

# Research Trends in Surveillance through Sousveillance

Siraj Munir<sup>1</sup>

Department of Computer Science  
Mohammad Ali Jinnah University  
Karachi, Pakistan

Syed Imran Jami<sup>2</sup>

Faulty of Computer Science  
Mohammad Ali Jinnah University  
Karachi, Pakistan

**Abstract**—Collective Intelligence is an immense research area that has wide application to cross-disciplines, like social, legal, and computation. Research trends in Surveillance find its place in the work of this area generating curated data set helpful in answering complex queries. Sousveillance is a recent term coined by researchers and had been discussed in different literatures. However our findings suggest that integration of Surveillance through Sousveillance data set has not been given much importance in collective fashion. In this literature we introduced an effective model of collective intelligence by integrating surveillance through sousveillance in a campus environment. For testbed networking devices are used to generate sousveillance data to provide validation, and cleaning to enable reliability and trust in the target object.

**Keywords**—Semantics; querying; profiling; IoT; surveillance; sousveillance

## I. INTRODUCTION

Recent advancement in technology has given rise to several practical implications of surveillance and sousveillance. Sousveillance is a French origin word sous means below and veiller means watch combinational it means watching from below. Sousveillance Term was coined by Steve Mann et al. in [1, 2], that can be described as inverse of surveillance, surveillance on-demand and activity of particular entity for example person, officer, politician etc. using wearable computing. Analytics for Surveillance is still an active area in research community as researchers recently proposed some outstanding techniques for surveillance as shown in [3, 4]. Several use cases are identified for integration of surveillance with sousveillance, for better results in terms of accuracy in answering complex queries. Consider a scenario of police officer's behavior with citizens. It has been noticed in several incidents that on personal biasness, officer's behavior was non ethical and main concern is that these type of events were also surveilled. In some events no action was taken or either surveillance clip was not present that is somehow deleted. This raises a huge question mark on surveillance systems, and therefore requires the support of sousveillance. Surveillance has already proven its usage by providing potential solutions in different areas including computer science, and social sciences. Integrated approach of

Surveillance with Sousveillance would help in resolving different queries that are complex to solve. A detailed taxonomy of veillance is presented in Fig. 1 which clearly differentiates types of veillance and their sub-categories. There are eleven different categories of veillance as reported in [1]. Each category of veillance has its role like Dataveillance is used for doing veillance over online activities, while Counterveillance is using veillance for recording own actions. Beinveillance deals with the usage of veillance for benefits like presence of sence and turning on lights using sensors. Malveillance is veillance for malicious intent and Coveillance is peer-to-peer veillance like veillance of neighbors, family members etc. Other areas include Kineveillance and Stativeveillance that are veillance of mobile and stationary objects like electromagnetic waves etc. Autoveillance is veillance of quantified self/ body hacking. Uberveillance is surveillance which can be embedded in human body using state-of-the-art IoT based wearable computing. Some major problems with surveillance are:

- 1) Surveillance is a type of veillance about/ around a fix point.
- 2) What if surveillance system was on update while certain event happened.
- 3) What if any high profile person uses his/ her resources and delete surveillance data from system.
- 4) What if server was down when X terrorism event happened.

These are some of the major queries that require resolution using intelligent query engine. A potential solution to these queries is the integration of surveillance systems with sousveillance. The ongoing digital age where technology and computing are ubiquitous, the tracking of generated data through viillance will eventually help in solving many hurdles of our daily life. The major contribution of this work is the identification of problem with the discussion on research trends in ongoing work and proposed an integrated approach of Sousveillance with surveillance in the campus setting. Next section will discuss research trends in surveillance through sousveillance.

