IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 31, 2021, accepted September 20, 2021, date of publication September 22, 2021, date of current version October 1, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3114447

Challenges and Solutions of Surveillance Systems in IoT-Enabled Smart Campus: A Survey

THEODOROS ANAGNOSTOPOULOS[1], PANOS KOSTAKOS[2], ARKADY ZASLAVSKY[3], (Senior Member, IEEE), IOANNA KANTZAVELOU[4], (Member, IEEE), NIKOS TSOTSOLAS[1], IOANNIS SALMON[1], JEREMY MORLEY[5], AND ROBERT HARLE[6]

[1]Department of Business Administration, University of West Attica, 12243 Aigaleo, Greece
[2]Center for Ubiquitous Computing, University of Oulu, 90570 Oulu, Finland
[3]School of Information Technology, Deakin University, Burwood, VIC 3125, Australia
[4]Department of Informatics and Computer Engineering, University of West Attica, 12243 Aigaleo, Greece
[5]Ordnance Survey, Southampton SO15 2AA, U.K.
[6]Department of Computer Science and Technology, University of Cambridge, Cambridge CB2 1TN, U.K.

Corresponding author: Theodoros Anagnostopoulos (theodoros.anagnostopoulos@uniwa.gr)

This work was supported in part by the Course of Advanced Quantitative Statistical Analyses, Master of Business Administration (MBA), Department of Business Administration, University of West Attica, Athens, Greece, in part by the Academy of Finland 6 Genesis Flagship under Grant 318927, and in part by the EU Horizon 2020 Projects CUTLER: Coastal Urban developmenT through the LEnses of Resiliency under Grant 770469 and IDUNN Cognitive Detection System for Cybersecure Operational Technologies under Grant 101021911.

ABSTRACT A Smart Campus is a miniature of a Smart City with a more demanding framework that enables learning, social interaction and creativity. To ensure a Smart Campus uninterruptible secure operation, a key requirement is that daily routines and activities are performed protected in an environment monitored unobtrusively by a robust surveillance system. The various components that compose such an environment, buildings, labs, public spaces, smart lighting, smart parking, or even smart traffic lights, require us to focus on surveillance systems, and recognize which detection activities to establish. In this paper, we perform a comparative assessment in the area of surveillance systems for Smart Campuses. A proposed taxonomy for IoT-enabled Smart Campus unfold five research dimensions: (1) physical infrastructure; (2) enabling technologies; (3) software analytics; (4) system security; and (5) research methodology. By applying this taxonomy and by adopting a weighted scoring model on the surveyed systems, we first present the state-of-the-art, and then we make a comparative assessment and classify the systems. We extract valuable conclusions and inferences from this classification, providing insights and directions towards required services offered by surveillance systems for Smart Campus.

INDEX TERMS Smart Campus, surveillance systems, IoT, software analytics, security, research methodology, weighted scoring model.

I. INTRODUCTION

Smart Cities, also known as Cities 2.0, are embodiments of urban living in the digital age [1]. In the coming years, suburban and rural citizens are expected to move towards urban areas, forming a vast concentration of population in the inner city. It is anticipated that emerging paradigms such as Industry 4.0 will support the new needs of cities [2]. A key component is the incorporation of the Internet of Things (IoT) paradigm as the backbone of society [3]. IoT-enabled services will produce a vast amount of data that can be used to support and optimize critical infrastructure and provide new insights and advances. However, the majority of these data will be sensitive and should be treated unobtrusively not to harm freedom and individual privacy. The challenge today is to understand how to build and deploy massively interconnected systems such that they are both effective and trustworthy.

An area where we might hope to learn something significant is in the application of surveillance mechanisms in Smart Campuses. A College or University campuses is

The associate editor coordinating the review of this manuscript and approving it for publication was Giacomo Verticale.

a scaled-down version of a city: they contain a somewhat closed community that is large enough to experience many of the technological, social and human issues at a city scale. However, to the best of our knowledge, there has not been a thorough and systematic survey on surveillance Smart Campus systems. The present article is motivated by the lack of research that seeks to characterize the state-of-the-art on Smart Campus surveillance.

Against this backdrop, the article surveys IoT-based surveillance systems in Smart Campuses, as these environments, although similar to Smart Cities, have some unique requirements that call for additional security and privacy measures. The present survey was carried out on 44 systems that were deployed for campus safety. We developed a taxonomy for these systems along with a scoring model for each one of them. The functionality of the surveyed systems was sized up against five dimensions: (1) physical infrastructure; (2) enabling technologies; (3) software analytics; (4) system security; and (5) research methodology. The set of weights provided in the taxonomy enable a robust comparative assessment and classification model of state-of-the-art systems. Furthermore, the proposed method facilitates the extraction of valuable conclusions and inferences and gives insights and directions towards required services offered by a surveillance system of a Smart Campus. Finally, the survey brings forth a set of research efforts for the development of future surveillance systems specific to Smart Campuses.

The contributions of this article are:

- Characterize the state-of-the-art on surveillance systems deployed at Smart Campuses.
- Define five unique dimensions (physical infrastructure, enabling technologies, software analytics, the system security, and the research methodology) used to analyze the selected systems.
- Propose a taxonomy process, based on the aforementioned five dimensions that incorporates a weighted scoring system used for the classification of the surveillance systems.
- Provide a comparative assessment and classification based on the proposed weighted scoring system, with valuable findings to be used for future surveillance systems specific to Smart Campuses.
- Discusses the derived results and the way these can be used to improve the development of future surveillance systems for Smart Campuses.

The rest of the paper is structured as follows. In Section II we specify the use of surveillance systems in Smart Campus and describe the proposed taxonomy along with the scoring model designed to classify the research efforts. In Section III we perform the survey of the selected systems. In Section IV we conduct comparative research. In Section V we perform classification focusing on the proposed research efforts for Smart Campus safety and reliability. Finally, Section VI concludes the paper and proposes future work.

II. SURVEILLANCE SYSTEMS

A. GEOSPATIAL IOT

Smart Campus monitoring is enhanced by the proliferation of sensors and actuators incorporated to support geospatial IoT awareness. Specifically, geospatial location prediction as well as time of arrival estimation is feasible due to stochastic processes based on IoT networks [4]. In such systems it is possible to apply a publish subscribe utility to assign sensors' activity to certain geospatial data sources of observed measurements used for surveillance purposes [5]. Edge computing approaches focus on data collection that collects only the meaningful data from IoT devices. Such localized data sources are used to support services based on geospatial constraints [6]. Disaster management services are supported by IoT data streams, which are geospatially annotated to assist big data analytics aiming to provide campus recovery [7]. Geospatial modelling is applied to support safe students' transportation within Smart Campus by exploiting geolocated sensors' infrastructure design to provide a secure IoT-enabled architecture [8].

A survey on geospatial IoT is examined, in [9], which exploits context-aware personalized location-based services to provide potential geospatial analytical methods and monitoring applications incorporated by Smart Campus physical infrastructure. An event driven architecture is proposed in [10] that enables asynchronous transactions through campus sensor network by exploiting spatiotemporal data sources for online analytical streaming processing. Geospatial analysis is feasible to visualize and monitor campus area based on data generated by wireless IoT sensors and actuators. Such a system is used to design and maintain a safe Smart Campus public area architecture [11]. Location awareness is supported by a system proposed in [12], which leverages geospatial IoT driven applications, for providing an integrated solution for campus monitoring. A software architecture is proposed in [13] that enables geospatial data sources analytical processing for providing Smart Campus integrated microservices exploited by students. Such geospatial IoT services are essential to enable efficient campus surveillance utilities.

B. SMART CAMPUS SURVEILLANCE

IoT technology facilitates the incorporation of sensors and actuators for efficient Smart Campus surveillance. In such an environment, students are monitored unobtrusively to retain privacy and human rights. Ethical and legal requirements dictate the need for students to be aware that they are being monitored to provide well-being in their working place. Monitoring of public spaces is a major deterrent against delinquent behavior, enabling a safer space for all [14], [15]. Furthermore, the motivation behind surveillance systems in IoT-enabled Smart Campus is to capture such behavior and to better understand the individual reasons and root causes. Inferences from the collected data, can then inform prevention, prediction, and early warning of delinquent behavior

before this happens, acting as a security shield to contemporary Smart Campus life.

In this paper, we survey a high number of systems in the Smart Campus surveillance domain to reveal their strengths and weaknesses. The aim is to set up the basis of classifying contemporary systems proposed in research efforts and patents according their utility in surveillance. However, before we are ready to provide an outcome of this survey, it is essential to compare systems based on certain research dimensions of the proposed taxonomy. To realize a comparative assessment, we proceed with the definition of a concrete taxonomy that exploits the available systems. This taxonomy will become the basis for mapping any Smart Campus surveillance system to allow comparisons with any other system found in the respective literature. Through the proposed taxonomy and the provided classification, readers and researchers will be able to identify any shortcomings in contemporary research and propose efficient methods to deal with new frameworks in the domain.

C. PROPOSED TAXONOMY

The current survey focuses on research approaches that incorporate surveillance systems in IoT-enabled Smart Campus. The adoption of surveillance systems is depicted in our taxonomy. We report on the proposed taxonomy before we survey the existing research efforts to give the necessary overview of the domain. Hence, it will be easily to determine the main characteristics of each system and their place in the related literature.

We define the Smart Campus context that aims to set up the rationale for classifying surveillance systems. The Smart Campus context incorporates hardware, tools, data, software, and research methods that a surveillance system adopts to become the basis for realizing a solution for a Smart Campus. In general, IoT-enabled Smart Campus Surveillance System context can be categorized in five main dimensions: (1) physical infrastructure; (2) enabling technologies; (3) software analytics; (4) system security; and (5) research methodology. These dimensions are discrete which means that the relevant context of each system belongs only to one of the aforementioned dimensions. Our taxonomy is structured in a dimensionally specific way (i.e. we give equal attention to each dimension) to cover a range of diverse components and features. Each contextual component and feature are assigned specific values denoting their role in the proposed taxonomy. Components are related to the tools and hardware adopted in each category, while features are related to the contextual information (e.g. data) adopted in each dimension and system.

First, the Physical Infrastructure involves the following components: (1) sustainable Smart Campus, (2) smart transport, and (3) autonomous vehicles. Sustainable campus can be further categorized according to the type of infrastructure to: (1) smart buildings, (2) smart classes, (3) smart labs, (4) public spaces, (5) smart parking, and (6) smart lighting. Smart transport can be divided to (1) smart traffic lights, and (2) electric vehicles. Autonomous vehicles can be characterized to: (1) Unmanned Aerial Vehicles (UAV), and (2) Connected and Autonomous Vehicles (CAV). Fig. 1 visualizes the conceptual map of the physical infrastructure dimension.

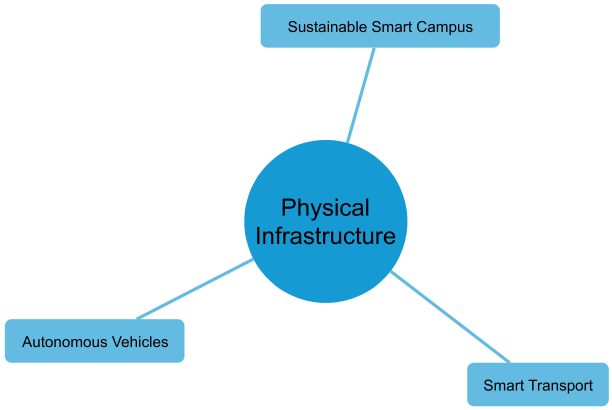

FIGURE 1. Conceptual map of physical infrastructure dimension.

The second dimension entails the Enabling Technologies of the IoT-enabled Smart Campus surveillance ecosystem, consisting of the following components: (1) core IoT technology, (2) passive monitoring technology, and (3) active monitoring devices. Core IoT technology can be further decomposed according to the type of computation to: (1) IoT platform, (2) Raspberry Pi, (3) Arduino Uno, (4) Wireless Sensor Network (WSN), (5) sensors, and (6) actuators. Respectively, passive monitoring technology can be categorized to: (1) Radio Frequency IDentifier (RFID) equipment, (2) Global Positioning System (GPS) device, (3) Ethernet protocol, (4) Wi-Fi, (5) Bluetooth, (6) ZigBee, (7) Near Field Communication (NFC), (8) 4G, (9) 5G, and (10) Low Power Wide Area Networks (LPWAN), which contain technologies such as SigFox, LoRa, LTE-M or NB-IoT, [16]–[23]. Active monitoring devices are divided to: (1) cameras, (2) microphones, (3) smartphones, (4) smart watches, and (5) Autonomous Teller Machines (ATM). A conceptual map of the enabling technologies dimension is visualized in Fig. 2.

The third dimension of the proposed taxonomy, software analytics, incorporates a surveillance system design component that is further categorized according to its location coverage to: (1) ad hoc i.e., static, (2) mobile i.e., dynamic, and (3) mesh, i.e., mixed location coverage. In addition, the features of this dimension spread out to: (1) computing methodology, (2) affective computing, (3) user context, (4) software architecture, (5) inference system, (6) inference algorithms, (7) eXtended Reality (XR), and (8) application. Computing methodology focuses on the computing paradigm of: (1) edge computing, (2) cloud computing. Affective computing is decomposed according to the recognition of human affections into: (1) voice recognition, (2) face recognition, and (3) gesture recognition. User context is divided into: (1) social, (2) movement, (3) crowdsourcing, (4) crowd

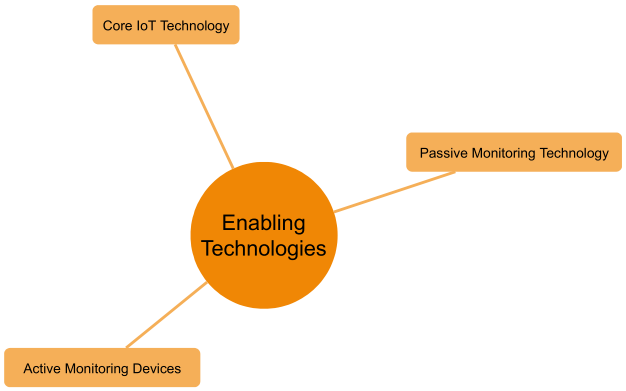

FIGURE 2. Conceptual map of enabling technologies dimension.

sensing, and (5) Ambient Intelligence (AmI). Furthermore, corresponding to the provided service, software architecture is characterized by: (1) big data, and (2) service-oriented. The inference system feature is divided according to conceptual focus and is build up by: (1) context aware and (2) decision support. Inference algorithms based on machine learning and artificial intelligence approaches are categorized into: (1) supervised, (2) unsupervised, and (3) semi supervised. XR according to type is separated into: (1) Virtual Reality (VR), and (2) Augmented Reality (AR). Finally, the application feature branch off according to execution location type as follows: (1) desktop i.e., static location, and (2) mobile i.e., dynamic location. Fig. 3 visualizes the conceptual map of software analytics dimension.

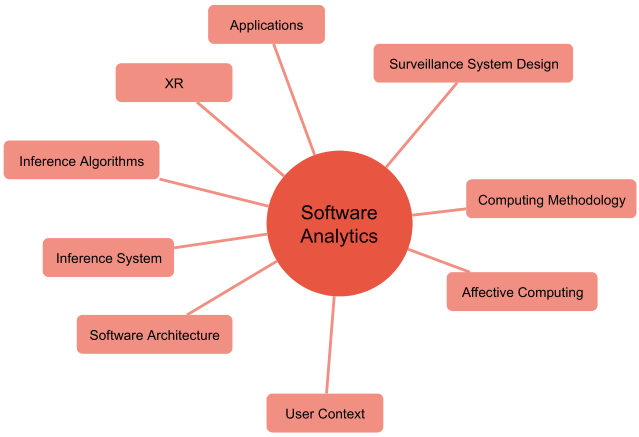

FIGURE 3. Conceptual map of software analytics dimension.

System security involves cybersecurity system component as well as specific features. Such features are: (1) regulations, (2) attacks, and (3) security mechanisms. The cybersecurity system component is further decomposed into the following domains according to the safety level: (1) authentication system, and (2) intrusion detection system. With regards to legal requirements, the system security regulation feature builds up to: (1) security standards, and (2) privacy compliance. Attacks are divided according to their type into: (1) cryptanalysis, (2) Denial of Service (DoS), (3) eavesdropping, (4) hacking, (5) spoofing, (6) sniffing, (7) Man in the Middle Attack (MTM), (8) jamming, (9) data leakage, (10) password capture, and (11) virus infection. Security mechanisms can be further grouped into: (1) anonymization, (2) steganography, (3) data encryption, (4) biometrics, (5) network monitoring, (6) firewall, (7) password, and (8) anti-virus system [24]–[31]. A conceptual map of the system security dimension is visualized in Fig. 4.

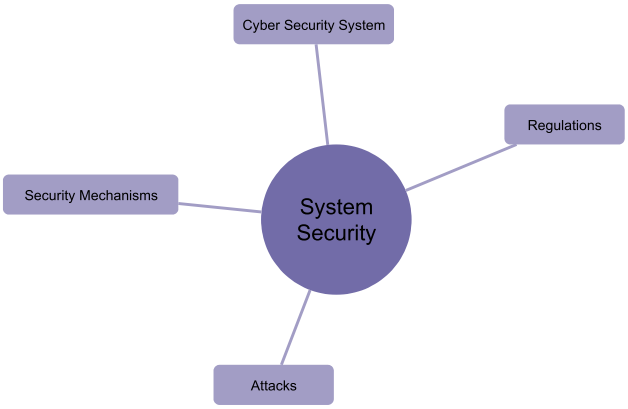

FIGURE 4. Conceptual map of system security dimension.

The last dimension of IoT-enabled Smart Campus Surveillance System context, i.e., research methodology, focuses on the following two features: (1) research context, and (2) data context. Research context regarding the time required to conduct research and the type of the research, is further categorized to: (1) acquisition time, (2) quantitative, (3) qualitative, and (4) mixed. Data context according to type is decomposed to: (1) real, (2) synthetic, (3) streaming, (4) batch, (5) text, (6) sound, (7) image, and (8) video. A conceptual map of the research methodology dimension is visualized in Fig. 5.

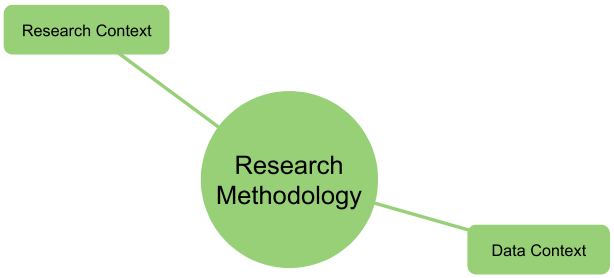

FIGURE 5. Conceptual map of research methodology dimension.

Fig. 6 visualizes the proposed taxonomy in a concise conceptual tree map. Specifically, the map is constructed by using the relative frequencies of the taxonomy components and features as encountered during processing certain research efforts. Concretely, the surveillance system category appears more frequently than the category of software analytics, thus it appears with larger font size. Subsequently, data context category appears less frequently than that of software analytics, thus it is represented by smaller font size.

