# Spatiotemporal Authentication System Architecture for Smart Campus Safety

Theodoros Anagnostopoulos
*DigiT.DSS.Lab*
*Department of Business Administration*
*University of West Attica*
Athens, Greece
Theodoros.Anagnostopoulos@uniwa.gr

Panos Kostakos
*Center for Ubiquitous Computing*
*University of Oulu*
Oulu, Finland
panos.kostakos@oulu.fi

Ioannis Salmon
*Department of Business Administration*
*University of West Attica*
Athens, Greece
isalmon@uniwa.gr

Yannis Psaromiligkos
*DigiT.DSS.Lab*
*Department of Business Administration*
*University of West Attica*
Athens, Greece
yannis.psaromiligkos@uniwa.gr

Klimis Ntalianis
*Department of Business Administration*
*University of West Attica*
Athens, Greece
kntal@uniwa.gr

S.R. Jino Ramson
*VIT Bhopal University*
Bhopal, India
jinoramson@gmail.com

***Abstract*— A Smart Campus is a protected area within Smart Cities (Cities 2.0) where physical security of assets is vital for the continuous operation of the university. Concretely, there are specific mission-critical areas on the campus, which should be protected from unauthorized and malicious individuals. This paper describes a sustainable Smart Campus system architecture based on individuals' spatiotemporal authentication fingerprint, generated by fusing data from mobile GPS devices and CCTV cameras infrastructure to detect malicious user behavior. The system incorporates unobtrusive monitoring to collect data from such individuals. While the system monitors for unauthorized access to restricted locations within the campus area, data are analyzed by an intrusion detection algorithm that sets off alarms and prompts physical evacuation. The efficiency of the proposed system is evaluated by gauging the prediction accuracy of alarms triggered and response time to the actual incidents on the campus. Results are promising for the adoption of the proposed system architecture by universities in Cities 2.0.**

***Keywords—Smart Campus, IoT, Security, Spatiotemporal Authentication, Intrusion Detection***

## I. Introduction

The Smart Campus concept is an innovative testbed within Smart Cities (Cities 2.0) where human behavior can be examined thoroughly without posing operational problems on the daily schedule of city life [1]. The physical security of Internet of Things (IoT) is fundamental in a living area such as a university Smart Campus, which should be examined in more depth [2]. Specifically, critical areas and zones should be defined, which will protect sensitive assets of campus area such as the computer network administration and server room, Heating Ventilation and Air Conditioning (HVAC) temperature management system, electrical power supply centre, etc. To achieve this, prior works on Smart Campus architectures have proposed specific security mechanisms, such as authentication and Intrusion Detection Systems (IDSs) and a variety of safety countermeasures like anonymization, data encryption, biometrics and network monitoring [3].

In this paper, we incorporate a system architecture based on spatiotemporal authentication fingerprint, as invented by the authors in [4] and [5], where a user is assigned a facial photo and a mobility trace when entering the campus premise. The Smart Campus testbed, which will provide synthetic data to the system, is the campus of the University of West Attica, Greece. A mobile app is required for a user to enter the university, which takes their photo and assigns it to the user profile. In addition, users give consent that the university traces their mobile device for as long as they are physically located on campus. The system can detect users unobtrusively by logging their behavior in certain time periods while visiting the university campus. When malicious activity is detected, the system sets an intrusion detection alarm and passes the control to the safety personnel guards of the campus for physical evacuation from the specific university area.

The rest of the paper is structured as follows. Section II presents the prior work in Smart Campus security. The proposed system architecture for unobtrusive monitoring of the campus is described in Section III. In Section IV, analyzes the intrusion detection algorithm used for setting an alarm for physical evacuation of certain areas as well as passing control to physical security personnel. Research experiments with regards to prediction accuracy of an alarm as well as time to response in an actual threat are presented in Section V. Section VI, discusses the observed results. Finally, Section VII concludes with proposed future work in the filed of Smart Campus safety.

