). For example, an observer can deduce the location of the camera, by looking at the less-sensitive region (background of an image/recording) or by knowing the location and timestamp of a past event. Thus, metadata needs to be managed with the same care as the surveillance data is, otherwise, it can cause a privacy breach.

### 3.1.5 Forward and Backward Privacy

Forward secrecy or privacy refers to the concept that if a certain observer or service had access to certain data in certain situations (in the past) and now that those conditions are not available, then they should not be able to access them. Backward secrecy or privacy means that if an observer accesses a recording in the present time, then he should not be able to access previous information when he did not have the present situation (Hoang,2019). For example, if a police officer was given access to surveillance

footage that detected an accident, then he should only be allowed to access the footage during the time of the accident (within a reasonable and sufficient time window), and not before the accident and not after the situation is resolved. If the observer needs to access more information, regarding a particular incident then the request should be evaluated with additional conclusive attributes.

### 3.1.6 Modular Privacy Framework

If several entities are contributing and accessing data via central SC-VSS, then there can be many differences in terms of physical infrastructure, systems and security requirements, data capturing and storage formats, metadata characteristics, access control policies, privacy requirements and many more (Simion, 2015). In this scenario, as all the services are offered based on aggregated data, the security and privacy needs of different departments (observers) may overlap with each other. As data is collected from different locations with different purposes, and privacy requirements of locations, individuals, assigned observers could be different. Utility (based on information from data) of one observer might surpass the need for the privacy of another observer, which poses grave privacy risks. Modular and central security concept both needs to be implemented here, in modular architecture, all observers ( departments offering services) should implement privacy measures according to their specific needs (at their end) and centralized VSS should have an integrated privacy-aware approach, keeping in mind the privacy needs of the general public. This will provide two-tier security; if anything is missed in the modular architecture then the central architecture will manage it. For example, in case a surveillance camera registers a traffic violation, it requests the vehicle registration database to reveal the information about the specific vehicle that performed a violation and share this with another system that will issue the fine. No involved entities will share data in any other scenario unless the specified conditions are met. All systems have their own security measures that will not allow unauthorized observers to access the private information of any user, though in specific conditions they may share the private information of an individual.

### 3.1.7 Legislation

There are different data protection legislations followed around the world, which standardize how personal information should be collected and processed, so the privacy of an individual is not

compromised (Cranor, 2002). These standards reduce the trust issues between individuals and different applications. Systematic auditing and accountability by regulatory authorities will provide checks and balances for observers as well as for individuals. When it comes to SC-VSS, privacy-preserving measures should show compliance with these legislations especially the ones they are obligated to legally (regional, federal or international law). Some countries have fewer restrictions on surveillance systems when LEAs are using them, sometimes there is privacy intrusion, but they are not considered illegal. Other countries have strict surveillance regulations, for instance, Canada and Denmark do not allow obtaining personal information from surveillance data, unless it is legally authorized for a specific purpose, and even then, the authorization has a short time window (Rajpoot, 2014). In the USA, surveillance systems must abide by both national and federal laws while obtaining personal information for any purpose.

## 4 CONCLUSION

Due to the unceasing data gathering in smart city video surveillance systems, citizens expect local administrations to offer real-time and informed services in different areas such as public safety and traffic management, without violating their privacy. This paper analyses an SC-VSS model, and inspects its different modules and data aspects to look for privacy concerns, and suggests essential privacy-preserving measures. It concludes that the flow of information to observers should be looked upon critically as most of the privacy breaches happens at their end i.e. how they use it for different purposes. Therefore, it is essential to know how surveillance data is collected and distributed, who has access to this data, and whether they pose any threat to the privacy of individuals whose information is part of the data. To preserve privacy, it is important to limit observers' access to information for authorized purposes with situation-aware access control mechanisms made in accordance with applicable legislation.