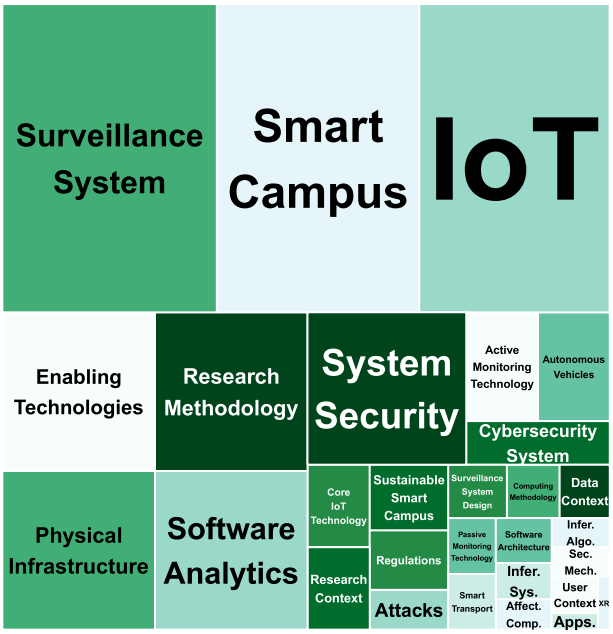

FIGURE 6. Conceptual tree map of the proposed taxonomy.

The final visualization is a relative frequencies-based mosaic of different font size categories of certain taxonomy items and presented as a conceptual tree map.

Fig. 7 presents an overview of the above-discussed components and features in a marked up conceptual tree graph. Specifically, components and features of the proposed taxonomy are divided into five categories (dimensions), forming a high-level description of the core concepts placed on the left side of the figure. In the intermediate levels, the emerged research component categories are presented in hierarchical order, according to the taxonomy's significance. The conceptual tree graph is completed by assigning certain features to certain categories as presented in the right side of the figure. Note that certain features are assigned to certain component categories, which means that the taxonomy is sound, and thus, does not contain cross-reference misleading information.

D. ADOPTED WEIGHTED SCORING MODEL

To provide a quantitative characterization of the reviewed surveillance research in IoT-enabled Smart Campus, we adopted a weighted scoring model that evaluates the value of the research and classifies them in a descending order i.e., by using three classes, namely: ''High Adequacy'', ''Medium Adequacy'', and ''Low Adequacy''. The taxonomy we have proposed in the previous section allows us to use as a performance measure the relative frequencies of the appearance of the instances (nominal scale values) of systems' components and features in the different research efforts. These instances are evaluated through an additive value function that incorporates a normalized weight value that is based on the importance order provided by the experts for each value of the nominal scale and its corresponding appearance frequency.

For the estimation of an overall evaluation of each research effort a weighted scoring model is applied. As the proposed taxonomy indicates, the evaluation criteria are categorized in a structural way using a two-level categorization, namely dimensions and categories. The multilevel scoring model takes into consideration this tree-structure of the criteria and incorporates preference information from a group of experts for assigning weights at the dimensions and categories of these criteria. The categories according to the taxonomy correspond to components and features of the efforts under discussion.

A compensatory criteria weight elicitation model, e.g. a trade-off approach [32] could be used. However, this would lead to an intensely time-consuming process given the number of the criteria and their categories and sub-categories, so a non-compensatory approach will be adopted.

Existing non-compensatory methods which are widely used to assess the criteria for the importance of weights are classified into two categories: (i) direct assessment procedures, where the decision maker or a field expert is asked to explicitly express the criteria weights in terms of percentages or determine how important a criterion is, e.g. on an absolute scale from 1 (no important at all) to 10 (very important), or on an ordinal scale, and (ii) indirect methods, inferring the weights from pairwise comparisons of the criteria or reference alternatives [33]. In the second category, the methods include among others: (a) the method of cards proposed in [34], [35], (b) the method of centralized weights [36] that requests from the decision maker a number of ordinal comparisons of criteria that are formulated as linear inequalities, in order to obtain the centroid of the vertices of a polyhedron, and (c) WAP method [37] based on cards method but it includes enriched preferential information towards more robust weight vectors.

In our case and after taking into consideration the size of our classification problem and available effort from the experts, we have decided to adopt a direct assessment procedure for the assignment of weights at all levels of the structured evaluation criteria. We assign normalized weights, i.e., sum up to 1, on the dimensions and the categories (i.e., components and features).

A category can be either a component or a feature category containing either components or features, respectively. A mixture of components and features is allowed in the same dimension.

At the first level, namely the dimensions, the experts are asked to explicitly express the weights in terms of percentages. These weights shall be normalized by making their sum equal to 1. Dimensions are conceptually regarded as equally weighted, since each dimension emerges a unique niche per surveillance system of the proposed taxonomy. Let us define w_d, as the normalized dimension weight, then for the 5 adopted dimensions it holds that:

$$\sum_{d=1}^{5} w_d = 1 \tag{1}$$

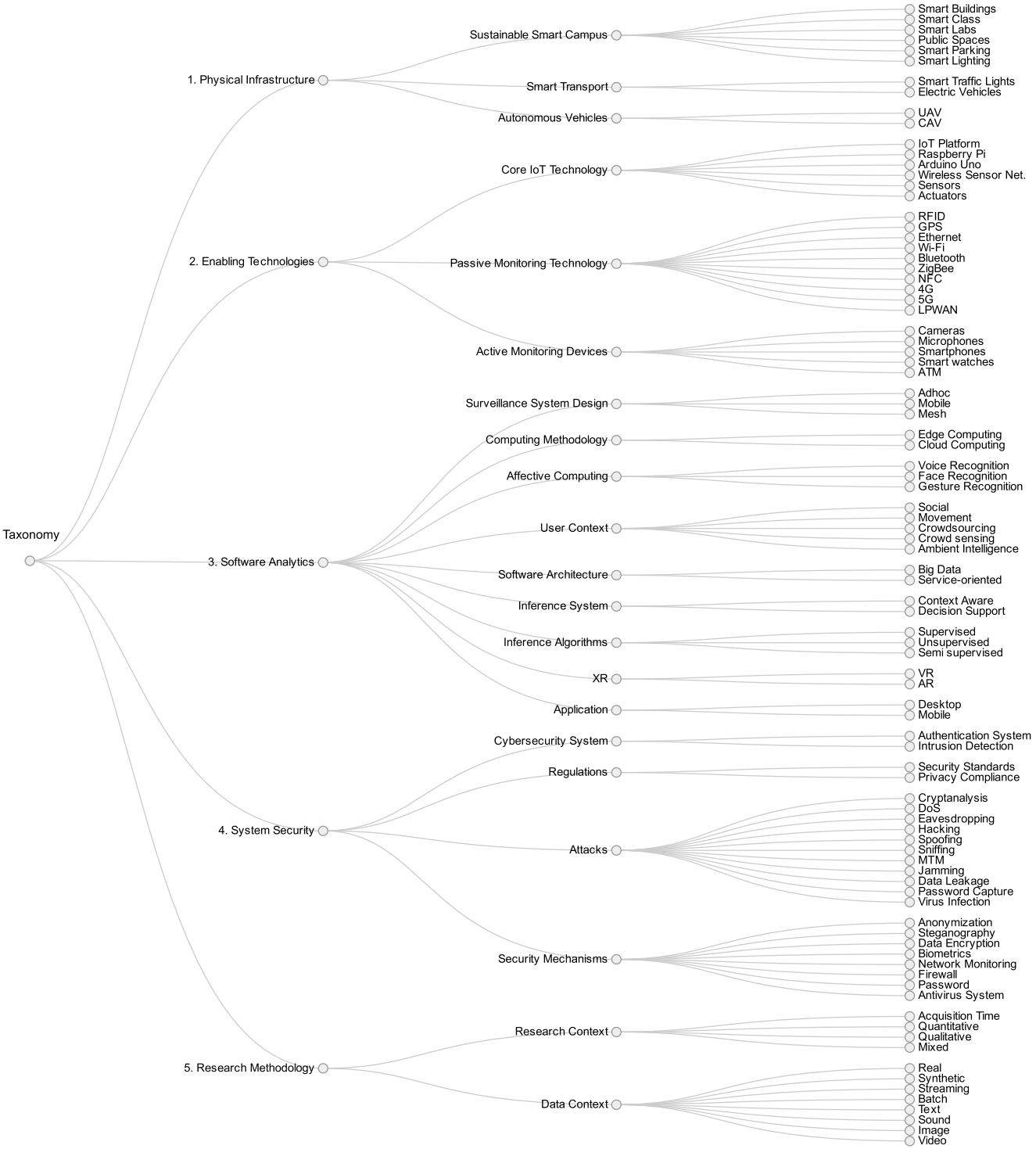

FIGURE 7. **Overview tree graph of the proposed taxonomy.**

For the next level, namely categories, the determination of the corresponding weights is implemented by asking the experts to rank the categories for the least important to the most important. No ties are allowed. Let r be the ranking of category ca in a dimension d. After ranking the categories based on their significance within each dimension the analyst calculates the relative importance of each category as follows:

$$w_{ca}(r) = \frac{|R_d| + 1 - r}{\sum_{i=1}^{|R_d|} i} \tag{2}$$

where $w_{ca}(r)$, is the normalized category weight at rank r and $|R_d|$ is the cardinality of the specific ranking R_d of a dimension d.

For the evaluation of the research efforts we need to calculate the value of each instance in the defined categories. In each category a specific ordinal scale is used. In order to estimate a value that will incorporate the appearance frequencies as well, we built an additive value function, assuming that it has a linear form. We asked the experts to rank the values of each ordinal scale from the best to the worse and we assigned numeric values $v_{ca}(r)$ to each position r (1^{st} =1, 2^{nd} =2, etc.) of a ranking R per category ca as follows:

$$v_{ca}(r) = \frac{|R_{ca}| + 1 - r}{|R_{ca}|} \tag{3}$$

where $|R_{ca}|$ is the cardinality of the specific ranking R_{ca} of a category ca. $v_{ca}(r)$ is the normalized value (e.g. max value is 1) of each ranking position r.

In order to incorporate the appearance frequencies of each value of a category we need to calculate the relative frequencies of its appearance in the research efforts. The meaning of relative frequencies is to count and then normalize the frequency of a specific value to occur in a certain category. Let us define f_v, as the normalized relative frequency value, then for the total number of the g_{ca} values of a certain category it holds that:

$$\sum_{v=1}^{g_{ca}} f_v = 1 \tag{4}$$

So, the value of a specific research effort i concerning specific nominal values $v_{ca}(r)$ in a category ca is calculated as follows:

$$v_{ca}(i) = \sum_{r=1}^{|R_{ca}|} v_{ca}(r, i) \cdot f_v(r, i) \tag{5}$$

where $f_v(r, i)$ is the relative frequency assignment for the ranking position r of the instance of i and $v_{ca}(r, i)$ is the normalized value for the ranking position r of the instance of i in a certain category.

When all the taxonomy data has assigned with certain relative frequency values, we feed them to the weighted scoring model to receive the overall evaluation of each research effort i. Let us define $v(i)$, as the overall value of each research effort i. Then for the overall evaluation of each research effort it holds that:

$$v(i) = \sum_{d=1}^{5} w_d \sum_{ca=1}^{e_d} w_{ca} \cdot v_{ca}(i) \tag{6}$$

The necessary classification will be performed through the comparison of the overall values of the research efforts to some value thresholds that define the lower bound of each class, as follows:

$$\begin{cases} v(i) \geq v_H \Rightarrow i \epsilon C_H \\ v_H > v(i) \geq v_M \Rightarrow i \epsilon C_M \\ v_M > v(i) \Rightarrow i \epsilon C_L \end{cases} \tag{7}$$

where $v_H > v_M$ are thresholds defined by the experts in the global value scale [0, 1], after the calculation of the values of all research efforts, to discriminate the groups. v_H is lower bound of group C_H (research efforts with High Adequacy) and v_M is the lower bound of group C_M (research efforts with Medium Adequacy). The selection of the thresholds is related to the specific values that have been calculated for the 44 research efforts in order to assign 10 efforts under the category "High Adequacy", and 10 more under the category "Low Adequacy". The remaining research efforts will lay in the category "Medium Adequacy".

Research efforts i, with a value v_i greater than v_H, are regarded as the best efforts and are the proposed solutions of the survey.

Fig. 8 shows the flow diagram of the classification algorithm that is proposed by the authors in this section that is based on direct assessment procedures for expressing the importance of the various levels of the taxonomy elements.

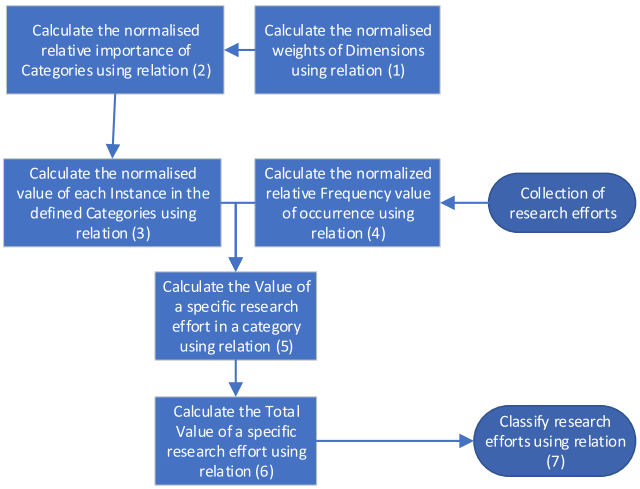

FIGURE 8. Work flow diagram of the proposed scoring model.

III. SURVEY

The research efforts we survey, corresponding to the proposed taxonomy above, are compared and their strengths and weaknesses are clearly stated. These research efforts cover more than ten years of research in the area of IoT-enabled Smart Campus surveillance systems. We survey 42 papers and 2 patents, covering all the dimensions of the proposed taxonomy. The distribution of research outputs by year of publication is presented in Fig. 9. Specifically, from year 2008 to 2012 the annual research yield is rather sparse. Instead, in years 2016 to 2020 we observe a more systematic research approach in the published literature, indicating the maturity of the research community towards surveillance systems for Smart Campus, from an IoT perspective. Based on the survey results, we perform a classification and comparative assessment of the reviewed systems.

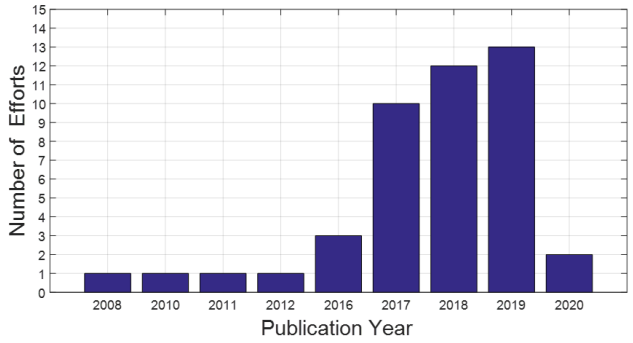

FIGURE 9. Surveyed research efforts per year of publication.

A. SURVEY OF SYSTEMS

Researchers in [38] propose a system that develops a Smart Campus where every place in the campus is connected to a central Wi-Fi control unit. This was achieved by incorporating IoT technology to provide automation, security and surveillance services to students and the university personnel. The system focuses on smart buildings and smart lighting surveillance, while it incorporates electric vehicles infrastructure. It also uses IoT platform, Arduino Uno, WSN, sensors and actuators core enabling technologies. To provide passive monitoring services it incorporates RFID, GPS, Ethernet, Wi-Fi, Bluetooth and ZigBee technology. In addition, active monitoring is achieved with cameras and smartphones. Quality of Service (QoS) is assured with an ad hoc surveillance system, enabling context awareness through supervised inference algorithms. An intrusion detection system is incorporated which complies with security standards. The system handles MTM and password capture attacks through extensive network monitoring, firewall setup and password security mechanisms. Authors worked with mixed research methodology, while data used are real-life and streaming. Data types used for the experiments were text and video.

Experiments of this approach are performed in the area of smart buildings, smart lighting and electric vehicles surveillance within Smart Campus with real equipment of Arduino sensors and RFID technology. Results are promising and tend to be incorporated my more areas within Smart Campus. However, there do exist scalability issues in testing the approach to the wide area of the campus due to upcoming complexity to required components. Overall, it is an interesting use case where real equipment is used to test the robustness of smart buildings surveillance consistency; however, new areas should be examined to extend the current test bed.

In [39], a system that enables Smart Campus safety based on RFID technology is presented. The system uses Tabu search to find the optimal places in the campus to deploy the RFID readers to provide students' surveillance services. The research mainly focuses on smart class and public places surveillance, while core technology includes an IoT platform, WSN and sensors infrastructure. Passive monitoring is achieved with RFID and GPS sensors, while students' smartphones are used for active monitoring. A mobile surveillance system is designed, based on cloud computing, while inference is based on supervised algorithms running on mobile smartphone applications. The research incorporates an intrusion detection system compliant with security standards. The system handles DoS and hacking attacks with the incorporation of biometric security mechanisms. A quantitative research method is used and it is stated the acquisition time of the research to completion. Text data is produced and streamed from the smartphones.

Real-life experiments are performed within the campus by incorporating RFID technology to exploit smart class and public spaces surveillance systems. Proposed system is able to sense students entering dangerous areas in Smart Campus as well as to distinguish campus visitors apart from student population. Large numbers of RFID tags make system hard to managed efficiently, which is obviously a limitation. Overall, the system is well designed and proved to be able to protect users' personal safety within the campus, however a more detailed design should be done to provide a less complex RFID tag infrastructure.

Authors in [40] introduce a system that uses Arduino Uno and wireless technology to provide necessary Smart Campus security and surveillance. The proposed system is focusing mainly on public spaces and smart lighting areas of the university campus. It incorporates an IoT platform to process available Arduino Uno, WSN and sensors' data produced in the campus. Smartphone GPS sensor is used as passive monitoring technology and cameras are used to capture images of the surveillance area. The surveillance system is established on a mesh infrastructure based on both ad hoc and mobile nodes that enables gesture recognition of the suspicious subjects. User movement context inputs supervised inference algorithms to enable surveillance services running on mobile smartphone applications. The system incorporates both an authentication and an intrusion detection system complied with certain security standards. Such security systems can treat hacking attacks by using password security mechanisms. A quantitative methodology is used to evaluate real streaming image data produced by smartphone cameras.

The system is tested with real data in laboratory setup exploiting Arduino sensors technology. Results emerged the need of a light infrastructure for applied Smart Campus surveillance systems. Experiments, however, mainly focused on image capturing and video analyses. Extending potentiality of the system is its ability to detect users' behavior activity and perform face recognition. Overall, it is a solid approach, however at the current stage it needs further experiments to exploit its potentiality.

Researchers in [41] propose a system that analyses human behavioral data to provide surveillance services to students during their daily life on the Smart Campus. Analyzed data is also evaluated by system administrators to provide certain positive social impact to the university. The system is mainly applied for smart buildings as well as smart labs and public spaces surveillance areas. Core IoT enabling technologies used by the system include sensor devices, as well

as GPS and Wi-Fi passive monitoring techniques. Active surveillance monitoring is achieved with the proliferation of cameras and smartphones as part of an ad hoc integrated system. The system incorporates social, movement and crowdsourcing user context to provide surveillance services. Supervised inference algorithms run in mobile applications to output a decision support system for QoS surveillance. Authentication mechanisms and intrusion detection systems enhance the effectiveness of the proposed research, consistent with current security and privacy regulations. The system can handle sniffing attacks by using network monitoring, firewall and antivirus system countermeasures. Acquisition time of the mixed research methodology is provided, and data used are mainly batch and synthetic videos.

This approach uses synthetic data to perform certain experiments. Results are promising in defining the context of surveillance life-style report system based on students' data from the campus. However, the fact that the data used for analyses are synthetic is a limitation of the current system in case it is considered to be deployed on a real-life experimental setup. It is a well-formed approach with safe and sound research methodology, however in its current form it lacks the real ground truth setup that would be used for further evaluation.