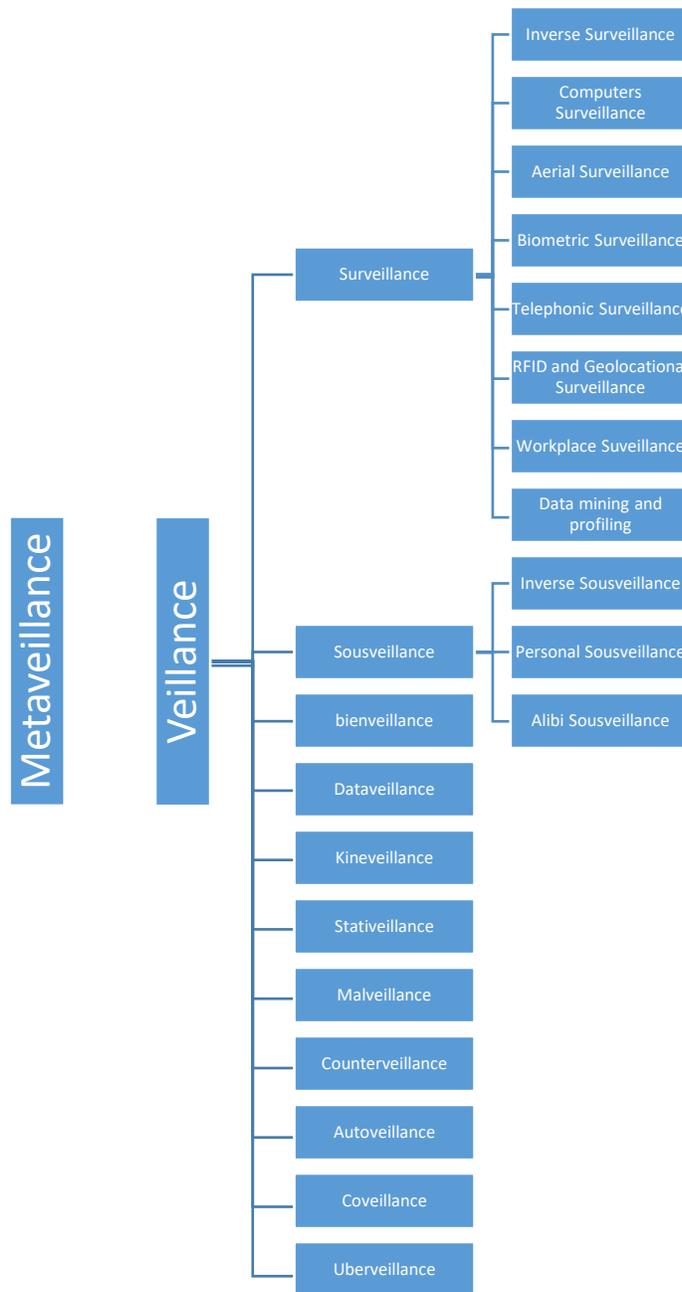


Fig. 1. Taxonomy of Veillance [2].

## II. RESEARCH TRENDS IN SURVEILLANCE AND SOUSVEILLANCE

Surveillance is a French originated word sur means over and veiller means watch collectively it means watching from above or about any fixed point. Furthermore, it can also be described as monitoring of individual/ individuals through different available sources that is social media, physical cameras etc. Moreover, there are two types of surveillance: Preconstructive surveillance and Reconstructive surveillance. Preconstructive surveillance is about to veillance any individual or group of individuals in a closed room under CCTV (Closed Circuit Television) while Reconstructive Surveillance is about veillancing using different law and

technological tools including fingerprinting, phone tapping, internet tracking etc. Several ways are available for surveillance including telephones, physical cameras, social network analysis, biometric surveillance, aerial surveillance etc. Recent research trends show wide range of problems to be solved in surveillance through computer vision [3, 4, 5, 7, 8, and 10]. Research in surveillance through computer vision deals with the analysis on huge bulk of collection of images and videos and provision of solutions in the identification and tracking of target object. In [3] authors have provided insights of video surveillance, with four million CCTV cameras by BSIA (British Security Industry Association) who deployed across the Britain states alone. A novel technique for hierarchical architecture was proposed as FVSA (Fused Video