## REFERENCES

- L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C, April 2002
- GDPR and Video Surveillance, 2016. [https://edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance\\_en](https://edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en)
- Rajpoot Q.M., Jensen C.D. 2014. Security and Privacy in Video Surveillance: Requirements and Challenges. In ICT Systems Security and Privacy Protection. SEC 2014. Springer, Berlin, Heidelberg
- B. Simion, D. N. Ilha, S. Ray, L. Barron, A. Demke Brown, and R. Johnson, "Slingshot: A modular framework for designing data processing systems," 2015 IEEE International Conference on Big Data (Big Data), Santa Clara, CA, 2015
- S. Oni, Z. Chen, A. Crainiceanu, K. Joshi and D. Needham, 2019, "Situation-Aware Access Control in Federated Data-as-a-Service for Maritime Search and Rescue," 2019 IEEE International Conference on Services Computing (SCC), Milan, Italy.
- T. Hoang, A. A. Yavuz and J. Guajardo Merchan, 2019. "A Secure Searchable Encryption Framework for Privacy-Critical Cloud Storage Services," in IEEE Transactions on Services Computing.
- Rajpoot, Qasim & Jensen, Christian Damsgaard & Krishnan, Ram. (2015). Integrating Attributes into Role-Based Access Control.
- M.Ambrosin, P.Braca, Mauro Conti, and Riccardo Lazzaretti. 2018. ODIN: Obfuscation-based privacy preserving consensus algorithm for Decentralized Information fusion in smart device Networks. 1, 1, Article 1 (July 2018)
- Jensen, Christian D., 2014, The importance of trust in computer security. In *Proceedings of the 8th IFIP WG 11.11 International Conference on Trust Management (IFIPTM 2014)*.
- F. Kandah Y. Singh W. Zhang C. Wang "Mitigating colluding injected attack using monitoring verification in mobile ad-hoc networks" *Security and Communication Networks* pp. 1939-0122 2013.
- M.U. Farooq M. Waseem A. Khairi S. Mazhar "A Critical Analysis on the Security Concerns of Internet of Things (IoT)" *International Journal of Computer Applications* (0975 8887) vol. 111 no. 7 February 2015.
- Atrey, P.K., Yan, W., Kankanhalli, M.S.: A Scalable Signature Scheme for Video Authentication. *Journal of Multimedia Tools and Applications* 34, 107–135 (2007)
- Liu, F., Hartmut, K.: A Survey of Video Encryption Algorithms. *Journal of computers & security* 29, 3–15 (2010)
- Z.Khan, Z.Pervez, A.G.Abbasi, "Towards a secure service provisioning framework in a Smart city environment", *Future Generation Computer Systems*, Volume 77, 2017, Pages 112-135
- G. Hynes, V. Reynolds, and M. Hauswirth, "A context lifecycle for web-based context management services," in Smart Sensing and Context, ser. *Lecture Notes in Computer Science*. Springer Berlin/ Heidelberg, 2009, vol. 5741, pp. 51–65.
- C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, "Context-Aware Computing for The Internet of Things: A Survey," in *IEEE*

- Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414-454, First Quarter 2014
- Shanhong Liu, 2018, BIS Research, <https://www.statista.com/statistics/864838/video-surveillance-market-size-worldwide/>
- Thom, 2017, <https://www.get-licensed.co.uk/get-daily/eight-places-youll-always-be-on-cctv-cameras-in-2018/>
- V. C. Banu, I. M. Costea, F. C. Nemtanu, I. Bădescu, "Intelligent video surveillance system," *2017 IEEE 23rd International Symposium for Design Technology in Electronic Packaging (SIITME)*, Constanta, 2017, pp. 208
- S. Zhang, Y. Lin and Q. Liu, "Secure and Efficient Video Surveillance in Cloud Computing," *2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems*, Philadelphia, PA, 2014, pp. 222-226
- T. Limna and P. Tandayya, "Video surveillance as a service cost estimation and pricing model," *2015 12th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, Songkhla, 2015, pp. 174-179.
- Wagner, Isabel, and David Eckhoff. "Technical Privacy Metrics." *ACM Computing Surveys* 51.3 (2015): 1-38.
- D. Eckhoff C. Sommer F. Dressler R. German T. Gansen "SlotSwap: Strong and affordable location privacy in intelligent transportation systems" *IEEE Commun. Mag.* vol. 49 no. 11 pp. 126-133 Nov. 2011.