In [42], a system is introduced that uses IoT technology and devices to provide a sustainable Smart Campus surveillance environment. Specifically, the system focuses on smart labs and public spaces, as well as with smart parking and smart lighting surveillance areas. Core enabling technology covers IoT platform, Raspberry Pi, Arduino Uno, sensors and actuators devices. Passive monitoring is feasible due to the incorporation of RFID sensors as well as Bluetooth, ZigBee, and NFC network communication protocols. Cameras and microphones are used as active monitoring devices for efficient campus surveillance. The proposed surveillance system has an ad hoc design and incorporates cloud technology to achieve face and gesture recognition. User movement context was sent to unsupervised inference algorithms, enhancing the functionalities of mobile surveillance applications. Research exploits the potentiality of incorporating an intrusion detection system, which covers certain security standards. The system can handle sniffing and password capture attacks with a variety of data encryption and firewall security mechanisms. Acquisition time of the adopted quantitative research is defined, while data used are real and streaming. Sound, image and video data are all incorporated.

Although the study proposed a compact initial system, for experimentation in the final stage the researchers used a subset containing mainly the Arduino processor and the connected sensors. The results in this limited edition of the proposed system were positive; however, the limitation of not having more components deteriorates the integration of such system in real scenarios. Overall, the rationale behind the experimental setup is interesting, but the experiments should be repeated with a superset of the current experimental setup.

While the past studies provided some interesting findings, further research in surveillance systems is required. Specifically, in [38], new areas should be examined, extending the current test bed into smart traffic control and integrated smart surveillance systems architecture. Since large numbers of RFID tags make the system hard to manage efficiently a more detailed design should be done to provide a less complex tag infrastructure [39]. The solution developed in [40], could be extended to include current surveillance system that detect students' behavior activity and face recognition captured from multiple data sources within the Smart Campus. Experimentation, in [41], with real datasets would lead to more robust results that could be further used by prospective researchers. Future research in [42] should be focused on resolve interoperability of integrated devices with heterogeneous functionalities towards a smart environment.

1) SYSTEMS THAT FOCUS ON PUBLIC SPACES AND SMART PARKING

In [43] and [44] researchers adopt surveillance systems that focus on public spaces and smart parking. Specifically, in [43] the authors propose a computational cognitive modeling approach to understand and design a mobile crowdsourcing system for improving campus safety and reporting. The system uses an IoT platform to process data produced by the incorporated sensors located in the Smart Campus. Sensor communication is achieved by Wi-Fi passive monitoring technology and the system also exploits data captured by cameras and user smartphones. The designed surveillance system is mainly mobile, exploiting cloud computing utilities to process social, movement and crowdsourcing user context. A big data architecture is used to input data to a DSS for inferring an incident based on a supervised algorithm that runs on mobile devices. The system incorporates both authentication mechanisms and intrusion detection techniques for system security, which are standards compliant. Spoofing attacks are faced with the adoption of specific password security mechanisms. Acquisition time of the quantitative research methodology is defined, while the data used are real and batch. Data types processed by the system include text and video.

Laboratory experiments were performed exploiting MTurk environment. Results enhanced the understanding of different human factors that may have an effect in students' commitment to share safety reports. The study applied on a Smart Campus with certain student population. Experiments were based on hypothetical scenarios where the responses were self-reported and thus may be biased. Overall current research is well designed and evaluated, however, incorporating experiments could optimize it based on real life scenarios.

In [44], the authors present a system that introduces a security responder framework to reinforce Smart Campus safety and reduce surveillance costs. The system also adopts UAV infrastructure. An IoT platform, Raspberry Pi, WSN and sensors are used as core technology to enable the proposed surveillance system. The system uses 4G for data

communication and RFID and GPS sensor are also incorporated. Active monitoring is supported with the exploitation of cameras, microphones and smartphones, forming a mesh surveillance system design. Cloud computing is used to process social and user movement context to provide context awareness. Inference algorithms are used to include supervised and unsupervised techniques and the system incorporates mobile applications. Authentication and intrusion detection systems, which comply with privacy regulations, are used to face virus infection attacks. Network monitoring is the basis of the security mechanism to face malicious threats from the surrounding environment. Acquisition time of the quantitative research methodology is defined, and data used are real and streaming. The data types processed by the system include text, sound, images and videos.

The research is based in laboratory experiments. Results indicate that finalizing the implementation of the proposed system may improve its capability to achieve an optimum performance. However, applying a vast number of sensors in the Smart Campus is possible to make the configuration of the technical parts a challenging issue. In addition, limited financial resources of universities will be a trade off in applying such a complex system. The architecture is well defined; however, it does not explain how it will face possible forceful opposition from students on the Smart Campus regarding the invasion of their privacy.

Although significant work has been done there is a need for further research in the area of surveillance systems that focus on public spaces and smart parking. Future research, in [43], will focus on a more diverse set of participants expanding the narrow area of the Smart Campus to experimentation in the wide area of a Smart City. Refined information provided by the proposed system, in [44], would lead to an early prediction of crimes and future prevention.

2) SYSTEMS THAT FOCUS ON SMART BUILDINGS, SMART LABS, PUBLIC SPACES AND SMART LIGHTING

Authors in [45] and [46] introduce Smart Campus surveillance systems which focus on smart buildings, smart labs, public spaces and smart lighting. Specifically, in [45] researchers propose a smart system based on a smart card biometrics approach that can be integrated to a university campus providing contemporary surveillance services. It incorporates an electric vehicles physical infrastructure. The system uses a wide range of enabling technologies including IoT platform, Raspberry Pi, Arduino Uno board, WSN, sensors and actuators located in several places in the campus. Passive monitoring is achieved with the incorporating RFID sensors as well as Ethernet, Wi-Fi, ZigBee and NFC communication protocols. The surveillance system is ad hoc based mainly on cameras technology. Cloud computing processes exploit social context to provide surveillance QoS, and it incorporates desktop and mobile applications. Security is based on authentication mechanisms and intrusion detection systems, which comply with privacy regulations. Sniffing attacks are handled with the adoption of network monitoring security mechanism. The research method used in this effort is quantitative and data used are real and streaming text.

At the current development phase experiments have been performed in a limited area of the implemented services. Results have been observed for the fields of environmental analysis, smart lighting, automation and proposed security system. Lack of implemented services to perform further experiments is a limitation of the effort. Overall, it is a promising research work, which evaluates the proposed system, however more experiments should be done to effectively assess the observed results.

In [46], researchers introduce a conceptual surveillance modeling of Smart Campus as a system, composed by certain smartness levels of the campus sustainable components. The system is based on IoT platform, WSN, sensors and actuators, and it incorporates RFID and Wi-Fi passive monitoring technology. Active monitoring is achieved through cameras, microphones, and smartphones that form an ad hoc surveillance system. Cloud computing processing is used to provide voice and face recognition. Big data architecture is incorporated to feed the supervised algorithms with data to infer an incident. The system also has VR and AR capabilities while it is built on mobile applications. Both an authentication mechanism and an intrusion detection system are used to protect the Smart Campus, according to certain security standards. In addition, anonymization, biometrics, and network monitoring security mechanisms are used. Conducted quantitative research methodology has defined acquisition time of completion. Data used are real and batch, and data types are sound, image and video.

Experimental setup of this effort is towards conducting conceptual modeling and system description of surveillance systems. Results prove the need of surveillance in the concept of Smart Campus though analytical experiments based on student population. The limitation of this effort, at the current phase, is the lack of integration of such system in real environment. It is a solid research based on real data sources, however more work should be done towards the adoption of such system in actual campus' surveillance system.

Systems of this category can undertake more future research work. Specifically, in [45], authors can extend their effort towards an integration of electric vehicle charging stations and smart structural health systems exploiting data generated form campus sensors nodes. Multiple components to support the proposed system, in [46], is required aiming to maintain distinctive surveillance features as well as dealing with software applications heterogeneity.

3) SYSTEMS THAT FOCUS ON PUBLIC SPACES AND SMART TRAFFIC LIGHTS

In [47], [48], and [49], researchers adopt surveillance systems that focus on public spaces and smart traffic lights physical infrastructure. Specifically, in [47], the authors present a system that analyzes the implementation of certain security mechanisms to provide a sustainable Smart Campus ecosystem. Such system is composed of an IoT platform, which

processes data produced by WSN and sensors located in the campus public spaces. Passive monitoring technology incorporates RFID and GPS sensors, while active monitoring is achieved through installed cameras, and all together form an ad hoc surveillance system. Big data architecture is running on the cloud, it is defined a DSS, and it is based on supervised and unsupervised inference algorithms running on desktop applications. Authentication mechanisms and intrusion detection systems provide security and privacy to users. The system faces DoS, data leakage and passwords capture attacks with the proliferation of anonymization, data encryption and biometrics prevention mechanisms. The adopted methodology is mixed including quantitative and qualitative analysis performed on a given research acquisition time period. Real and streaming text data are used for experimentation.

Research is performed by laboratory experiments based on real data. Results assess the quality of sensors along with the use of fiber optic sensors to replace electronic sensors. The system also enhances privacy protection technology for wireless sensor networks. In addition, more work should be conducted for providing a viable solution for the transport and application layers security problem, respectively. Overall, real data used to evaluate the system, however, more experiments should be performed to provide a robust outcome of the research effort.

The authors of [48] present a system that illustrates an ontology for IoT-enabled Smart Campus architecture. The system also introduces a continuous data processing unit, which is used for online reporting. Proposed system incorporates WSN, sensors, and GPS as key enabling technology. Surveillance system is ad hoc and it is based on cameras located in public spaces of the campus. The system focuses mainly on decision support process, incorporating VR supervised algorithms, running on desktop applications. Security standards are followed and authentication mechanisms as well as an intrusion detection system are both incorporated to provide certain levels of security to users. Virus infection attacks are prevented with the adoption of an antivirus system. The research methodology is based on quantitative approach. Data used for experimentation are real and synthetic text data.

Experiments are based on certain future plan exploiting various interests and skills. Results evaluate the proposed ontology presented with graphical diagram and mathematical analyses. Proposed research work has limited functionality and theoretical approach, which is not yet implemented. In addition, it has a plenty of dimensionality in design part for deeper presentation as well as implementation level. Overall, it is a solid effort, but more implementation required presenting its potentiality especially in the area of adoption and analyses of psychological and learning user attributes.

In [49], researchers introduce a system which is based on participatory sensing using smartphones to collect and process local student data to monitor the Smart Campus. The system is also able to infer students' activities during daily schedule by identifying user trends and stochastic behavioral patterns captured by sensors located in the campus. Specifically, GPS sensors as well as 4G and 5G technologies are used for passive monitoring. Smartphones and smart watches are incorporated to perform active campus monitoring. The proposed system is mobile and uses cloud computing capabilities to evaluate social and movement user context. A big data architecture is used to feed data into supervised and unsupervised inference algorithms running on mobile applications. An intrusion detection system protects the system by monitoring all its activity as a second line defense, while password capture attacks are confronted with the incorporation of data encryption and network monitoring security mechanisms. Acquisition time period of the research is defined, and the research methodology followed is quantitative. Furthermore, real and streaming text data are used for the experimentation of the system.

The proposed effort performs experiments based on real data of the system that exploit the research area of participatory sensing to improve services provided on the campus. Current results focus on the extraction of system features from fixed length time windows which feed a classifier to perform user activity recognition. More features should be incorporated to the classification schema to observe higher values of system effectiveness. Overall, the proposed system is efficient exploiting current implementation in terms of accuracy, precision and recall metrics.

Future work is vital to expand the findings observed during these research works. Specifically, in [47], more work should contain research that focuses on strengthening network security as well as protection of personal privacy in the sensing layer. Research, in [48], should incorporate experiments with power and saving mode which could be considered for defining adopted devices sustainability. In the future, in [49], a mechanism for sharing local data by users should be tuned, especially in cases where there are users who intentionally send corrupted data to deteriorate QoS. In such cases, reputation management techniques should be adopted.

4) SYSTEMS THAT FOCUS ON SMART BUILDINGS AND SMART CLASSES

Authors in [50], [51], and [52] introduce Smart Campus surveillance systems that focus on smart buildings, and smart classes. Specifically, in [50], researchers propose a system that uses the Open Authorization (OAuth) protocol to allow secure authorization from third party applications to access online surveillance services. The proposed system uses an IoT platform and sensors technology, as well as RFID and GPS to provide online services. It also incorporates cameras to achieve active monitoring of the university campus. In addition, the surveillance system is based on a mesh architecture using cloud computing capabilities to evaluate social context. The system incorporates both desktop and mobile applications. Regarding the security dimension, an intrusion detection system, which complies with security regulations, is established. The system can handle password capture

and virus infection attacks with the adoption of a password authentication mechanism and an antivirus system. Mixed research methodology is used combining quantitative and qualitative methods. Data used are real and streaming, and the data types incorporated in the study are text and video.

Proposed research conducts security experiments and theoretical analyses on laboratory real data. The system is running stably and credibly as well as it is flexible and easy to integrate with the existing Smart Campus service. In addition, unified management of user information should be treated with regards to certain ad hoc experimental policy. Overall, the current research effort provides a secure and reliable framework for third party applications considering certain strengths and limitations.

In [51], authors present a system that incorporates RFID technology to build a Smart Campus. A prototype of this system is introduced that takes into consideration maintenance services of electrical equipment as well as smart security locks of the university classes. The proposed system integrates smart traffic lights infrastructure. It uses RFID sensors and cameras, which communicate through Wi-Fi, Bluetooth, and ZigBee wireless protocols, to provide surveillance QoS. The adopted system is ad hoc and analyzes user movement context in the area of the campus while it is running on desktop applications. An authentication security system is incorporated, which confronts with security regulations. Cryptanalysis attacks are prevented by the system with the adoption of data encryption security mechanisms. The research method used for the completion of the effort is quantitative. The data used are real and streaming text sources.

Current research effort encompasses a well-designed laboratory experimental setup which is based on real data from RFID tags. Results prove that object tracking time and consumption on energy is decreased when credibility of attendance record and security of rooms are increased. A limitation of the current work is that most of features provided by the system could not be quantified after longer operational use. Overall, in the adopted effort certain experiments estimate the average electrical power consumed in a room with high efficiency, however more experiments required to scale up the system coverage area.

Researchers, in [52], propose a system that uses an encryption approach to provide advanced protection of students' privacy. It handles time range encryption to maintain a user traces utility. Specifically, the core IoT technology incorporated in this system covers sensors and actuators infrastructure. Passive monitoring is achieved by Wi-Fi wireless communication while active monitoring is based on smartphones adoption. The proposed system uses mesh surveillance architecture and the computation is performed locally at the edge components. Students' movement context is evaluated and inserted into supervised algorithms, that run on mobile smartphone applications. Authentication mechanisms and intrusion detection systems are incorporated to provide advanced surveillance services. The system complies with security and privacy regulations. Data leakage attacks are addressed with the use of anonymization, data encryption, network monitoring, and password security mechanisms. A quantitative research method is used to complete this effort. The data incorporated are from real and streaming text sources.

The performed experiments consider an encryption-based approach, providing stronger protection of user privacy. Results indicate that the adopted approach leads rather to moderate increase in network bandwidth, storage and computation overhead. Scalability issues should be also examined to assess the overall efficiency of the proposed system. Overall, the adopted effort provides a research direction, that incorporates encryption instead of anonymization for preserving user privacy in wireless environments.

Future work should be done towards the integration of the proposed research approaches. Specifically, in [50], it should be examined with more realistic use cases how the proposed system has a universal reference and significance with regards to the authentication and authorization process applied on the Smart Campus. More work is required in [51] where it is planned to expand the effectiveness of the system with biometrics and additional control equipment for campus surveillance purpose. Future work in [52] will focus mainly on expanding the proposed prototype to support other applications as well as investigating the possible use of multiple proxies in the system infrastructure.

5) SYSTEMS THAT FOCUS ON SMART BUILDINGS, PUBLIC SPACES, SMART LIGHTING AND SMART TRAFFIC LIGHTS

Researchers in [53], [54], and [55] propose surveillance systems that focus on smart buildings, public spaces, smart lighting, as well as smart traffic lights infrastructure. Specifically, in [53], the authors present a smart public safety system that is composed of contemporary surveillance equipment, a back-office system with a workflow engine and a mobile application for students. All the components are synchronized with an IoT platform, while passive monitoring is feasible due to GPS and 4G technologies. In addition, the system incorporates surveillance cameras and students' smartphones. Surveillance system combines both ad hoc and mobile architectures while it can perform face recognition based on movement user context. The system runs in mobile applications. An intrusion detection system is used that complies with security and privacy regulations, and a network monitoring security mechanism is incorporated to handle malicious attacks. A quantitative research methodology is used, while experiments are based on real and batch video data.

Experiments performed on the campus where smart cameras are deployed to provide surveillance services with a mobile application interface. Results suggest that the system is able to optimize university community safety. Maintenance of the proposed system is a challenging issue and needs to be examined in follow up experiments. Overall, the system is well deployed and tested, however more research should be done to achieve better maintenance services.

The authors of [54] introduce a sustainable Smart Campus system that integrates IoT technology and big data architecture, to provide surveillance services. The system also uses distributed and multilevel data analysis to find a reliable and efficient solution for implementing a sustainable university campus environment. An IoT platform along with sensors and actuators are incorporated. Passive monitoring is feasible due to RFID sensor technology, while active monitoring devices include surveillance cameras located in the campus. Surveillance system design is ad hoc and enhanced with edge computing technology that enables voice and face recognition based on social movement and crowd sensing user context. Big data architecture inserts data into a DSS that incorporates supervised algorithms to enhance surveillance QoS. The system uses both desktop and mobile applications. The adopted surveillance system features an intrusion detection system that complies with security and privacy standards. Eavesdropping attacks are tackled by anonymization, biometrics and network monitoring countermeasures, adopted by the proposed system. Acquisition time for mixed research methodology completion is defined within this effort, while the data used for experiments are real and batch, and the incorporated data types are text, sound, image and video sources.

Experiments of tuning certain parameters through simulation were performed based on real data exploiting campus operation. Results set the standards for real environments implementation that represent the system as a socioeconomic organization. Such system approach aims to consider university campus as small-scale testing environment. A limitation of the current study is the absence of system integration to scale up in the whole Smart Campus. Overall, it is a promising research effort that helps to define certain system standards for further implementation on campus, however scaling to the whole campus environment is required.

In [55], the authors propose a Name Data Networking (NDN) IoT university campus system, leveraging on connected devices and students' contents to provide efficient surveillance services. Specifically, an IoT platform, WSN, sensors and actuators core enabling technology are all used to support the proposed system. Passive monitoring achieved with the incorporation of RFID sensors, Ethernet, Wi-Fi, Bluetooth, and ZigBee wireless communication protocols. In addition, surveillance cameras and smart watches are used as active monitoring devices. Surveillance system design is mixed, combining ad hoc and mobile techniques, running on the cloud according to a certain big data architecture. The proposed system focuses on context aware inference of incidents and incorporates supervised and unsupervised algorithms. The system uses only mobile applications. The authentication system assures authorized access control to the system and cryptanalysis attacks are prevented by using data encryption and network monitoring security mechanisms. The research method used is qualitative, and acquisition time period is defined. Experiments are based on real and streaming data, and the supported data types supported are from text, image and video sources.