Surveillance Architecture) which can provide multi-layer hardware abstraction which can effectively use with Internet of Things (IOT) based systems. The work in [4] discusses detection of gender using surveillance images. This is applicable for cold climate where detection and surveillance of gender based approach can help to law enforcement departments to catch guys with malicious intent. Proposed technique includes RCNN (Region-based Convolutional Network) and transfer learning. In [5], the authors discussed behavior of employee under organizational surveillance through computer-mediated technique. They surveyed full time adult employees and tried to observe organizational trust, privacy, commitment to organization etc. This study also shows surveillance application in social life style and workplace life. A study has been carried out in [11] that tried to determine how can 'Surveillance of Things' can be connected to IOT. Authors used Sigfox, a wireless network for IoT based devices, with assumption that the gathered surveillance data is incorrect and thus can have impact on people. Moreover, authors also established a linkage for surveillance of people to surveillance of things. The literature in [12] puts lights on usage of Big Data for surveillance specifically for digital citizenship and contemporary democracy. Authors proposed critical analysis of existing research works alongwith the suggestion on the working of ambivalent digital citizen mechanism that should be constructed to target every citizen. In [13], the authors proposed usage of RFID for object detection which can be used for surveillance purpose. In [14], authors proposed a new open source database for video surveillance, tracking, recognition and re-identification. Database contains collection of high resolution images which can be used for several task like evaluation of algorithms. The work in [15] reviews classic and recent approaches for object detection in dynamic environment. Authors also discussed different areas where object detection can help to resolve critical issues. Authors in [16] briefs usage of social media data surveillance for different aspects including behavioral analysis, medical insights/ news etc. In [6] authors briefed usage of video surveillance of moving objects and it's challenges and in response to these challenges they proposed different techniques to resolve the highlighted problem. Author in [17] highlighted usage of surveillance in computer vision to assist drivers on safety critical event. Furthermore, they evaluated proposed system on challenging dataset. Author in [7] proposes a bridge between classical object detection techniques. As literature describes in real world we have huge collection of surveillance videos. Detection of dynamic objects from these long-term video is a complex task. In this literature authors proposed a framework using Bag-of-word and classification approach which can resolve the aforementioned problem effectively with the highest accuracy of 92% on LOST (Longterm Observation of Scenes (with Tracks)) dataset. Author in [8] explored cost effective and optimized technique for dynamic object detection. Author in [9] puts light on current and future status of surveillance. Authors discussed different techniques for object detection, image enhancement, object tracking, object recognition etc. Further, authors stressed on usage of latest techniques including fog, cloud, edge computing and DL. Literature

summed up on expected future of surveillance using AR (Augmented Reality). [10] highlighted multi-cue object detection in dynamic environment and proposed a novel technique under different modularity's with state-of-art results. Further, they claimed that many literatures discussed multi-cue pros but only some literatures brief its modularity: singular or plural. [18] proposed an effective approach for crowd segmentation and classification. Literature introduced intelligent video surveillance for crowd using four metrics: crowd density, crowd saliency, crowd segmentation and statistical analysis. Steve Mann in [2, 17] carried various forms of veillance including surveillance (viewing from top from a fix point), sousveillance (viewing from below through mobile locations pervasively or non-pervasively), autoveillance (extreme level of surveillance is autoveillance), kineveillance (sensing through moving frame-of-reference), dataveillance (continuous tracking user digital data and personal data through social media, online transactions etc.), coveillance (simply peer-to-peer surveillance), countersurveillance (measure or practices taken to counter surveillance), malveillance (dangerous type of surveillance), stativeillance (surveillance of static frame-of-reference), bienveillance (machine sensing our presence and respond accordingly), uberveillance (surveillance using embedded devices). The discussions on these veillances have been made in the domains of social sciences and its related perspective but their algorithmic implementation using pervasive approaches have not explored yet. In this work we evaluated research literatures in the area of Sousveillance and we have found no progress since last three years surveillance. Steve Mann worked on Sousveillance [1] starting with a neck worn camera in 1997, however, in 2003 Microsoft introduced a slightly modified version of neck worn camera, while in 2006 Mann again released another modified version and finally in 2013 Memoto released version of neck worn camera device. This leads to the development of glass based devices including Meta, Google Glass, EyeTap, etc. Next section will discuss proposed methodology along with the results.

### III. PROPOSED METHODOLOGY AND RESULTS

In this section we have proposed an effective model for Citizen Profiling using surveillance and sousveillance. Citizen profiling can also be done through surveillance but as discussed in previous sections there can be various limitations to surveillance based system, which can be solved through the integration of surveillance with sousveillance. The work in [19] briefly discussed the issue of 'sousveillance less' surveillance systems and considered such systems as a half-truth: "if buildings can wear cameras why humans cannot" [19].

In this work we have proposed a model which can be adopted to use collective benefits of both surveillance and sousveillance which is still an open research question to solve issues related to Collective Intelligence. In Fig. 2, we proposed a model for citizen profiling. Proposed model consist of five steps: (i) data acquisition (using surveillance and sousveillance), (ii) storage, (iii) data representation, (iv) semantic engine, and (v) querying.