Experiments focused on real-life data while further processing and testing were used to design an appropriate NDN for the studied campus. Results mark out the lack a reasonable naming and addressing mechanism in the developed system. Experimental setup has limited resources with regards to examined network nodes and available data. Overall, it is an interested research work that proposes a NDN based on Hybrid Naming Scheme (NDN-HNS) for IoT-enabled Smart Campus.

Current research is well performed, however there is a need for future work to bear down on the observe findings. Specifically, the system proposed in [53] should scale in an integrated environment of a Smart Campus. More work is required in [54] to include methods for enabling student population to accept the leading technological changes as part of the proposed automation process. Future work in [55] aims to evaluate the proposed system for aggregating provided data to better assess user satisfaction rate on system's services.

6) SYSTEMS THAT FOCUS ON SMART BUILDINGS AND SMART LABS

In [56], [57], [58], and [59], surveillance systems that focus on smart buildings and smart labs are proposed. Specifically, in [56], the authors present a Cyber Range platform that evaluates various real-world cyber threat scenarios to provide an unbiased security assessment of information and automation control systems for Smart Campus surveillance. Core enabling technologies that are incorporated include an IoT platform, WSN and sensors located in the university campus. Communication protocols used as part of the passive monitoring technology are Ethernet and Wi-Fi, while students' smartphones are used for active monitoring of the campus. The surveillance system design is mobile and exploits cloud computing capabilities. The system uses movement students' context to insert data into a context awareness inference system based on supervised and unsupervised machine learning algorithms and running on mobile devices. A network-based intrusion detection system is incorporated. Acquisition time period of research completion is defined, and the effort deploys a qualitative research methodology. The data used are real and batch images.

Experiments performed test out-of-band data focusing on attack resistance with the use of a virtual machine introspection technique. Results obtained propose an object-dependent method to analyze the evidence of illegal activity. Note that if the time range is not limited the process of evidence vectors may refer to different threads that results in insufficient system accuracy. Overall, the study proposes a scalable and robust system, however correlation of host-level events needs to be further examined.

In [57], the researchers propose an identification and authentication system for Smart Campus surveillance based on RFID and smart cards biometrics technologies. The proposed system also supports synchronous and asynchronous

data processing capabilities to provide security services to the university campus. Specifically, RFID sensors, Bluetooth and NFC wireless communication technologies are incorporated. Active monitoring is feasible due to the adoption of surveillance cameras and students' smartphones. The design of the surveillance system is ad hoc and able to perform face recognition. A DSS is used for inference of an incident based on supervised algorithms. The system incorporates desktop applications. An authentication mechanism and an intrusion detection system are established to ensure students' uninterruptible use of a secure system that provides efficient security services. Password capture attacks are prevented with the incorporation of an antivirus system. A firewall keeps the internal network safe protecting it from external untrusted networks. The research methodology used to accomplish the effort is quantitative, and the data used for the experiments are real and streaming. The data types of the sources incorporated are text and images.

Performed experiments exploit two use cases based on how much the proposed system security could be improved by combining RFID and smart cards technologies. Observed results of the first use case focus on the performance of the verification process with student population using synchronous and asynchronous techniques. In the second use case, the focus is shifted on the security of accessing Smart Campus sensitive areas. In addition, system should exploit individual user context and move towards an integrated campus environment. Overall, it is a robust framework that combines RFID and biometrics technologies; however, more experiments required to scale up the adopted system.

The authors in [58] present a Smart Campus surveillance system that makes use of RFID and GPS technologies to promote student's well-being in an efficient learning university environment. The proposed system uses WSN as IoT enabling technology while surveillance is carried out by cameras located in the campus and smartphone devices supporting active monitoring. The surveillance system design is ad hoc and evaluates the user movement context to insert data into an adopted DSS. Such a DSS is built on a supervised machine-learning algorithm and incorporates mobile smartphone applications. An intrusion detection system is included to ensure compliance with security regulations provided by biometrics and network monitoring security mechanisms to confront MTM attacks. Acquisition time period of research completion is provided, and the research methodology followed is quantitative. The data used for experimentation are from real and streaming text sources.

Experiments are performed with real laboratory data towards an exploratory research based on RFID and GPS communication technologies. Results present that the proposed system security can prevent safety accidents effectively. Research is limited to small-scale spatial granularity. Overall, campus security based on IoT technology can be achieved, however there is much research required to adopt such a system by student population.

In [59], the researchers propose a surveillance system that adopts edge-computing potentiality to achieve real time student monitoring. The system explores the feasibility of Harr-Cascade feature extraction technique and Support Vector Machine (SVM) classifier at the edge devices, while it introduces a lightweight Convolutional Neural Network (L-CNN) to enable human detection. Specifically, an IoT platform, Raspberry Pi, WSN and sensor technologies communicating with Wi-Fi wireless networks are incorporated. Active monitoring is based on cameras located in the Smart Campus. The surveillance system design is ad hoc, and computation is used at the edge devices. The system evaluates social user context handled by big data architecture. A DSS is designed to adopt supervised, unsupervised and semi supervised machine learning algorithms in order to infer possible suspicious incidents. The proposed system incorporates mobile applications. An intrusion detection system is established to preserves user security and privacy. Incorporating network monitoring prevents MTM attacks. This effort uses quantitative research methods based on real and streaming data sources. Adopted data types for performing experiments include images and video data.

Experiments are performed in the context of edge computing environment based on gathered real data. Results are promising with regards to the fact that the proposed system is able to track human movement with adequate accuracy in real time. More research should be performed to assess the proposed system accuracy by providing new unseen instances to optimize its accuracy. Overall, adopted research provides a decent system used to track malicious human activity, however training phase should be expanded to incorporate more real data.

Based on the observed results, it is evident that significant work should be done. Specifically, in [56], future work should include methods for improving the system's performance as well as reducing the required memory usage. In addition, a distributed computing deployment should be built. In [57] additional experimentation is needed with further technologies to ensure a highly accurate authentication, such as cameras and motion sensors. Further research work, in [58] should focus on extended experiments to deploy the proposed system in the whole Smart Campus environment. Further work required in [59], establishing a proactive surveillance system that will enable campus safety by identifying suspicious human activities as well as raising early warning alerts.

7) SYSTEMS THAT FOCUS ON SMART BUILDINGS AND PUBLIC SPACES

In [60]–[67], and [68], researchers propose surveillance systems that focus on smart buildings and public spaces. Specifically, in [60] the authors introduce a surveillance care and guiding framework that incorporates deep learning-enabled facial recognition. The deployed Smart Campus safety system is called "Deep Guiding" and uses video trajectory derived from campus students to infer malicious behavior. The system is based on an IoT platform, WSN, sensors and

actuators contemporary technologies. Active monitoring is feasible due to RFID and GPS sensors as well as Wi-Fi, Bluetooth, ZigBee, and 4G wireless data communication protocols. Surveillance cameras enable online active monitoring of the student population moving in the campus. The surveillance system design is ad hoc and exploits cloud computing capabilities to perform face recognition with the proliferation of efficient supervised and semi supervised algorithms, which compose a DSS, to infer abnormal behavior. The system is incorporated only into mobile devices. An intrusion detection system is also used as a second line of defense, and data encryption techniques prevent attacks. A quantitative research methodology is used to accomplish the effort, and the acquisition time period is defined. The data used by the system are from real and streaming video sources.

Experiments are based on the implementation of an Android-based surveillance system tested on real data. Results show that the proposed system achieves a seamless indoor and outdoor navigation between buildings in the campus for efficient face recognition. Proposed system should be used in more areas of the campus than only in smart buildings and public spaces. Overall, it is well-designed system that keeps additional construction cost low by utilizing existing surveillance infrastructure in the campus.

The authors in [61] propose a Smart Campus system designed to reduce the reaction delay in reporting incidents regarding their occurrence time, by developing a mobile application. This application enables users to send alerts, directly from their smartphones to the nearest police department which include their real time location. Specifically, the system focuses on indoor localization incidents by incorporating an IoT platform, GPS sensors as well as Wi-Fi and Bluetooth passive monitoring technologies. Such a system is based solely on students' smartphone devices to enable a mobile surveillance system design. Cloud computing processing evaluates user movement context to provide context aware information of the university campus. Machine learning supervised algorithms that run on mobile applications are incorporated into the solution. An intrusion detection system is included that complies with user-centric security regulations, and sniffing attacks are prevented with the adoption of an anonymization security mechanism. This effort is accomplished using a quantitative research method. Experiments are performed using real and streaming text data sources.

Experiments with real data conducted in the campus where it is evaluated the proposed fine-grained location-aware security system. Results indicate that the adopted hybrid system incorporates efficiently the Wi-Fi fingerprint location approach and improves location accuracy with low cost. Scalability of the system in more areas in the campus as well as the limited adoption of the solution by student population is an issue that should be fixed. Overall, it is a novel work that has high location accuracy, however methods for the system to be adopted by the university community should be further examined.

In [62] the researchers present a mutual authentication protocol exploiting mobile RFID sensor technology to provide Smart Campus surveillance services. Specifically, an IoT platform is adopted to assist active monitoring, enhanced with surveillance cameras. The adopted surveillance system design is ad hoc and exploits social and movement user context. The supervised inference algorithms run on desktop and mobile applications and are able to capture abnormal students' activity. Authentication mechanisms and intrusion detection systems, which assure user privacy, are adopted to provide an integrated security solution. DoS, MTM and data leakage attacks are efficiently prevented by the system with the incorporation of anonymization, data encryption, biometrics and network monitoring mechanisms. A qualitative research methodology is followed, and the acquisition time of the research data is defined. Synthetic and batch text data sources are used for research experimentation.

Experiments are based on synthetic data used to improve existing mutual authentication protocol in mobile RFID card technology for Smart Campus. The experimental results are promising and the proposed system appears to lead to a strong, reliable, and effective security mechanism. Current research is tested only on synthetic data, thus there is a need to develop a new version that will be evaluated with real data as well. Overall, it is a well-defined mutual authentication approach for mobile RFID technology, however more experiments with real data required.

The researchers in [63] propose a surveillance system for Smart Campus that focuses on data storage security, by incorporating a steganography security mechanism. The system aims at developing a cloud-based security architecture for efficient surveillance in the university campus. Specifically, an IoT platform, WSN and sensor technology is adopted while Wi-Fi wireless data communication for passive monitoring are incorporated in the solution. Active monitoring is based mainly on the use of cameras located in the campus. The surveillance system design is ad hoc and evaluates cloud computing potentiality to process social user context. The system adopts mobile application technology. An intrusion detection system and an authentication system are incorporated to preserve students' security and privacy. Cryptanalysis, eavesdropping and jamming attacks are prevented by the adoption of a steganography security mechanism. This effort is based on a quantitative research method. The data used for the experiments are from synthetic and streaming data sources, and the supported data types cover text and images.

Experiments are based on synthetic data in the area of a cloud computing testbed exploiting IoT technology. The main results are promising for the application of the proposed cloud computing architecture to real campus environment. A limitation of this research effort is that the system is currently in development phase, and thus, its overall feasibility cannot be assessed. Overall, it is a cloud computing architecture that combines high importance IoT potentiality, for Smart Campus surveillance, however a deployment of the system in real environment is missing.

In [64], the authors introduce a surveillance system for Smart Campus based on signal strength maps. A prediction framework is developed, which incorporates random forests, to improve signal strength maps from limited measures. The core IoT enabling technology used in the research effort are sensor devices. Specifically, GPS sensor equipment enhanced with 5G communication technology is used for passive monitoring. Active monitoring is achieved through the incorporation of students' smartphones. The surveillance system design is mobile supported by cloud computing. Movement, crowdsourcing and crowd sensing user context are all evaluated by the proposed system to provide a DSS for inferring abnormal student behavior. In addition, efficient supervised and semi supervised machine learning algorithms are used for activity recognition. An intrusion detection system is introduced, and spoofing attacks are prevented by the incorporation of a password authentication mechanism. The research method followed in this effort is quantitative. Experiments are based on real and streaming data, and the system supports text data sources.

The experiments are performed in a laboratory with real data provided by participants. Results prove that the proposed system can significantly improve the tradeoff between prediction error and appropriate number of measurements required. Laboratory experimental setup is a limitation of the considered study. Specifically, incorporating data provided from more areas of the Smart Campus should do scaling of the system. Overall, the system achieves efficient prediction accuracy, however scaling of the research work is a need to evaluate the system in the whole area of the campus.

In [65], the researchers present a context aware authentication framework, using students' information available is the Smart Campus. The developed authentication framework can be the basis for the development of certain mobile context aware services. Specifically, the proposed system incorporates smart traffic lights from the physical infrastructure. In addition, an IoT platform is adopted, which handles data produced by connected sensors, such as RFID and GPS sensors. These sensors communicate through Wi-Fi, Bluetooth and NFC wireless data communication protocols, while cameras and users' smartphones achieve active monitoring. The surveillance system design is ad hoc. The user social activity and movement is inserted into a context aware system. The service-oriented architecture adopted to provide the capability of supervised inference algorithms, and the system incorporates mobile applications. An authentication system and an intrusion detection system are proposed to preserve security goals and comply with certain security standards. Sniffing attacks are prevented by the adoption of efficient data encryption and password mechanisms. This effort is based on a quantitative research method. The data used for experiments derive from real and batch image data sources.

Laboratory experiments based on real data provided mainly by soft sensors and other IoT equipment is the core of the evaluation schema. Results present an extensible context-aware authentication system which is able to adopt contextual information available in the university campus environment. The system should scale up to more places in the campus rather than only focusing on smart buildings and public spaces. This is an interesting research effort that lacks large scale deployment.

The authors in [66] introduce a flexible Smart Campus surveillance system, which is based on service-oriented architecture, to support social behavior in a university campus environment. A mobile middleware able to process social context is designed in the client frontend. In the server backend, context is aggregated and analyzed to facilitate social interactions. Specifically, the proposed system leverages IoT platform and sensor technologies. Passive monitoring is achieved through the incorporation of GPS sensors, and Ethernet, Wi-Fi and Bluetooth communication protocols. Active monitoring is supported by the adoption of students' smartphone devices. The surveillance system design is mobile and exploits both social context and movement of the user to support a service-oriented architecture. A DSS is designed to infer a possible student abnormal behavior incident based on supervised and unsupervised machine learning algorithms. The suggested system incorporates mobile applications. An authentication system is used according to security standards. Sniffing attacks are prevented by the adoption of efficient biometrics and network monitoring security mechanisms. A quantitative research methodology is adopted, and the acquisition time of research completion is defined. The textual data used for experimentation are from real and streaming data sources.

Experiments exploit real data and elaborate a flexible system architecture based on detailed service-oriented specification to support social interaction in university campus. Results prove that the designed mobile middleware can collect social context to provide surveillance service on campus environment. The system runs on a prototype deployed only on smart buildings and public places. Overall, it is a solid work with appropriate experimental testing, however it should be expanded to the whole university campus environment.

In [67], the researcher presents a surveillance system subject to a spatiotemporal authentication method. The system generates a unique identifier for use in authentication, by adopting context aware student's data, during actual presence in the Smart Campus. Particularly, the system adopts an IoT platform, WSN, sensors, and actuators technologies. Passive monitoring is based on RFID and GPS sensors and on Ethernet, Wi-Fi, NFC and 5G data communication protocols. Active monitoring devices include cameras and ATM located in the university campus. The surveillance system design is mesh, combining ad hoc and mobile components, and the movement and crowd sensing user context are processed in the cloud. A big data architecture is used, which inserts data into a context aware system, for inferring abnormal student behavior. Inference is based on supervised and unsupervised algorithms, and the system incorporates desktop applications. An authentication system is proposed

to fulfill students' security and privacy requirements, and incorporates data encryption, biometrics and network monitoring security mechanisms. Adopted research is based on a quantitative research methodology, and experimentation data include real and streaming data. The supported data types are from text, image and video data sources.

Experimental setup exploits real data provided for laboratory test purposes. Results provide a spatiotemporal authentication system, which is based on users' movement data collected on the Smart Campus. A limitation of the adopted effort is that the system evaluates only data captured by limited data sources. Overall, it is an interesting research work towards the definition of a spatiotemporal authentication scheme in university campus, however more data sources should be incorporated to evaluate the research effort.

The researcher in [68] proposes an extension of the surveillance system introduced in [67], to provide a more robust and integrated context aware spatiotemporal authentication method for Smart Campus adoption. To avoid duplications, we present only these components and features, which are not listed in the previous research effort since this effort is a superset of the prior one. Specifically, the proposed system adopts UAV and CAV technologies as part of the physical surveillance infrastructure. The system differs from the previous one because it takes into consideration as well microphones and smartphones as part of the active monitoring components. It extends adopted inference algorithms by using semi supervised machine learning algorithms, as well as mobile applications. Regarding experimental data, it uses additional sound data sources.

Experimental setup is based on real data captured from certain areas of the university campus. Results provide a spatiotemporal authentication schema, which is based on users' spatiotemporal history data as well as biometric recognition data sources. A limitation of current effort is that there is a need for data sources provided by robots moving in the Smart Campus environment. Broadly, a solid work, which provides spatiotemporal authentication as part of an integrated Smart Campus surveillance system, however robots should be used to explore areas that other devices cannot reach. Future work is required to observe better results of the proposed systems in the area of Smart Campus surveillance systems. Specifically, more work it required, in [60], towards an extension of current research towards gesture recognition detection for surveillance in campus. More work should be performed, in [61], focusing on the addition of more single techniques to enhance the proposed hybrid localization system. Extensive work, in [62], should focus on the application of the proposed authentication protocol to a wider area of the campus extending smart buildings and public spaces. Future directions, in [63], should focus on the development of appropriate software, which will improve security of the campus cloud resources. More work is required, in [64], which should include a hybrid machine learning propagation model to optimize current research schema. Contemporary work, in [65], should focus on fingerprinting context as well as of using cues from users' stochastic history to define unique user profiling for authentication purposes. Future research work, in [66], should focus on exploiting stochastic social interactions captured by the system to provide extensive authentication services. More work, in [67], should take into consideration online data sources provided by CAVs and UAVs as part of an integrated surveillance system. Future work, in [68], should focus on how CAVs, UAVs and robotic data will be fused to infer and provide an integrated surveillance system for the purposes of Smart Campus.

8) SYSTEMS THAT FOCUS ON SMART CAMPUS AMBIENT INTELLIGENCE USER CONTEXT

In [69]–[73], and [74], researchers propose surveillance systems that focus on smart campus Ambient Intelligence (AmI) user context. Specifically, in [69] the authors propose a surveillance system for Smart Campus, which focuses in smart labs and public spaces. Proposed system incorporates an IoT platform, which exploits sensors and WSN potentiality. Passive monitoring is based on RFID and Ethernet technology, while active monitoring is achieved by the use of cameras installed in the Smart Campus. Surveillance system design is based on mobile technology, while computing methodology adopted is cloud computing. It is used face recognition to enhance the operability of the system, while user context supported is focusing in user movement and AmI. Service-oriented software architecture is proposed, while inference system exploits context aware potentiality. Inference algorithms are based on supervised classification models, while VR capabilities are also supported. System runs in both desktop and mobile application environments. An intrusion detection system is used to support security standards. Security standards are exploiting network monitoring potentiality. Acquisition time to complete the research is mentioned, while the effort is using mixed research methodology. Data context incorporating includes real text data as well as images and video data sources.

Experimental setup is based real data captured from Smart Campus labs and public spaces. Results indicate an intrusion detection system, which is based on network monitoring. A limitation of the adopted effort is that it should incorporate more security mechanisms to provide a safer surveillance environment. Overall, it is an interesting research effort, which provides surveillance utilities based on an intrusion detection system, however a list of attacks it faces should be listed in more detail.

The researchers in [70] propose a surveillance system for university campus, which focuses on smart buildings, smart classes, public spaces and smart lighting. Adopted system uses IoT technology exploiting WSN, sensors and actuators capabilities. Passive monitoring is achieved through GPS, Wi-Fi, Bluetooth and ZigBee connectivity. Active monitoring is based on cameras and smartphones. Surveillance system design exploits mobile potentiality, while computing methodology incorporates cloud computing. Social, movement, and AmI user context is processed, while software architecture

is service-oriented. Inference system incorporates context aware techniques, while inference algorithms used exploit semi supervised models' capabilities. Proposed system uses virtual reality interfaces, while it is executed on mobile application environment. An intrusion detection system is elaborated to provide anonymization and network monitoring security mechanisms operability. Acquisition time required to complete current effort is provided, while research is based on quantitative methodology. Real steaming data sources are incorporated exploited text, image and video data types.

Experiments are based on real streaming data produced in Smart Campus' buildings, classes, public spaces and smart lighting infrastructure. Results prove that the adopted surveillance system is able to efficiently monitor network data traffic. A limitation of the proposed system is that it does not declare possible types of attacks it treats. Overall, it is an interesting research work, which provides surveillance capabilities incorporating AmI user context, however a more detailed list of security standards used should also be mentioned.

In [71], the researchers present a surveillance system, which is focusing on providing safety services to Smart Campus' building, classes, public spaces and smart parking physical infrastructure. Proposed research effort also incorporates electric vehicle technology, while adopted IoT platform exploits sensors' potentiality. Passive monitoring technology incorporates Bluetooth connectivity among mobile surveillance devices, while active monitoring is based on security cameras. Surveillance system supported is mobile, while computing methodology is focused on edge computing techniques. Social and AmI user context is analyzed, while it is used a service-oriented software architecture. Adopted context aware inference system enhances the capabilities of incorporated supervised inference algorithms, which are running on mobile application environments. Proposed authentication cyber security system complies with security standards and privacy regulations. Security system is able to face DoS attacks by incorporating network monitoring safety mechanisms. Acquisition time of research is mentioned, while it is adopted quantitative methodology. Research effort exploits real streaming video data sources.

Experiments are based on real streaming data captured from Smart Campus physical infrastructure. Results indicate that the adopted surveillance system complies with certain security standards and privacy regulations. A limitation of the proposed effort is the rather limited amount of data sources used to provide early warning surveillance services. Overall, it is a precise research work, which provides decent surveillance results, however more experiments should be performed by incorporating more precise data sources.

The authors in [72] present a Smart Campus surveillance system, which faces inefficiencies in smart buildings, smart labs, public spaces and smart lighting infrastructure. Proposed system incorporates an IoT platform exploiting sensors capabilities. Passive monitoring devices contain GPS technology, while active monitoring is mainly based on cameras installed in the university campus infrastructure. Surveillance system design is ad hoc, while adopted system exploits edge computing potentiality. Social, crowd sensing and AmI user context is exploited. Software architecture is based on big data, while it is used a decision support inference system. Classification algorithms enhance the inference process of the proposed system, while there are elaborated mobile applications to test and evaluate the system. Cyber security system is based on intrusion detection mechanisms, while security standards are incorporated. Password capture attacks are faced with the incorporation of data encryption, network monitoring and password policy security mechanisms. Time required to conduct the research is mentioned, while the type of the research is mixed incorporating quantitative and qualitative methodology. Data context used is based on real text data sources.

Experimental setup exploits real text data sources captured from the university campus infrastructure. Results towards an efficient intrusion detection system are promising. A limitation of the proposed research effort is that it is based only of text data sources. Overall it is a solid surveillance system work, however more rich data sources should be incorporated to enhance potentiality of current system.

In [73], the authors propose a surveillance system, which provides unobtrusive monitoring to public spaces and smart traffic lights of a university campus. Adopted system also incorporates UAV technology for achieving high quality of supported surveillance in the Smart Campus. An IoT platform is used to enhance the efficiency of the system along with WSN and sensors capabilities. Passive monitory is based on GPS technology, while active monitoring is achieved through installed cameras in the campus infrastructure. It is supported a mobile surveillance system design, while cloud computing potentiality is exploited. System incorporates face recognition techniques, while user context is based on crowdsourcing, crowd sensing and AmI technologies. Software architecture incorporates big data design, while it is used a decision support inference system, which exploits unsupervised and semi supervised inference algorithms. Adopted system application is running in both desktop and mobile environments. Cyber security is preserved with an authentication system. Security standards and privacy compliance regulations are supported by the proposed system, while it is incorporated a network monitoring mechanism to treat upcoming attacks. Research methodology is mixed, while time span of the effort is defined. Data used are real and synthetic, while there are also incorporated streaming, image and video data sources.

Experiments are based on both real and synthetic online data streaming. Results indicating the importance of a Smart Campus dedicated surveillance system are well presented. A limitation of the presented research effort is that security mechanisms are only based on network monitoring, while there are a lot of other mechanisms to enhance cyber security system efficiency. Overall it is a well-structured work, however more advanced security

mechanisms are needed to support the proposed research effort.

The researchers in [74] present a university campus surveillance system, which focuses on smart buildings, smart classes, smart parking and smart lighting. Proposed system also adopts smart traffic lights surveillance capabilities. IoT technology is incorporated along with WSN and sensors potentiality. Passive monitoring technology is achieved by RFID, Wi-Fi, Bluetooth, ZigBee and NFC supported equipment, while cameras are used for active monitoring. Surveillance system design is mobile, while computing methodology is based on cloud technology. User context is based on crowd sensing and AmI, while software architecture is service-oriented. Inference system is context aware, while the inference algorithms are based on supervised, unsupervised and semi supervised techniques. XR capabilities are based on VR technology, while the system runs on a mobile application environment. It is adopted an authentication cyber security system, while the surveillance technology incorporates security standards. Password capture and virus infection attacks are faced with the incorporation of network monitoring and antivirus system security mechanisms. Acquisition time of the effort is defined, while research methodology used is quantitative. Data context is composed of real streaming data, while there are also used image and video data sources.

Experimental setup is based on real streaming data sources produced from the Smart Campus area. Results are encouraging in adopting a well-defined surveillance system. A limitation of the effort is that it uses only cameras as an active monitoring technology. Overall, it is a compact research effort in the area of university campus surveillance systems, however more active monitoring devices should be adopted to enhance the efficiency of the system.

Based on the observed results it is obvious that significant work should be done. Specifically, in [69], future work should include a detailed list of upcoming attacks the system handles to provide a safer infrastructure. Further analysis of attacks faced by proposed system, in [70], should be listed in more detail. More experimentation is needed, in [71], with incorporating more precise data sources. Further research work is required in, [72], establishing a robust surveillance system, which will use multiple data sources to unobtrusively detect anomalies in the Smart Campus infrastructure. Further use of more security mechanisms are required, in [73], to enhance the potentiality of the proposed surveillance system. Further work is required, in [74], to support a more robust system by incorporating a variety of active monitoring technology devices.

9) SYSTEMS THAT FOCUS ON SMART CAMPUS LOW POWER WIDE AREA NETWORKS TECHNOLOGY

In [75]–[80], and [81], researchers propose surveillance systems that focus on smart campus LPWAN technology. Specifically, in [75] the authors propose a university campus surveillance system. Such system monitors unobtrusively students' behavioral context captured in smart buildings, public spaces, smart parking and smart lighting infrastructure. Electric vehicles are also used as monitoring devices. Adopted system incorporates an IoT platform along with Raspberry Pi, Arduino Uno, WSN, sensors and actuators devices. Passive monitoring is achieved with the incorporation of GPS, Ethernet, Wi-Fi, Bluetooth, and LPWAN technologies. Active monitoring is based on cameras installed in the Smart Campus infrastructure as well as students' smartphones. Surveillance system design is mobile, while it is supported cloud computing methodology. Social and movement user context is evaluated, while software architecture is service-oriented. A decision support inference system is incorporated, while there are supported supervised inference algorithms. Proposed system is running on mobile application environment. An intrusion detection system, which preserves security and privacy regulations is used to face hacking attacks. There are also incorporated anonymization, data encryption and network monitoring security mechanisms to treat malicious intruders' behavior. Time span of research conducted is declared, while qualitative research methodology is followed in the adopted effort. Real data context is used, while there are supported text, image and video data sources.

Experiments are based on real online data sources. Results focus on a robust surveillance system adopted by a certain university campus. A limitation of the proposed research is that there are only used supervised inference algorithms. Overall it is a solid work, however more precise inference algorithms and techniques should be incorporated in the presented research effort.

The researchers in [76] present a Smart Campus surveillance system which is based on the monitoring of smart buildings, smart labs and smart traffic lights. Specifically, IoT technology is adopted, which incorporates WSN, sensor and actuators devices. Passive monitoring is based on Wi-Fi, Bluetooth, 5G and LPWAN technologies. Active monitoring is mainly achieved with cameras, which are installed in the university campus area. Surveillance system design is mobile, while edge computing methodology is adopted. Software architecture is service-oriented, while inference system is based on decision support models. Adopted system runs in both desktop and mobile application environments. An authentication cyber security system is incorporated, which confronts with security standards. Proposed system is able to face sniffing attacks by using data encryption and network monitoring security mechanisms. Acquisition time to conduct the research is mentioned, while research methodology followed is quantitative. Data context required by the adopted system incorporates text and image data sources.

Experimental setup is based mainly on text and image data sources. Results lead to a surveillance system, which exploits LPWAN technology to achieve unobtrusive monitoring. A limitation of the adopted work is that it is not described in detail either the user context or the algorithms used to infer a malicious behavior in the Smart Campus.

In [77] the researchers propose a surveillance system for university campus, which focuses on smart buildings,

smart classes, and smart laboratories. An IoT platform along with WSN and sensor devices is also incorporated. Passive monitoring is using RFID, GPS, Bluetooth, 5G, and LPWAN technology, while active monitoring incorporates mainly surveillance cameras located in certain places within the Smart Campus infrastructure. Surveillance system design in based on mobile technology, while it is adopted cloud computing methodology. There are also supported face recognition techniques along with social and movement user context. Big data software architecture is incorporated, while context aware inference system potentiality is exploited. Proposed system is running on mobile application environment. Cyber security is based on an authentication system, which confronts with security and privacy regulations. Adopted system supports data encryption and network monitoring security mechanisms. Time span of the effort is mentioned, while research methodology used is mixed containing both quantitative and qualitative research. Data context is mainly online real streaming composed by sound, image and video data sources.

Experiments are performed with online real streaming data. Results indicate a well-structured surveillance system proposed to a university campus. A limitation of the adopted research effort is that there are not mentioned the algorithms, which infer an outlier student behavior. Overall it is a robust effort, however inference algorithms should be presented to be clearer how the system produces a security alarm.

The authors in [78] describe a Smart Campus surveillance system, which is based on the monitoring of smart buildings, smart classes, smart laboratories and public spaces. IoT technology exploits Raspberry Pi and sensors capabilities. Passive monitoring is enhanced with RFID, Ethernet, ZigBee, 4G, and LPWAN technologies. Active monitoring is achieved through cameras and microphones installed with university campus infrastructure. A mobile surveillance system design is adopted, which uses cloud computing potentiality. User context incorporated is based on social, crowdsourcing and crowd sensing techniques. Software architecture is service-oriented, while inference system is context aware exploiting AR capabilities. System application is running on mobile environment. An intrusion detection system is defined, which assures privacy compliance regulations. Security mechanism to face upcoming attacks is based on network monitoring. Acquisition time of research performed is defined, while it is used mixed research methodology. Data context incorporated is based on real sound and video data sources.

Experimental setup is based in online real sound and video data sources. Results are promising towards a robust surveillance system, which exploits LPWAN capabilities. A limitation of the proposed research effort is that it does not describes the inference algorithms incorporated as well as it does not describe emerged attacks that are treated by the system.

In [79] the authors present a university campus surveillance system, which unobtrusively monitors smart buildings, smart labs, smart parking places, and smart traffic lights. Core IoT technology is based on Arduino Uno, WSN, sensors, and actuators devices. Passive monitoring is able through RFID, GPS, Ethernet, Bluetooth, and LPWAN technologies, while active monitoring is mainly based on cameras and students' smartphones. Surveillance system design is mobile, while computing methodology is based on cloud capabilities. Social, movement and crowdsensing user context is exploited. A big data software architecture is supported, which evaluates unsupervised and semi supervised inference algorithms potentiality. XR is enhanced with VR techniques, while proposed system is running on mobile platform. Both an authentication and an intrusion detection system are used, which confront with safety and privacy regulations. DoS, eavesdropping, and MTM attacks are faced by adopted anonymization, data encryption, network monitoring and password security mechanisms. Time span of the effort is mentioned, while research methodology adopted is quantitative. Real data sources are used, which exploit text, image and video data context.

Experiments are based on text, image and video real data sources, while results are promising towards an advanced surveillance system for Smart Campus stability. A limitation of the adopted system is that is does not defines the inference system, which is responsible for deciding the category of an attack that may emerged in the university campus infrastructure.

The researchers in [80] propose a Smart Campus surveillance system that focuses on smart buildings, public spaces, and smart traffic lights. An IoT platform is incorporated, which exploits Raspberry Pi, Arduino Uno, WSN, sensors and actuators capabilities. Passive monitoring is based on RFID, Ethernet, Bluetooth, ZigBee and LPWAN technologies, while active monitoring is achieved by cameras installed on university campus places. Surveillance system design is based on mesh technology, while cloud computing potentiality is exploited. Social user context is evaluated, while inference system focuses on context aware principles. Proposed system incorporates supervised learning classification algorithms, while it is running on mobile application environment. Adopted system uses both an authentication and an intrusion detection security system, which confronts with safety and privacy regulations. Certain cryptanalysis, DoS, and jamming attacks are faced by adopted data encryption, biometrics, network monitoring, and firewall security mechanisms. Time acquisition of the efforts is defined, while research methodology used is mixed combining quantitative and qualitative research methods. Data context is based on real and streaming data sources.

Experimental setup focuses on exploitation of real and streaming data sources, while results prove that the proposed research effort university campus surveillance system has efficient behavior in facing emerged malicious attacks. A limitation of the system is that it does not reveal the software architecture it incorporates to perform its effective outcomes.

The authors in [81] present a university campus surveillance system, which examines user unobtrusive monitoring

in smart buildings, smart classes, smart labs, smart parking, and smart traffic lights. IoT technology exploit potentiality of WSN, sensors, and actuators. Passive monitoring is achieved through the adoption of RFID, Wi-Fi, 5G, and LPWAN infrastructure, while active monitoring is mainly based on cameras technology. Surveillance system is built upon mobile infrastructure, while it is supported cloud computing methodology. Adopted system exploits face recognition capabilities, while it is incorporated social and movement user context. Software architecture is based on big data programing design, while inference algorithms adopted include supervised, unsupervised and semi supervised model approaches. Proposed system runs on mobile application environment. An intrusion detection system is supported, which confronts with security standards and privacy compliance regulations. Adopted system treats DoS, spoofing, and sniffing malicious attacks with the incorporation of certain anonymization, data encryption, network monitoring, and password security mechanisms. Time span of the effort is mentioned, while research methodology followed is quantitative. Data context contain real, synthetic, streaming, text and image data sources.

Experiments are based on real, synthetic, streaming, text, and image data sources, while results indicate that the adopted Smart Campus surveillance system is robust. A limitation of the system is that it does not analyzes in deep detail the inference system it adopts to reach such a stable behavior.

Observed results dictate that there is much work, which should be undertaken. Specifically, in [75], more precise inference algorithms should be incorporated by the adopted surveillance system. Future work is required, in [76], where it should be incorporated in greater detail the user context and the inference algorithms used by the proposed surveillance system. In [77], there is needed more work towards presenting the inference algorithms incorporated to produce an early warning and prevention of an upcoming attack. Future research is required, [78], where it should be mentioned system's inference algorithms and emerged attacks, which is able to face. In [79], more research is needed to be undertaken towards the detailed definition of the inference system, which is supported to secure the proposed system. Further research should be performed, in [80], to reveal and exploit the capabilities of the supported software architecture. In [81], more research work is required to provide in more detail the adopted inference system, which is used to towards such a robust surveillance system behavior.

IV. COMPARATIVE ASSESSMENT

The summary of the comparative assessment performed on this survey is summarized in Table 1. Forty-four research efforts, 42 research papers and 2 patents, are reviewed and their strengths and weaknesses are shown. Through the survey, we attempt to classify each system according to our taxonomy developed to depict important parts of the research efforts. Concerning the dimension of physical infrastructure, smart buildings are adopted in 34 systems, smart classes in 10 systems, smart labs in 15 systems, public spaces in 31 systems, smart parking in 8 systems, and smart lighting in 12 systems. Also, smart traffic lights are incorporated in 14 systems, and electric vehicles in 4 systems. UAV are used in 3 systems, and in just one system there CAV are used. Regarding the enabling technologies dimension, IoT platform is applied in 35 systems, Raspberry Pi in 7 systems, Arduino Uno in 6 systems, WSN in 26 systems, sensors in 40 systems, and actuators in 16 systems. RFID is adopted in 25 systems, GPS in 23 systems, Ethernet in 12 systems, Wi-Fi in 22 systems, Bluetooth in 17 systems, ZigBee in 10 systems, NFC in 7 systems, 4G in 5 systems, 5G in 6 systems, and LPWAP in 7 systems.

Likewise, cameras are incorporated in 37 systems, microphones in 5 systems, smartphones in 18 systems, smart watches in 2 systems, and in ATM in 2 systems. Regarding the dimension of software analytics, ad hoc surveillance system design is used in 17 systems, mobile design in 18 systems, and mesh design in 9 systems. Edge computing methodology is adopted in 4 systems and cloud computing in 23 systems. Voice recognition is incorporated in 2 systems, face recognition in 10 systems and gesture recognition in 2 systems. Social user context is supported in 21 systems, movement context in 25 systems, crowdsourcing context in 5 systems, crowd sensing context in 10 systems, and AmI in 6 systems. Big data architecture is used in 14 systems, and service-oriented architecture in 9 systems. Context aware system is adopted in 14 systems, and DSS in 16 systems. Supervised machine learning algorithms are incorporated in 32 systems, unsupervised algorithms in 13 systems, and semi supervised algorithms in 9 systems. VR is supported in 4 systems and AR in 4 systems. Desktop applications are used in 11 systems, while mobile applications in 38 systems.

Regarding the system security dimension, an authentication system is adopted in 24 systems, while intrusion detection systems in 33 systems. Security standards are defined in 36 systems, and privacy compliance in 24 systems. Cryptanalysis attacks are targeted in 4 systems, DoS in 7 systems, eavesdropping in 3 systems, hacking in 3 systems, spoofing in 3 systems, sniffing in 8 systems, MTM in 5 systems, jamming in 2 systems, data leakage in 3 systems, password capture in 8 systems, and virus infection in 4 systems. Anonymization security mechanism is supported in 10 systems, steganography just in one system, data encryption in 17 systems, biometrics in 10 systems, network monitoring in 28 systems, firewall in 5 systems, password in 9 systems, and antivirus system in 4 systems. As for the dimension of research methodology, acquisition time of research completion is defined in 28 systems, a quantitative research method in 28 systems, qualitative research method in 5 systems, and a mixed research method in 11 systems. Real data are used in 40 systems, synthetic data in 5 systems, streaming data in 30 systems, batch data in 8 systems, text

TABLE 1. Comparative assessment.