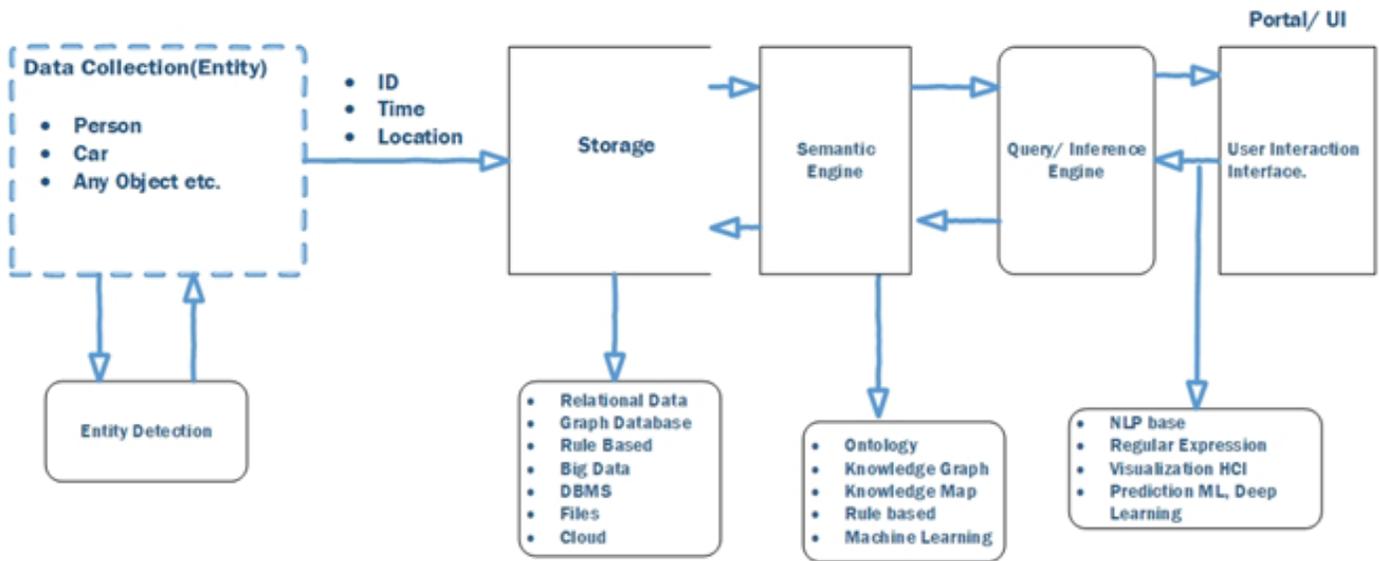


Fig. 2. Model for Citizen Profiling.

In Data acquisition the curated data is collected from environment using sensors and cameras that are dumped into storage as raw data. Storage can be of any variant of available services i.e. Relational database, graphs, NoSQL, etc. whose usage is dependent on the scenario related to the magnitude of organization from small scale to large scale to social media. In campus setting we employed NoSQL for fast processing where it does not require structure. To maintain semantics among entities, Semantic engine is implemented using ontology and Knowledge Graph to employ temporal data from sousveillance devices. Other potential solutions include Rule based or Machine Learning approaches to learn rules and infer them on the creation of new entities. Fourth and fifth phases deal with the querying engine and user interface, that may use NLP, Regular Expression, Machine Learning / Deep learning to search out object data in storage and display profile data to end-user. For proof of concept we made a dataset of network traces having three columns namely (Timestamp having time and date, MAC address represents each individual device and switch id represents location). We randomly generated data for aforementioned columns. Furthermore, we collected data from NMS (Network Management System) through smartwatch where smartwatch is supposed to be used as a sousveillance device. Here Fig. 3 shows how our data looks like in general format.

Some sample semantic queries are as follows:

- 1) Where was XYZ person at time X.
- 2) At what timestamp X person visited library.
- 3) Through which switch did Person X having MAC XX was connected.
- 4) Who was connected to switch X at XYZ time?

The result of sample query 4 is shown in Fig. 4.

	TimeStamp	MAC_add	Switch_id
0	2018-05-10 5:19:26	10:AA:BE:CC:CE:26	3
1	2018-05-30 16:2:51	12:BA:CD:RW:01:89	7
2	2018-04-19 8:12:33	SW:NI:TE:MO:ET:98	7
3	2018-05-22 0:16:36	OL:JQ:OK:QR:UL:16	6
4	2018-05-16 22:59:8	NA:HF:LU:TF:RX:98	8

Fig. 3. Surveillance and Sousveillance Data.

TimeStamp	MAC_add	Switch_id
2018-05-30 16:2:51	12:BA:CD:RW:01:89	7

Fig. 4. Query Result.

Surveillance devices are used in detection of objects while Sousveillance data is gathered from network monitoring devices. The network monitoring devices help in verifying, validating and cleaning the object detection data from the surveillance fields. Result in Fig. 4 is showing that the object having network device with given MAC address is currently located at the given location (where switch number 7 is placed) at the given time and date.

#### IV. CONCLUSION

In this paper we proposed a model for citizen profiling which uses surveillance and sousveillance for data acquisition. We also reviewed some recent research work for surveillance and sousveillance. Previous sections highlighted key problems and solutions of surveillance and sousveillance with the discussion on detailed taxonomy for veillance. Our results show that integration of sousveillance with surveillance system will give extended data that will increase reliability and trust.