Research Effort	Physical Infrastructure			Enabling Technologies			Software Analytics								System Security				Research Methodology	
	Components/Hardware			Components/Hardware			Components/Hardware	Features							Components/Hardware	Features			Features	
	Sustainable Smart Campus	Smart Transport	Autonomous Vehicles	Core IoT Technology	Passive Monitoring Technology	Active Monitoring Devices	Surveillance System Design	Computing Methodology	Affective Computing	User Context	Software Architecture	Inference System	Inference Algorithms	XR	Application	Cyber security System	Regulations	Attacks	Security Mechanisms	Research Context	Data Context
[38]	1, 6	2		1, 3, 4, 5, 6	1, 2, 3, 4, 5, 6	1, 3	1					1	1			2	1	7, 10	5, 6, 7	4	1, 3, 5, 8
[39]	2, 4			1, 4, 5	1, 2	3	2	2					1		2	2	1	2, 4	4	1, 2	1, 3, 5
[40]	4, 6			1, 3, 4, 5	2	1, 3	3		3	2			1		2	1, 2	1	4	7	2	1, 3, 7
[41]	1, 3, 4			5	2, 4	1, 3	1			1, 2, 3		2	1		2	1, 2	1, 2	6	5, 6, 8	1, 4	2, 4, 8
[42]	3, 4, 5, 6			1, 2, 3, 5, 6	1, 5, 6, 7	1, 2	1	2	2, 3	2		2			2	2	1	6, 10	3, 6	1, 2	1, 3, 6, 7, 8
[43]	4, 5			1, 5	4	1, 3	2	2		1, 2, 3	1	2	1		2	1, 2	1	5	7	1, 2	1, 4, 5, 8
[44]	4, 5		1	1, 2, 4, 5	1, 2, 8	1, 2, 3	3	2		1, 2		1	1, 2		2	1, 2	2	11	5	1, 2	1, 3, 5, 6, 7, 8
[45]	1, 3, 4, 6	2		1, 2, 3, 4, 5, 6	1, 3, 4, 6, 7	1	1	2		1					1, 2	1, 2	2	6	5	2	1, 3, 5
[46]	1, 3, 4, 6			1, 4, 5, 6	1, 4	1, 2, 3	1	2	1, 2		1		1	1, 2	2	1, 2	1		1, 4, 5	1, 3	1, 4, 6, 7, 8
[47]	4	1		1, 4, 5	1, 2	1	1	2			1	2	1, 2		1	1, 2	1, 2	2, 9, 10	1, 3, 4	1, 4	1, 3, 5
[48]	4	1		4, 5	2	1	1					2	1	1	2	1, 2	1	11	8	2	1, 3, 5
[49]	4	1		5	2, 8, 9	3, 4	2	2		1, 2	1		1, 2		2	2		10	3, 5	1, 2	1, 3, 5
[50]	1, 2			1, 5	1, 2	1	3	2		1					2	2	1	10, 11	6, 8	4	1, 3, 5, 8
[51]	1, 2	1		5	1, 4, 5, 6	1	1			2					1	1	1	1	3	2	1, 3, 5
[52]	1, 2			4, 5	4	3	3	1		2			1		2	1, 2	1, 2	9	1, 3, 5, 7	2	1, 3, 5
[53]	1, 4, 6	1		1	2, 8	1, 3	3		2	2					2	2	1, 2		5	2	1, 4, 8
[54]	1, 4, 6	1		1, 5, 6	1	1	1	1	1, 2	1, 2, 4	1	2	1		1, 2	2	1, 2	3	1, 4, 5	1, 4	1, 4, 5, 6, 7, 8
[55]	1, 4, 6	1		1, 4, 5, 6	1, 3, 4, 5, 6	1, 4	3	2			1	2	1, 2		2	1	1, 2	1	3, 5	1, 3	1, 3, 5, 7, 8
[56]	1, 3			1, 4, 5	3, 4	3	2	2		2		1	1, 2		2	2			5	1, 3	1, 4, 7
[57]	1, 3			5	1, 5, 7	1, 3	1		2			2	1		1	1, 2	1, 2	10	6, 8	2	1, 3, 5, 7
[58]	1, 3			4	1, 2	1, 3	1			2		2	1		2	2	1	7	4, 5	1, 2	1, 3, 5
[59]	1, 3			1, 2, 5, 6	4	1	1	1		1	1	2	1, 2, 3		2	2	1, 2	7	5	2	1, 3, 7, 8
[60]	1, 4			1, 4, 5, 6	1, 2, 4, 5, 6, 8	1	1	2	2			2	1, 3		2	2	1, 2		3	1, 2	1, 3, 8
[61]	1, 4			1	2, 4, 5	3	2	2		2		1	1		2	2	1	6	1	2	1, 3, 5
[62]	1, 4			1	1	1	1			1, 2			1		1, 2	1, 2	2	2, 7, 9	1, 3, 4, 5	1, 3	2, 4, 5
[63]	1, 4			1, 4, 5	4	1	1	2		1					2	1, 2	1, 2	1, 3, 8	2	2	2, 3, 5, 7
[64]	1, 4			5	2, 9	3	2	2		2, 3, 4		2	1, 3			2	2	5	7	2	1, 3, 5
[65]	1, 4	1		1, 5	1, 2, 4, 5, 7	1, 3	1			1, 2	2	1	1		2	1, 2	1	6	3, 7	2	1, 4, 7
[66]	1, 4			1, 5	2, 3, 4, 5	3	2			1, 2	2	1	1, 2		2	1	1	6	4, 5	1, 2	1, 3, 5
[67]	1, 4			1, 4, 5, 6	1, 2, 3, 4, 7, 9	1, 5	3	2		2, 4	1	1	1, 2		1	1	1, 2		3, 4, 5	2	1, 3, 5, 7, 8
[68]	1, 4		1, 2	1, 4, 5, 6	1, 2, 3, 4, 7, 9	1, 2, 3, 5	3	2		2, 4	1	1	1, 2, 3		1, 2	1	1, 2		3, 4, 5	2	1, 3, 5, 6, 7, 8
[69]	3, 4			1, 4, 5	1, 3	1	2	2	2	2, 5	2	1	1	2	1, 2	2	1		5	1, 4	1, 5, 7, 8
[70]	1, 2, 4, 6			1, 4, 5, 6	2, 4, 5, 6	1, 3	2	2		1, 2, 5	2	1	3	1	2	2			1, 5	1, 2	1, 3, 5, 7, 8
[71]	1, 2, 4, 5	2		1, 5	5	1	2	1		1, 5	2	1	1		2	1	1, 2	2	5	1, 2	1, 3, 8
[72]	1, 3, 4, 6			1, 5	2	1	1	1		1, 4, 5	1	2	1		2	2	1	10	3, 5, 7	1, 4	1, 5
[73]	4	1	1	1, 4, 5	2	1	2	2	2	3, 4, 5	1	2	2, 3	2	1, 2	1	1, 2		5	1, 4	1, 2, 3, 7, 8
[74]	1, 2, 5, 6	1		1, 4, 5	1, 4, 5, 6, 7	1	2	2		4, 5	2	1	1, 2, 3	1	2	1	1	10, 11	5, 8	1, 2	1, 3, 7, 8
[75]	1, 4, 5, 6	2		1, 2, 3, 4, 5, 6	2, 3, 4, 5, 10	1, 3	2	2		1, 2	2	2	1		2	2	1, 2	4	1, 3, 5	1, 3	1, 5, 7, 8
[76]	1, 3	1		1, 4, 5, 6	4, 5, 9, 10	1	2	1			2	2			1, 2	1	1	6	3, 5	1, 2	5, 7
[77]	1, 2, 3			1, 4, 5	1, 2, 5, 9, 10	1	2	2	2	1, 4	1	1			2	1	1, 2		3, 5	1, 4	1, 3, 6, 7, 8
[78]	1, 2, 3, 4			1, 2, 5	1, 3, 6, 8, 10	1, 2	2	2		1, 3, 4	2	1		2	2	2	2		5	1, 4	1, 6, 8
[79]	1, 3, 5	1		1, 3, 4, 5, 6	1, 2, 3, 5, 10	1, 3	2	2		1, 2, 4	1		2, 3	2	2	1, 2	1, 2	2, 3, 7	1, 3, 5, 7	1, 2	1, 5, 7, 8
[80]	1, 4	1		1, 2, 3, 4, 5, 6	1, 3, 5, 6, 10	1	3	2		1		1	1		2	1, 2	1, 2	1, 2, 8	3, 4, 5, 6	1, 4	1, 3
[81]	1, 2, 3, 5	1		1, 4, 5, 6	1, 4, 9, 10	1	2	2	2	1, 2	1		1, 2, 3		2	2	1, 2	2, 5, 6	1, 3, 5, 7	1, 2	1, 2, 3, 5, 7

TABLE 1. *(Continued.)* **Comparative assessment.**

Legends

Sustainable Smart Campus: (1) Smart Buildings, (2) Smart Class, (3) Smart Labs, (4) Public Spaces, (5) Smart Parking, (6) Smart Lighting **Smart Transport:** (1) Smart Traffic Lights, (2) Electric Vehicles **Autonomous Vehicles:** (1) Unmanned Aerial Vehicle (UAV), (2) Connected and Autonomous Vehicle (CAV)	**Core IoT Technology:** (1) IoT Platform, (2) Raspberry Pi, (3) Arduino Uno, (4) Wireless Sensor Networks, (5) Sensors, (6) Actuators **Passive Monitoring Technology:** (1) RFID, (2) GPS, (3) Ethernet, (4) Wi-Fi, (5) Bluetooth, (6) ZigBee, (7) NFC, (8) 4G, (9) 5G, (10) Low Power Wide Area Networks (LPWAN) **Active Monitoring Devices:** (1) Cameras, (2) Microphones, (3) Smartphones, (4) Smart watches, (5) ATM	**Surveillance System Design:** (1) Ad hoc, (2) Mobile, (3) Mesh **Computing Methodology:** (1) Edge, (2) Cloud **Affective Computing:** (1) Voice Recognition, (2) Face Recognition, (3) Gesture Recognition **User Context:** (1) Social, (2) Movement, (3) Crowdsourcing, (4) Crowd sensing, (5) Ambient Intelligence (AmI) **Software Architecture:** (1) Big Data, (2) Service-oriented **Inference System:** (1) Context Aware, (2) Decision Support **Inference Algorithms:** (1) Supervised, (2) Unsupervised, (3) Semi supervised **XR:** (1) VR, (2) AR **Application:** (1) Desktop, (2) Mobile	**Cybersecurity System:** (1) Authentication System, (2) Intrusion Detection System **Regulations:** (1) Security Standards, (2) Privacy Compliance **Attacks:** (1) Cryptanalysis, (2) DoS, (3) Eavesdropping, (4) Hacking, (5) Spoofing, (6) Sniffing, (7) Man in the Middle Attack (MTM), (8) Jamming, (9) Data Leakage, (10) Password Capture, (11) Virus Infection **Security Mechanisms:** (1) Anonymization, (2) Steganography, (3) Data Encryption, (4) Biometrics, (5) Network Monitoring, (6) Firewall, (7) Password, (8) Antivirus System	**Research Context:** (1) Acquisition Time, (2) Quantitative, (3) Qualitative, (4) Mixed **Data Context:** (1) Real, (2) Synthetic, (3) Streaming, (4) Batch, (5) Text, (6) Sound, (7) Image, (8) Video

data in 28 systems, sound data in 7 systems, image data in 22 systems, and video data in 23 systems.

V. CLASSIFICATION AND PROPOSED SOLUTION

Results of current research are mainly focused on the classification of the surveyed research efforts according to the adopted taxonomy while the final outcome is the proposed solution as a major contribution to the research community. Specifically, classification is based on exploitation of research efforts' significance according to certain metric values. Such metric values are the: (1) category normalized weight, (2) normalized values, and (3) values' relative frequencies. The metric values are computed by exhaustively analyzing the context of each effort and depicting its contribution by the proposed taxonomy.

Concretely, a weighting process is fundamental to assign quantitative numerical context to the examined metric values. Subsequently, the adopted scoring model is fed with data produced by the weighting process and produces a classification output according to certain values, which divide research efforts to three separate and disjoint classes. Proposed classes are divided based on certain value of adequacy introduced to the scoring model. Each class contains research efforts with similar behavior according to the outcome of the scoring model, while efforts of different classes have dissimilar behavior when compared with efforts of other classes. Based on the inferred three classes according to their efficiency we propose as a solution the research effort contained in the class with higher adequacy.

10) WEIGHTING PROCESS

To perform classification of the surveyed efforts and propose a generic solution, based on the adopted scoring model, we assigned normalized weights, i.e., sum up to 1, on the dimensions, the categories (i.e., components and features), and the values of the categories of the proposed taxonomy. The rationale behind the weighing process is to assign higher weights to dimensions, categories, and values of the categories, which have higher impact in IoT-enabled surveillance systems for Smart Campus, while lower weights are assigned in the opposite case. We assume that dimensions are conceptually regarded as equally weighted, since each dimension emerges a unique niche per surveillance system of the proposed taxonomy. Instead, the weights of categories within a certain dimension are varying according to the impact of the category to the surveillance systems. In addition, the values of each category are further weighted to have an in-depth knowledge of the weighting assignment process.

Specifically, for the physical infrastructure dimension, we have assigned higher weight to autonomous vehicles category, since it is more challenging to be achieved. Sustainable Smart Campus follows because buildings are the backbone of the infrastructure, and a smart transport category that has the lowest impact. Inside the autonomous vehicles' component category, UAV has higher weight than CAV, since UAV can record an incident where a CAV cannot reach it. In sustainable Smart Campus component category, smart buildings have the higher weight, because there are the main places of surveillance in the Smart Campus, and public spaces, smart parking, smart class, smart labs, and smart lighting follow. In smart transport component category, smart traffic lights achieve higher weight than electric vehicles, because they can capture more incidents, due to their location coverage area.

Subsequently, in the enabling technologies dimension, we assigned higher values to active monitoring devices category, because it has higher impact in surveillance process. The core IoT technology category follows, providing technology for surveillance mechanisms. Passive monitoring technology is considered as the passive part of the surveillance process.

In the active monitoring devices component category, cameras have the higher weight, because they can capture video and images of individuals in great detail. Microphones follow to provide ambient information, whereas smartphones, smart watches and ATM, are used for dedicated purpose only.

Within core IoT technology component category, we can distinguish the higher weight of IoT platform, because it processes all data produced from IoT devices, WSN, sensors, Arduino Uno, Raspberry Pi follow, which are also have distributed nature, and actuators because they perform only reaction processes. Passive monitoring technology component category contains high weights for 4G and 5G communication protocols due to their ambient nature, Wi-Fi, Ethernet, GPS, RFID, Bluetooth, NFC, and ZigBee follow, due to their limited coverage area.

TABLE 2. Normalized weights and relative frequencies.

Physical Infrastructure	Enabling Technologies	Software Analytics	System Security	Research Methodology
Dimensions' normalized weights are equal to 0.20				
Sustainable Smart Campus: (1) Smart Buildings, (2) Smart Class, (3) Smart Labs, (4) Public Spaces, (5) Smart Parking, (6) Smart Lighting **Category normalized weight:** 0.33 **Normalized Values:** (1) 1.00, (2) 0.50, (3) 0.33, (4) 0.83, (5) 0.67, (6) 0.17 **Values' relative frequencies:** (1) 0.31, (2) 0.09, (3) 0.14, (4) 0.28, (5) 0.07, (6) 0.11 **Smart Transport:** (1) Smart Traffic Lights, (2) Electric Vehicles **Category normalized weight:** 0.17 **Normalized Values:** (1) 1.00, (2) 0.50 **Values' relative frequencies:** (1) 0.78, (2) 0.22 **Autonomous Vehicles:** (1) Unmanned Aerial Vehicle (UAV), (2) Connected and Autonomous Vehicle (CAV) **Category normalized weight:** 0.50 **Normalized Values:** (1) 1.00, (2) 0.50 **Values' relative frequencies:** (1) 0.75, (2) 0.25	**Core IoT Technology:** (1) IoT Platform, (2) Raspberry Pi, (3) Arduino Uno, (4) Wireless Sensor Networks, (5) Sensors, (6) Actuators **Category normalized weight:** 0.33 **Normalized Values:** (1) 1.00, (2) 0.33, (3) 0.50, (4) 0.83, (5) 0.67, (6) 0.17 **Values' relative frequencies:** (1) 0.29, (2) 0.10, (3) 0.14, (4) 0.24, (5) 0.19, (6) 0.05 **Passive Monitoring Technology:** (1) RFID, (2) GPS, (3) Ethernet, (4) Wi-Fi, (5) Bluetooth, (6) ZigBee, (7) NFC, (8) 4G, (9) 5G, (10) Low Power Wide Area Networks (LPWAN) **Category normalized weight:** 0.17 **Normalized Values:** (1) 0.50, (2) 0.60, (3) 0.70, (4) 0.80, (5) 0.40, (6) 0.20, (7) 0.30, (8) 1.00, (9) 0.90, (10) 0.10 **Values' relative frequencies:** (1) 0.20, (2) 0.17, (3) 0.09, (4) 0.16, (5) 0.12, (6) 0.07, (7) 0.05, (8) 0.04, (9) 0.05, (10) 0.05 **Active Monitoring Devices:** (1) Cameras, (2) Microphones, (3) Smartphones, (4) Smart watches, (5) ATM **Category normalized weight:** 0.50 **Normalized Values:** (1) 1.00, (2) 0.80, (3) 0.60, (4) 0.40, (5) 0.20 **Values' relative frequencies:** (1) 0.55, (2) 0.07, (3) 0.31, (4) 0.03, (5) 0.03	**Surveillance System Design:** (1) Ad hoc, (2) Mobile, (3) Mesh **Category normalized weight:** 0.20 **Normalized Values:** (1) 0.67, (2) 0.33, (3) 1.00 **Values' relative frequencies:** (1) 0.39, (2) 0.41, (3) 0.20 **Computing Methodology:** (1) Edge, (2) Cloud **Category normalized weight:** 0.18 **Normalized Values:** (1) 1.0 0, (2) 0.50 **Values' relative frequencies:** (1) 0,18 (2) 0.82 **Affective Computing:** (1) Voice Recognition, (2) Face Recognition, (3) Gesture Recognition **Category normalized weight:** 0.07 **Normalized Values:** (1) 0.14, (2) 0.71, (3) 1.00 **Values' relative frequencies:** (1) 0.14, (2) 0.72, (3) 0.14 **User Context:** (1) Social, (2) Movement, (3) Crowdsourcing, (4) Crowd sensing, (5) Ambient Intelligence (AmI) **Category normalized weight:** 0.09 **Normalized Values:** (1) 0.40, (2) 1.00, (3) 0.60, (4) 0.80, (5) 0.20 **Values' relative frequencies:** (1) 0.32, (2) 0.36, (3) 0.08, (4) 0.14, (5) 0.11 **Software Architecture:** (1) Big Data, (2) Service-oriented **Category normalized weight:** 0.16 **Normalized Values:** (1) 0.50, (2) 1.00 **Values' relative frequencies:** (1) 0.61, (2) 0.39 **Inference System:** (1) Context Aware, (2) Decision Support **Category normalized weight:** 0.13 **Normalized Values:** (1) 1.00, (2) 0.50 **Values' relative frequencies:** (1) 0.48, (2) 0.52 **Inference Algorithms:** (1) Supervised, (2) Unsupervised, (3) Semi supervised **Category normalized weight:** 0.11 **Normalized Values:** (1) 0.67, (2) 0.33, (3) 1.00 **Values' relative frequencies:** (1) 0.59, (2) 0.24, (3) 0.17 **XR:** (1) VR, (2) AR **Category normalized weight:** 0.04 **Normalized Values:** (1) 1.00, (2) 0.50 **Values' relative frequencies:** (1) 0.44, (2) 0.56 **Application:** (1) Desktop, (2) Mobile **Category normalized weight:** 0.02 **Normalized Values:** (1) 0.50, (2) 1.00 **Values' relative frequencies:** (1) 0.22, (2) 0.78	**Cybersecurity System:** (1) Authentication System, (2) Intrusion Detection System **Category normalized weight:** 0.40 **Normalized Values:** (1) 1.00, (2) 0.50 **Values' relative frequencies:** (1) 0.42, (2) 0.58 **Regulations:** (1) Security Standards, (2) Privacy Compliance **Category normalized weight:** 0.30 **Normalized Values:** (1) 1.00, (2) 0.50 **Values' relative frequencies:** (1) 0.60, (2) 0.40 **Attacks:** (1) Cryptanalysis, (2) DoS, (3) Eavesdropping, (4) Hacking, (5) Spoofing, (6) Sniffing, (7) Man in the Middle Attack (MTM), (8) Jamming, (9) Data Leakage, (10) Password Capture, (11) Virus Infection **Category normalized weight:** 0.20 **Normalized Values:** (1) 0.18, (2) 0.64, (3) 1.00, (4) 0.36, (5) 0.09, (6) 0.91, (7) 0.82, (8) 0.55, (9) 0.73, (10) 0.27, (11) 0.45 **Values' relative frequencies:** (1) 0.24, (2) 0.12, (3) 0.05, (4) 0.05, (5) 0.05, (6) 0.14, (7) 0.08, (8) 0.03, (9) 0.05, (10) 0.14, (11) 0.05 **Security Mechanisms:** (1) Anonymization, (2) Steganography, (3) Data Encryption, (4) Biometrics, (5) Network Monitoring, (6) Firewall, (7) Password, (8) Antivirus System **Category normalized weight:** 0.10 **Normalized Values:** (1) 0.38, (2) 0.25, (3) 0.63, (4) 0.13, (5) 0.50, (6) 0.88, (7) 1.00, (8) 0.75 **Values' relative frequencies:** (1) 0.11, (2) 0.01, (3) 0.20, (4) 0.11, (5) 0.34, (6) 0.07, (7) 0.10, (8) 0.06	**Research Context:** (1) Acquisition Time, (2) Quantitative, (3) Qualitative, (4) Mixed **Category normalized weight:** 0.67 **Normalized Values:** (1) 1.00, (2) 0.75, (3) 0.25, (4) 0.50 **Values' relative frequencies:** (1) 0.39, (2) 0.39, (3) 0.07, (4) 0.15 **Data Context:** (1) Real, (2) Synthetic, (3) Streaming, (4) Batch, (5) Text, (6) Sound, (7) Image, (8) Video **Category normalized weight:** 0.33 **Normalized Values:** (1) 1.00, (2) 0.63, (3) 0.88, (4) 0.75, (5) 0.13, (6) 0.25, (7) 0.38, (8) 0.50 **Values' relative frequencies:** (1) 0.24, (2) 0.03, (3) 0.18, (4) 0.05, (5) 0.18, (6) 0.04, (7) 0.13, (8) 0.14

Regarding the software analytics dimension, we distinguish high weights for the surveillance system design category, because it is the most significant component in the surveillance process. In descending order of surveillance significance, computing methodology, software architecture, inference system, inference algorithms, user context, affective computing, XR and applications. Specifically, in the surveillance systems design component category, we assign higher weight to a mesh system design because it combines the strengths of other approaches. Ad hoc and mobile system design follow, because they are prone to relocation recording errors. In the computing methodology feature category, we have assigned higher weight to edge computing than to cloud computing, because the edge computing incidents are treated locally and distributed, not overloading the central infrastructure. Next in the software feature category a higher weight is assigned to the service-oriented architecture than to big data architecture, because emphasis is given to surveillance as a service approach. In the inference system feature category, a higher weight has assigned to context aware system compared with DSS, because it achieves an ambient behavior of the system. In addition, in the inference algorithms feature category, we distinguish and apply higher weight to semi supervised algorithms, because they use advanced machine learning modeling techniques, compared to supervised and unsupervised algorithms. In the user context feature category, we assign higher weight to the movement context, because it enables online location prediction of an abnormal behavior in the campus, compared to crowd sensing, crowdsourcing and social context. In the affective computing feature category, we assign higher weight to gesture recognition, because it reveals in more detail proactive intention of an individual compared to face and voice recognition. In the XR feature category, we assign higher weight to VR, because it is harder to be implemented in a Smart Campus environment compared to AR. In the application feature category, we applied higher weight to mobile applications, because they are able to capture more incidents, which are distributed in several locations within the university campus, compared to desktop applications.

Considering the system security dimension, we apply high weight to cybersecurity system, because it is the core security category compared to the regulations, attacks and security mechanisms supporting categories. Similarly, in the cybersecurity system component category, we assign higher weight to the authentication system, because it controls the authorized access to the system, compared to the intrusion detection system, which aims at detecting malicious behavior, based on information provided by the authentication system, and forms a second line of defense. In the regulations

TABLE 3. Scoring of research efforts.

Research Efforts	Score v(i)	Research Efforts	Score v(i)
[38]	0.399	**[60]**	0.405
[39]	0.322	**[61]**	0.322
[40]	0.387	**[62]**	0.321
[41]	0.333	**[63]**	0.487
[42]	0.398	**[64]**	0.285
[43]	0.248	**[65]**	0.349
[44]	0.267	**[66]**	0.408
[45]	0.287	**[67]**	0.380
[46]	0.333	**[68]**	0.500*
[47]	0.330	**[69]**	0.346
[48]	0.373	**[70]**	0.387
[49]	0.253	**[71]**	0.396
[50]	0.331	**[72]**	0.330
[51]	0.307	**[73]**	0.459
[52]	0.287	**[74]**	0.434
[53]	0.359	**[75]**	0.398
[54]	0.227	**[76]**	0.370
[55]	0.400	**[77]**	0.375
[56]	0.336	**[78]**	0.318
[57]	0.288	**[79]**	0.472
[58]	0.411	**[80]**	0.427
[59]	0.301	**[81]**	0.438
*Highest Score		**[68]**	0.500*

TABLE 4. Classification of research efforts.

Class	Research Effort
High Adequacy (v_H =0.405)	**[68], [63], [79], [73], [81], [74], [80], [58], [66], [60]**
Medium Adequacy (v_M =0.308)	**[55], [38], [42], [75], [71], [40], [70], [67], [77], [48], [76], [53], [65], [69], [56], [41], [46], [50], [47], [72], [39], [61], [62], [78]**
Low Adequacy	**[51], [59], [57], [45], [52], [64], [44], [49], [43], [54]**

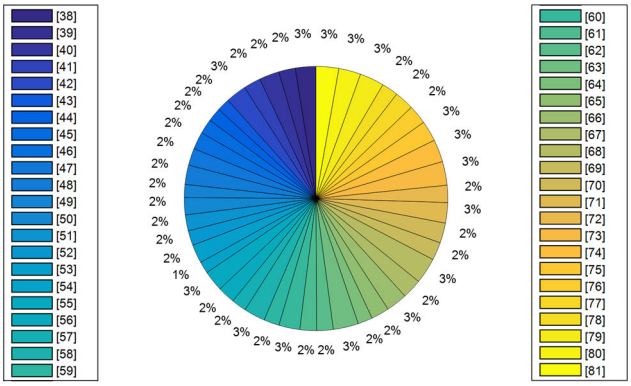

FIGURE 10. Scoring of research efforts visualization.

feature category, the standards have higher weight compared to the privacy compliance, because the standards form the contextual framework of security and privacy. In the attack feature, we assign higher weight to the attacks that happen more frequently and their descending order from the most frequent to the least one is eavesdropping, sniffing, MTM, data leakage, DoS, jamming, virus infection, hacking, password capture, cryptanalysis, and spoofing. In the security mechanisms feature category, we assign higher weight to the countermeasure used more often for system prevention, and their descending order from the most frequent countermeasure to the least frequent one is password, firewall, antivirus system, data encryption, network monitoring, anonymization, steganography, and biometrics.

Regarding the research methodology dimension, we assign high weights for the research context category, because it depicts the research impact of the effort to the scientific community. The data context category used during the research by the effort follows. In the research context feature category, we assigned high weight in efforts that mention the acquisition time of research completion, because this reveals more information about the work carried out by the researchers. The quantitative research receives higher weight, because its results can be generalized comparing to mixed and qualitative research methods. Subsequently, in the data context feature category, real and streaming data are advanced with higher weights, due to their dynamic nature when compared to batch and synthetic data. In addition, higher weight is assigned to video data, because it is more detailed comparing to image, sound and text data.

To further exploit the potential of the adopted scoring model, we also assign normalized relative frequencies, i.e., sum up to 1, to each value of a certain category. Counting and then normalizing the frequency of a specific value that occurs in a certain component or feature category, we produce relative frequencies assignment. Table 2 presents an overview of the normalized weights and the relative frequencies for certain dimensions, components, features and their corresponding values incorporated in the proposed taxonomy.

11) CLASSIFICATION PROCESS

Since all taxonomy data has assigned with certain normalized weights and relative frequency values, we feed them to the adopted scoring model to calculate the value of each research effort. Table 3 presents the scoring output of all research efforts. Visualization of the scoring percentage for the surveyed research efforts is provided in Fig. 10.

The final stage of the scoring model is the classification of the research efforts into the three classes. The threshold values v_H and v_M are set by the experts and the classified items are shown in Table 4. Visualization of the classification percentage for the surveyed research efforts is presented in Fig. 11.

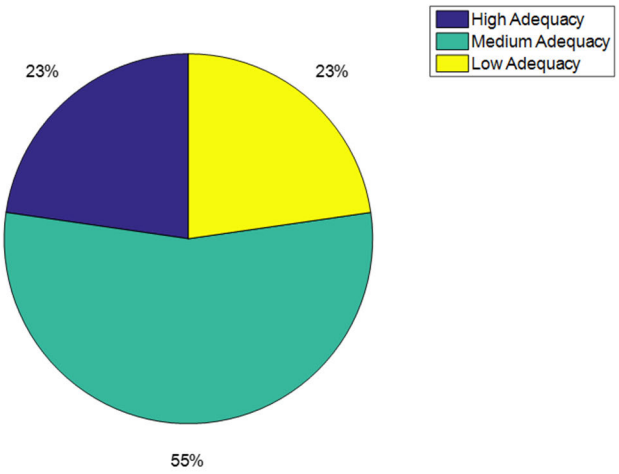

FIGURE 11. Classification of research efforts visualization.

The proposed solutions are those in the High Adequacy class, namely research efforts [58], [60] [63], [66], [68], [73], [74], [79], [80], and [81], which achieve higher score than the other efforts according to the proposed taxonomy and the adopted scoring model, thus is the outcome of this survey.

VI. CONCLUSION AND FUTURE WORK

We performed a survey on IoT-enabled Smart Campus Surveillance Systems available in the literature. We focused on Smart Campus as a socially acceptable solution, since advanced universities are open to change management as well as to experiment intuitively with unknown safety situations. Specifically, there are some real implications, which make these systems acceptable by the scientific community, such as prevent and repression of a delinquent behavior as well as studying the motivation and the development behind this behavior. Such knowledge will be of high importance when designing and evaluating advanced surveillance systems in Smart Cities, like the one in London, UK to prevent terrorism and terrorist attacks.

The survey is based on certain dimensions derived from the surveyed papers and patents, following certain conceptual patterns. The motivation behind this survey is that only relevant surveillance systems will be examined having a trace to all dimensions, which are: (1) Smart Campus physical infrastructure, (2) IoT core enabling technologies, (3) predictive software analytics, (4) system security and management, and (5) applied research methodology. We adopt a scoring model designed to evaluate the proposed taxonomy. The outcome of the survey is a classification of the research efforts, providing a set of proposed research efforts to be further analyzed by the scientific community and industry, according to their utility towards surveillance systems.

The findings of this survey, conducted to reveal crucial security relevant and other issues, are valuable and applicable for the construction of any robust surveillance model designed specifically for Smart Campuses. This construction should incorporate modules with advanced technological achievements that will efficiently supervise and monitor a modern Smart Campus system, towards preventing its uninterruptible operation and improving the standards of the provided services.

Important aspects in this future research direction should be the proposed taxonomy, and the results produced by the classification process. The survey findings have showed that the five main dimensions defined for the taxonomy, the physical infrastructure, the enabling technologies, the software analytics, the system security, and the research methodology should be incorporated as discrete key features and will formulate independent modules in surveillance systems for Smart Campuses.

In addition, the derived findings of the weighted scoring model, proposed in the adopted taxonomy, might be exploited to construct a secure architecture for efficient smart campus surveillance systems.

Finally, we could further expand the results of the current survey in the future to consider patents that will be produced by the surveyed research papers, while start-ups that will emerge based on the surveyed patents will also be analyzed. The aim of our future work is to research the impact of scientific invention in the area of IoT-enabled Smart Campus surveillance systems to industrial innovation for mankind well-being.

REFERENCES

[1] M. A. Rodriguez-Hernandez, A. Gomez-Sacristan, and D. Gomez-Cuadrado, "SimulCity: Planning communications in smart cities," *IEEE Access*, vol. 7, pp. 46870–46884, 2019.

[2] C. Garrido-Hidalgo, D. Hortelano, L. Roda-Sanchez, T. Olivares, M. C. Ruiz, and V. Lopez, "IoT heterogeneous mesh network deployment for human-in-the-loop challenges towards a social and sustainable industry 4.0," *IEEE Access*, vol. 6, pp. 28417–28437, 2018.

[3] B. Cheng, D. Zhu, S. Zhao, and J. Chen, "Situation-aware IoT service coordination using the event-driven SOA paradigm," *IEEE Tran. Netw. Services Manag.*, vol. 13, no. 2, pp. 349–361, Jun. 2016.

[4] S. G. Nagarajan, P. Zhang, and I. Nevat, "Geo-spatial location estimation for Internet of Things (IoT) networks with one-way time-of-arrival via stochastic censoring," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 205–214, Feb. 2017.

[5] I. Livaja, D. Skvorc, and K. Pripuzic, "Geospatial publish/subscribe systems for the Internet of Things," in *Proc. 25th Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, Split, Croatia, Sep. 2017, pp. 1–8.

[6] X. Cao and S. Madria, "Efficient geospatial data collection in IoT networks for mobile edge computing," in *Proc. IEEE 18th Int. Symp. Netw. Comput. Appl. (NCA)*, Cambridge, MA, USA, Sep. 2019, pp. 1–10.

[7] K. K. Lwin, Y. Sekimoto, W. Takeuchi, and K. Zettsu, "City geospatial dashboard: IoT and big data analytics for geospatial solutions provider in disaster management," in *Proc. Int. Conf. Inf. Commun. Technol. Disaster Manage. (ICT-DM)*, Paris, France, Dec. 2019, pp. 1–4.

[8] J. Zhang, Y. Wang, S. Li, and S. Shi, "An architecture for IoT-enabled smart transportation security system: A geospatial approach," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6205–6213, Apr. 2021.

[9] A. Kamilaris and F. O. Ostermann, "Geospatial analysis and the Internet of Things," *ISPRS Int. J. Geo-Inf.*, vol. 7, p. 269, Jul. 2018.

[10] M. Rieke, L. Bigagli, S. Herle, S. Jirka, A. Kotsev, T. Liebig, C. Malewski, T. Paschke, and C. Stasch, "Geospatial IoT—The need for event-driven architectures in contemporary spatial data infrastructures," *ISPRS Int. J. Geo-Inf.*, vol. 7, no. 10, p. 385, Sep. 2018.