Several extensions are planned in next phase. The increasing amount of data in terms of velocity and variability will require big data based solutions in analytics. Furthermore, automated learning algorithms based on Machine Learning can be devised on the basis of network stream. This work did not provide any solution for interface in translating queried result to natural language using NLP which is another area of research.

#### REFERENCES

- [1] S. Mann, J. Nolan, and B. Wellman, "Sousveillance : Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments," 2002.
- [2] S. Mann, "Surveillance (Oversight), Sousveillance (Undersight), and Metaveillance (Seeing Sight Itself)," in 2016 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2016, pp. 1408-1417.
- [3] S. O. Ajiboye, P. Birch, C. Chatwin, and R. Young, "Hierarchical video surveillance architecture: a chassis for video big data analytics and exploration," in SPIE/IS&T Electronic Imaging, 2015, p. 10.
- [4] D. Chahyati, M. I. Fanany, and A. M. Arymurthy, "Man woman detection in surveillance images," in 2017 5th International Conference on Information and Communication Technology (ICoICT), 2017, pp. 1-4.
- [5] R. M. Chory, L. E. Vela, and T. A. Avtgis, "Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses," *Employee Responsibilities and Rights Journal*, vol. 28, pp. 23-43, March 01 2016.
- [6] P. K. Mishra and G. P. Saroha, "A study on video surveillance system for object detection and tracking," in 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016, pp. 221-226.
- [7] M. M. Saemi, J. See, and S. Tan, "Lost and found: Identifying objects in long-term surveillance videos," in 2015 IEEE International Conference on Signal and Image Processing Applications (ICSIPA), 2015, pp. 99-104.
- [8] S. Sajjanar, S. K. Mankani, P. R. Dongrekar, N. S. Kumar, Mohana, and H. V. R. Aradhya, "Implementation of real time moving object detection and tracking on FPGA for video surveillance applications," in 2016 IEEE Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), 2016, pp. 289-295.
- [9] V. Tsakanikas and T. Dagiuklas, "Video surveillance systems-current status and future trends," *Computers & Electrical Engineering*, vol. 70, pp. 736-753, 2018/08/01/ 2018.
- [10] G. S. Walia and R. Kapoor, "Robust object tracking based upon adaptive multi-cue integration for video surveillance," *Multimedia Tools and Applications*, vol. 75, pp. 15821-15847, 2016/12/01 2016.
- [11] P. Doucek, A. Pavlicek, and L. Luc, "Internet of Things or Surveillance of Things?," in *Research and Practical Issues of Enterprise Information Systems*, Cham, 2018, pp. 45-55.
- [12] J. Duncan, "Uncertainty and Desire: Big Data Surveillance and Digital Citizenship," *The iJournal: Graduate Student Journal of the Faculty of Information*, vol. 3, 2018.
- [13] N. Fescioglu-Unver, S. H. Choi, D. Sheen, and S. Kumara, "RFID in production and service systems: Technology, applications and issues," *Information Systems Frontiers*, vol. 17, pp. 1369-1380, December 01 2015.
- [14] M. Fularz, M. Kraft, A. Schmidt, and J. Niechciał, "The PUT Surveillance Database," *Cham*, 2016, pp. 73-79.
- [15] J. S. Kulchandani and K. J. Dangarwala, "Moving object detection: Review of recent research trends," in 2015 International Conference on Pervasive Computing (ICPC), 2015, pp. 1-5.
- [16] S. Liu and S. D. Young, "A survey of social media data analysis for physical activity surveillance," *Journal of Forensic and Legal Medicine*, vol. 57, pp. 33-36, 2018/07/01/ 2018.
- [17] E. Ohn-Bar, A. Tawari, S. Martin, and M. M. Trivedi, "On surveillance for safety critical events: In-vehicle video networks for predictive driver assistance systems," *Computer Vision and Image Understanding*, vol. 134, pp. 130-140, 2015/05/01/ 2015.
- [18] S. Yang, H. Yang, J. Li, and J. Zhu, "An Effective Crowd Property Analysis System for Video Surveillance Application," in *Digital TV and Wireless Multimedia Communication*, Singapore, 2017, pp. 115-127.
- [19] S. Mann, R. Janzen, M. A. Ali, and K. Nickerson, "Declaration of veillance (Surveillance is Half-Truth)," in 2015 IEEE Games Entertainment Media Conference (GEM), 2015, pp. 1-2.