[11] L. Kang, "Street architecture landscape design based on wireless Internet of Things and GIS system," *Microprocessors Microsyst.*, vol. 80, Feb. 2020, Art. no. 103362.
[12] L. Miloudi and K. Rezeg, "Leveraging the power of integrated solutions of IoT and GIS," in *Proc. 3rd Int. Conf. Pattern Anal. Intell. Syst. (PAIS)*, Tebessa, Algeria, Oct. 2018, pp. 1–7.
[13] M. Mena, A. Corral, L. Iribarne, and J. Criado, "A progressive web application based on microservices combining geospatial data and the Internet of Things," *IEEE Access*, vol. 7, pp. 104577–104590, 2019.
[14] L. Wang, C. Yao, Y. Yang, and X. Yu, "Research on a dynamic virus propagation model to improve smart campus security," *IEEE Access*, vol. 6, pp. 20663–20672, 2018.
[15] J. Mullins, "Ring of steel II–New York City gets set to replicate London's high-security zone," *IEEE Spectr.*, vol. 43, no. 7, pp. 12–13, Jul. 2006.
[16] C. R. Storck and F. Duarte-Figueiredo, "A survey of 5G technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by internet of vehicles," *IEEE Access*, vol. 8, pp. 117593–117614, 2020.
[17] A. Zourmand, A. L. Kun Hing, C. Wai Hung, and M. AbdulRehman, "Internet of Things (IoT) using LoRa technology," in *Proc. IEEE Int. Conf. Autom. Control Intell. Syst. (I2CACIS)*, Selangor, Malaysia, Jun. 2019, pp. 324–330.
[18] M. Iqbal, A. Y. M. Abdullah, and F. Shabnam, "An application based comparative study of LPWAN technologies for IoT environment," in *Proc. IEEE Region 10 Symp. (TENSYMP)*, Dhaka, Bangladesh, 2020, pp. 1857–1860.
[19] F. J. Dian and R. Vahidnia, "LTE IoT technology enhancements and case studies," *IEEE Consum. Electron. Mag.*, vol. 9, no. 6, pp. 49–56, Nov. 2020.
[20] O. Elgarhy, L. Reggiani, H. Malik, M. M. Alam, and M. A. Imran, "Rate-latency optimization for NB-IoT with adaptive resource unit configuration in uplink transmission," *IEEE Syst. J.*, vol. 15, no. 1, pp. 265–276, Mar. 2021.
[21] M. S. Chishti, C. T. King, and A. Banerjee, "Exploring half-duplex communication of NFC read/write mode for secure multi-factor authentication," *IEEE Access*, vol. 9, pp. 6344–6357, 2021.
[22] A. Lavric, A. I. Petrariu, and V. Popa, "Long range sigfox communication protocol scalability analysis under large-scale, high-density conditions," *IEEE Access*, vol. 7, pp. 35816–35825, 2019.
[23] S. Long and F. Miao, "Research on ZigBee wireless communication technology and its application," in *Proc. IEEE 4th Adv. Inf. Technol., Electron. Autom. Control Conf. (IAEAC)*, Chengdu, China, Dec. 2019, pp. 1830–1834.
[24] J. Galeano-Brajones, J. Garmona-Murillo, J. F. Valenzuela-Valdes, and F. Luna-Valero, "Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: An experimental approach," *Sensors*, vol. 20, no. 3, p. 816, Feb. 2020.
[25] C.-H. Liao, H.-H. Shuai, and L.-C. Wang, "Eavesdropping prevention for heterogeneous Internet of Things systems," in *Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2018, pp. 1–2.
[26] N. Wang, L. Jiao, P. Wang, M. Dabaghchian, and K. Zeng, "Efficient identity spoofing attack detection for IoT in mm-wave and massive MIMO 5G communication," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–6.
[27] F. Ahmad, A. Adnane, V. N. L. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies," *Sensors*, vol. 18, no. 11, p. 4040, Nov. 2018.
[28] S. Shin and K. Kobara, "A secure anonymous password-based authentication protocol with control of authentication numbers," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA)*, Monterey, CA, USA, Oct./Nov. 2016, pp. 325–329.
[29] J. M. Carracedo, M. Milliken, P. K. Chouhan, B. Scotney, Z. Lin, A. Sajjad, and M. Shackleton, "Cryptography for security in IoT," in *Proc. 5th Int. Conf. Internet Things: Syst., Manage. Secur. (IoTSMS)*, Valencia, Spain, Oct. 2018, pp. 23–30.
[30] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, Jul. 2019.
[31] H. Lei, D. Wang, K. H. Park, I. S. Ansari, J. Jiang, G. Pan, and M. S. Alouini, "Safeguarding UAV IoT communication systems against randomly located eavesdroppers," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1230–1244, Feb. 2020.
[32] R. L. Keeney and H. Raiffa, *Decisions With Multiple Objectives–Preferences and Value Tradeoffs*. Cambridge, U.K.: Cambridge Univ. Press, 1993, pp. 1–569.
[33] E. Siskos and N. Tsotsolas, "Elicitation of criteria importance weights through the Simos method: A robustness concern," *Eur. J. Oper. Res.*, vol. 246, no. 2, pp. 543–553, Oct. 2015.
[34] J. Figueira and B. Roy, "Determining the weights of criteria in the ELECTRE type methods with a revised Simos' procedure," *Eur. J. Oper. Res.*, vol. 139, no. 2, pp. 317–326, Jun. 2002.
[35] J. Pictet and D. Bollinger, "Extended use of the cards procedure as a simple elicitation technique for MAVT. Application to public procurement in Switzerland," *Eur. J. Oper. Res.*, vol. 185, no. 3, pp. 1300–1307, Mar. 2008.
[36] T. Solymosi and J. Dombi, "A method for determining the weights of criteria: The centralized weights," *Eur. J. Oper. Res.*, vol. 26, no. 1, pp. 35–41, Jul. 1986.
[37] N. Tsotsolas, A. Spyridakos, E. Siskos, and I. Salmon, "Criteria weights assessment through prioritizations (WAP) using linear programming techniques and visualizations," *Oper. Res.*, vol. 19, no. 1, pp. 135–150, Mar. 2019.
[38] S. Datta and S. Sarkar, "Automation, security and surveillance for a smart city: Smart, digital city," in *Proc. IEEE Calcutta Conf. (CALCON)*, Kolkata, India, Dec. 2017, pp. 26–30.
[39] Y. C. Chang, "Evaluation and exploration of optimal deployment for RFID services in smart campus framework," in *Computer Science and its Applications* (Lecture Notes in Electrical Engineering), vol. 203, S. S. Yeo, Y. Lee, and H. Chang, Eds. Dordrecht, The Netherlands: Springer, 2012, pp. 493–502.
[40] S. Gahlaut and K. R. Seeja, "IoT based smart campus," in *Proc. Int. Conf. Innov. Control, Commun. Inf. Syst. (ICICCI)*, Grater Noida, India, Aug. 2017, pp. 1–4.
[41] G. Sun, Y. Zhou, and J. Li, "Build smart campus using human behavioral data," in *Proc. Int. IEEE Conf. Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People, Smart World Congr. (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, Toulouse, France, Jul. 2016, pp. 133–136.
[42] M. Ro, R. Swathi, M. Sneha, S. Kotian, and N. Rao, "An IoT based smart campus system," *Int. J. Sci. Eng. Res.*, vol. 9, no. 4, pp. 146–151, Apr. 2018.
[43] Y. Huang, C. White, H. Xia, and Y. Wang, "A computational cognitive modeling approach to understand and design mobile crowdsourcing for campus safety reporting," *Int. J. Hum.-Comput. Stud.*, vol. 102, pp. 27–40, Jun. 2017.
[44] A. Abdullah, M. Thanoon, and A. Alsulami, "Toward a Smart campus using IoT: Framework for safety and security system on a university campus," *Adv. Sci., Technol. Eng. Syst. J.*, vol. 4, no. 5, pp. 97–103, Sep. 2019.
[45] K. Phougat, M. Sinha, S. Pruthi, and S. B. Wakurdekar, "An IoT approach for developing a smart campus," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 5, no. 4, pp. 7405–7412, Apr. 2017.
[46] V. L. Uskov, J. P. Bakken, S. Karri, A. V. Uskov, C. Heinemann, and R. Rachakonda, "Smart university: Conceptual modeling and systems' design," in *Proc. Int. Conf. Smart Educ. Smart E-Learn. (SEEL)* (Smart Innovation, Systems and Technologies), vol. 70, V. Uskov, J. Bakken, R. Howlett, and L. Jain, Eds. Cham, Switzerland: Springer, 2018, pp. 49–86.
[47] L. Wang, K. Li, and X. Chen, "Internet of Things analysis of smart campus," in *Proc. Int. Conf. Cloud Comput. Secur. (ICCCS)* (Lecture Notes in Computer Science), vol. 11067, X. Sun, Z. Pan, and E. Bertino, Eds. Cham, Switzerland: Springer, 2018, pp. 418–428.
[48] K. U. Sarker, A. B. Deraman, R. Hasan, S. Mahmood, A. Abbas, and M. Sohail, "Kids' smart campus ontology to retrieve interest," in *Proc. 4th MEC Int. Conf. Big Data Smart City (ICBDSC)*, Muscat, Oman, Jan. 2019, pp. 1–4.
[49] F. Concone, P. Ferraro, and G. Lo Re, "Towards a smart campus through participatory sensing," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Taormina, Italy, Jun. 2018, pp. 393–398.
[50] B. Gao, F. Liu, S. Du, and F. Meng, "An OAuth2.0-based unified authentication system for secure services in the smart campus environment," in *Proc. Int. Conf. Comput. Sci. (ICCS)* (Lecture Notes in Computer Science), vol. 10862, Y. Shi, Ed. Cham, Switzerland: Springer, 2018, pp. 752–764.
[51] A. Z. Abbasi and Z. A. Shaikh, "Building a smart university using RFID technology," in *Proc. Int. Conf. Comput. Sci. Softw. Eng.*, Hubei, China, 2008, pp. 641–644.

[52] L. Zhang, O. Oksuz, L. Nazaryan, C. Yue, B. Wang, A. Kiayias, and A. Bamis, "Encrypting wireless network traces to protect user privacy: A case study for smart campus," in *Proc. IEEE 12th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, New York, NY, USA, Oct. 2016, pp. 1–8.

[53] J. E. Ferreira, J. A. Visintin, J. Okamoto, and C. Pu, "Smart services: A case study on smarter public safety by a mobile app for University of São Paulo," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, San Francisco, CA, USA, Aug. 2017, pp. 1–5.

[54] W. V. Ch, X. P. Pacheco, and S. L. Mora, "Application of a smart city model to a traditional university campus with a big data architecture: A sustainable smart campus," *Sustainability*, vol. 11, no. 10, p. 2857, May 2019.

[55] S. Arshad, M. A. Azam, S. H. Ahmed, and J. Loo, "Towards information-centric networking (ICN) naming for Internet of Things (IoT) the case of smart campus," in *Proc. Int. Conf. Future Netw. Distrib. Syst. (ICFNDS)*, Cambridge, U.K., vol. 2017, pp. 1–6.

[56] Z. Tian, Y. Cui, L. An, S. Su, X. Yin, L. Yin, and X. Cui, "A real-time correlation of host-level events in cyber range service for smart campus," *IEEE Access*, vol. 6, pp. 35355–35364, 2018.

[57] M. E. Beqqal, M. A. Kasmi, and M. Azizi, "Access control system in campus combining RFID and biometric based smart card technologies," in *Europe and MENA Cooperation Advances in Information and Communication Technologies* (Advances in Intelligent Systems and Computing), vol. 520, A. Rocha, M. Serrhini, and C. Felgueiras, Eds. Cham, Switzerland: Springer, 2016, pp. 559–569.

[58] H. Pinggui and C. Xiuqing, "Design and implementation of campus security system based on Internet of Things," in *Proc. Int. Conf. Robots Intell. Syst. (ICRIS)*, Huai'an, China, Oct. 2017, pp. 86–89.

[59] S. Y. Nikouei, Y. Chen, S. Song, R. Xu, B.-Y. Choi, and T. Faughnan, "Smart surveillance as an edge network service: From harr-cascade, SVM to a lightweight CNN," in *Proc. IEEE 4th Int. Conf. Collaboration Internet Comput. (CIC)*, Philadelphia, PA, USA, Oct. 2018, pp. 256–265.

[60] L. W. Chen, T. P. Chen, D. E. Chen, J. X. Liu, and M. F. Tsai, "Smart campus care and guiding with dedicated video footprinting through Internet of Things technologies," *IEEE Access*, vol. 6, pp. 43956–43966, 2018.

[61] K. Liu, N. Warade, T. Pai, and K. Gupta, "Location-aware smart campus security application," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, San Francisco, CA, USA, Aug. 2017, pp. 1–8.

[62] L. Zheng, C. Song, N. Cao, Z. Li, W. Zhou, J. Chen, and L. Meng, "A new mutual authentication protocol in mobile RFID for smart campus," *IEEE Access*, vol. 6, pp. 60996–61005, 2018.

[63] D. E. Popescu, M. F. Prada, A. Dodescu, D. J. Hemanth, and C. Bungau, "A secure confident cloud computing architecture solution for a smart campus," in *Proc. 7th Int. Conf. Comput. Commun. Control (ICCCC)*, Oradea, Romania, May 2018, pp. 240–245.

[64] E. Alimpertis, A. Markopoulou, C. Butts, and K. Psounis, "City-wide signal strength maps: Prediction with random forests," in *Proc. World Wide Web Conf. (WWW)*, San Francisco, CA, USA, 2019, pp. 2536–2542.

[65] D. Goel, E. Kher, S. Joag, V. Mujumdar, M. Griss, and A. K. Dey, "Context-aware authentication framework," in *Mobile Computing, Applications, and Services (MobiCASE)* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 35, T. Phan, R. Montanari, and P. Zerfos, Eds. Berlin, Germany: Springer, 2010, pp. 16–41.

[66] Z. Yu, Y. Liang, B. Xu, Y. Yang, and B. Guo, "Towards a smart campus with mobile social networking," in *Proc. Int. Conf. Internet Things 4th Int. Conf. Cyber, Phys. Social Comput.*, Dalian, China, Oct. 2011, pp. 162–169.

[67] T. Anagnostopoulos, "Spatiotemporal authentication," E.U. Patent 17 172 573.2, Nov. 3, 2020.

[68] T. Anagnostopoulos, "Spatiotemporal authentication," U.S. Patent 15 976 517, Nov. 3, 2020.

[69] N. Bazhenov and D. Korzun, "Event-driven video services for monitoring in edge-centric Internet of Things environments," in *Proc. 25th Conf. Open Innov. Assoc. (FRUCT)*, Helsinki, Finland, Nov. 2019, pp. 47–56.

[70] D. Korzun, E. Balandina, A. Kashevnik, S. Balandin, and F. Viola, *Ambient Intelligence Services in IoT Environments: Emerging Research and Opportunities*. Hershey, PA, USA: IGI Global, Jun. 2019, pp. 1–199.

[71] A. Hassani, A. Medvedev, P. D. Haghighi, S. Ling, M. Indrawan-Santiago, A. Zaslavsky, and P. P. Jayaraman, "Context-as-a-service platform: Exchange and share context in an IoT ecosystem," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Athens, Greece, Mar. 2018, pp. 385–390.

[72] O. Bates and A. Friday, "Beyond data in the smart city: Repurposing existing campus IoT," *IEEE Pervas. Comput.*, vol. 16, no. 2, pp. 54–60, Apr. 2017.

[73] A. Rimboux, R. Dupre, E. Daci, T. Lagkas, P. Sarigiannidis, P. Remagnino, and V. Argyriou, "Smart IoT cameras for crowd analysis based on augmentation for automatic pedestrian detection, simulation and annotation," in *Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, Santorini, Greece, May 2019, pp. 304–311.

[74] Y.-C. Chang and Y.-H. Lai, "Campus edge computing network based on IoT street lighting nodes," *IEEE Syst. J.*, vol. 14, no. 1, pp. 164–171, Mar. 2020.

[75] M. Alvarez-Campana, G. Lopez, E. Vazquez, V. A. Villagra, and J. Berrocal, "Smart CEI Moncloa: An IoT-based platform for people flow and environmental monitoring on a smart university campus," *Sensors*, vol. 17, no. 12, p. 2856, Dec. 2017.

[76] P. Kulkarni, Q. O. A. Hakim, and A. Lakas, "Experimental evaluation of a campus-deployed IoT network using LoRa," *IEEE Sensors J.*, vol. 20, no. 5, pp. 2803–2811, Mar. 2020.

[77] X. Xu, D. Li, M. Sun, S. Yang, S. Yu, G. Manogaran, G. Mastorakis, and C. X. Mavromoustakis, "Research on key technologies of smart campus teaching platform based on 5G network," *IEEE Access*, vol. 7, pp. 20664–20675, 2019.

[78] C. Prandi, L. Monti, C. Ceccarini, and P. Salomoni, "Smart campus: Fostering the community awareness through an intelligent environment," *Mobile Netw. Appl.*, vol. 25, no. 3, pp. 945–952, Feb. 2019.

[79] V. Hassija, V. Chamola, V. Saxena, D. Jaim, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[80] P. I. Radoglou-Grammatikis, P. G. Sarigiannidis, and I. D. Moscholios, "Securing the Internet of Things: Challenges, threats and solutions," *Internet of Things*, vol. 5, pp. 41–70, 2018.

[81] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2671–2701, 3rd Quart., 2019.

THEODOROS ANAGNOSTOPOULOS was born in Athens, Greece, in 1976. He received the B.Eng. degree in computer engineering from the University of West Attica, Greece, in 1997, the B.Sc. and M.Sc. (IS) degrees in applied computer science from Athens University of Economics and Business, Athens, in 2001 and 2003, respectively, the Ph.D. degree in computer science from the National and Kapodistrian University of Athens, Athens, in conjunction with the University of Geneva, Switzerland, in 2012, and the M.Ed.Sc. degree in education sciences from Hellenic Open University, Greece, in 2018. He is currently a Lecturer (teaching) in computer science with the DigiT.DSS.Lab, Department of Business Administration, University of West Attica. He has worked in private and public sector as well as in industry and academia worldwide. He also has chase funding and involved in national and international academic research and industrial innovation projects. He holds two patents in U.S. and EU, where he is the inventor, while Intellectual Property (IP) is with Ordnance Survey: Great Britain's Mapping Authority, U.K.

PANOS KOSTAKOS received the B.A. degree (Hons.) in international relations and politics with economics from the University of the West of England and the Ph.D. degree from the Department of Politics, Languages and International Studies, University of Bath, U.K. He is currently a Research Scientist in the field of intelligence and security informatics at the Center for Ubiquitous Computing and a Lead Researcher with the Distributed Computing Research Theme of the 6G Flagship Research Program, University of Oulu, Finland. He is the Chair of the first UNODC Education for Justice (E4J) Winter School on Transitional Organised Crime and the 2019 European Intelligence and Security Informatics Conference (EISIC).

ARKADY ZASLAVSKY (Senior Member, IEEE) is currently a Professor of distributed systems and security at Deakin University, Melbourne, Australia. He is leading and participating in research and development projects in the Internet of Things, mobile analytics, and context-awareness science areas. He is also a Technical Leader of the EU Horizon-2020 Project bIoTope—building the IoT Open Innovation Ecosystem for connected smart objects. He holds adjunct-professorship appointments with a number of Australian and international universities, including UNSW, La Trobe University, University of Luxembourg, and ITMO University, St. Petersburg. He has published more than 400 research publications throughout his professional career and supervised to completion more than 40 Ph.D. students. He is a Senior Member of ACM and IEEE Computer and Communication Societies.

IOANNA KANTZAVELOU (Member, IEEE) received the B.Sc. degree in informatics from the Department of Informatics, Technological Educational Institute of Athens, the M.Sc. degree (research) in computer security from the Department of Computer Science, University College Dublin, National University of Ireland, and the Ph.D. degree on intrusion detection in information technology security from the Department of Information and Communication Systems Engineering, University of the Aegean. She is currently an Assistant Professor with the Department of Informatics and Computer Engineering, School of Engineering, University of West Attica. She has worked in research and development projects funded by Greek Government, Irish Government, and EU. Her published work includes chapters in books (IOS Press), conferences and journals, and recording remarkable citations in her research work. She is a member of Greek Computer Society (GCS), ACM, and IEEE Computer Society. She has joint editorship of three IOS Press collections. She has been a Repetitive Reviewer in many international conferences, such as ACM SEC, IEEE TrustCom, IFIP SEC, ESORICS, and IEEE CIS. She is currently a reviewer for high ranking journals, such as IEEE, Elsevier, Springer, and Emerald.

NIKOS TSOTSOLAS received the Diploma degree in production engineering and management, the M.Sc. degree in operational research, and the Ph.D. degree in statistical science. Since 1995, he has been working as an Independent Consultant in the field of design and implementation of information technology and business process reengineering. He is currently an Assistant Professor at the Business and Administration Department, University of West Attica. He has published over 90 research papers and studies in scientific journals, international conferences, and edited volumes. He is active in the fields of logistics, operational research, and decision support systems. He has worked with numerous organizations and businesses in Greece, Denmark, and Ireland. He has been a member of the Board of Directors of Hellenic Operations Research Society, since 2007.

IOANNIS SALMON received the Ph.D. degree in change management and human resource development from the National and Kapodistrian University of Athens. He is currently an Assistant Professor of business administration with the University of West Attica. He is the author or coauthor of articles in prestigious international journals and conference proceedings. He has participated in a number of European and national research programs. His research interests include information and communication technologies (ICT)-enabled change management, computer-aided human resource development, and digital knowledge representation management for strategic business.

JEREMY MORLEY has been the Chief Geospatial Scientist at Ordnance Survey, since 2015. He has been working in geospatial research since the mid-90s, starting in environmental Earth observation and radar mapping. From this, he progressed into geographic information science, focusing on crowd-sourcing and citizen science, open and interoperable geographical information services, and applications of geospatial science, working at University College London and then the University of Nottingham. At Ordnance Survey, he leads the Research Team, focusing on commissioning, planning, and executing research projects with external partners, particularly universities, promoting active knowledge transfer and horizon scanning to identify new business opportunities and emerging research.

ROBERT HARLE received the bachelor's degree from Downing College, Cambridge. He is currently a Senior Lecturer at the Computer Laboratory, University of Cambridge, U.K. His research interests include all forms of sensing, but particularly where mobile and wearable systems are involved. He has published extensively in the fields of indoor positioning, context-awareness, and ubiquitous computing. He is a fellow at the Downing College, where he is currently the Dean. He is also a Bye-Fellow at Fitzwilliam College. He received Pilkington Prize for excellence in teaching, in 2016.