## II. Prior Work

Smart Campus safety is an area that has drawn increased attention from both researchers and practitioners in recent years. Specifically, suspicious user traces are fingerprinted by an ant colony system which enables recognition of malicious activity, while a Convolution Neural Network (CNN) was trained to recognize malevolent behavior of unauthorized individuals, which then triggers specific responses to mitigate the security risk [6]. Alerting capabilities can enable accurate event prediction when users are equipped with mobile devices, such as smartphones or tablets. A challenging issue is delivering alerts and warning messages to individuals on campus when a security alert has been raised [7]. Students are monitored unobtrusively to balance between privacy and basic freedoms and human rights. Specifically, current ethical and legal requirements dictate that students should be aware that they are being monitored to provide well-being in their working place [8]. A participatory sensing model, which incorporates smartphone potentiality, collects, and analyses student data for user profiling. Such a system can detect

This work has financially supported by the course of Advanced Quantitative Statistical Analyses, Master of Business Administration (MBA), Department of Business Administration, University of West Attica, Athens, Greece.

students' malicious actions during their accommodation to the campus [9].

RFID technology is also applied to university premises to provide a robust Smart Campus infrastructure. The system can consider electrical equipment's maintenance services to track malicious activity in the campus [10]. Public safety intrusion detection system has been used to track student's mobile equipment and set a warning in case of an emergency. The system incorporates CCTV cameras for space monitoring, focusing on remote campus areas [11]. A Smart Campus monitoring system, which incorporates both RFID and GPS technologies, is used to promote well-being of the student population. Such system also exploits the potentiality of IoT and smartphones for unobtrusive surveillance purposes [12]. A Smart Campus surveillance system, based on context-aware spatiotemporal authentication fingerprint for assuring university physical security, is proposed by authors in [13], based on the exploitation of the patented system presented in [5]. Specifically, the system in [5] is inferred as the optimal weighted scoring research effort compared with other contemporary efforts proposed in [13]. In such system sensitive information is provided by IoT technology being ubiquitous in the university campus.

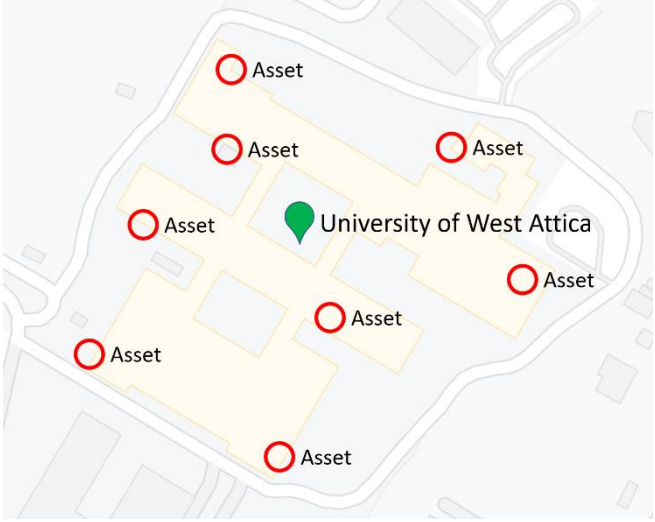


Fig. 1. Annotated campus map with asset locations and geofences.

Current research in surveillance systems dictates that although certain technical solutions are designed and provided for adaptation in contemporary Smart Campus area, there is a lack of a robust architecture system that will orchestrate all the research findings towards a sustainable surveillance system for universities. In this paper, the importance of a highly scored system architecture as provided in [5], will be demonstrated by applying a surveillance infrastructure of GPS devices and CCTV cameras technology to synthetic data provided by the University of West Attica, Greece. The efficiency of the proposed system is evaluated by applying prediction accuracy and time to response metrics on incidents occurred during the synthetic system operation.

## III. System Architecture

The surveillance system proposed in [5] is applied for conceptual experimental use at the University of West Attica, Greece campus. Thus, this is a synthetic example based on actual and simulated data sources since such a system does not really exist in the university. The system should be able to protect certain areas, like the following, to name a few:

- Centre of computer network administration
- Buildings' temperature management center
- Remote areas within buildings
- Car parking remote areas
- Electrical power supply centre
- Water grid supply centre
- Fuel management centre
- Restaurant storage centre

The university assets are protected passively by assigned certain digital passive spatial geofences around their area of coverage. Such information is also encoded in the system's knowledge base and invoked in case of a match with a possible detection of illegal behavior. The passive geofence is defined as a circle with center, $c$, which is the reference point of the asset and a radius, $r$, which is the safe distance that a user should be away from the asset. The geofence is characterized as passive because it does not provide feedback to the system in case of a violation, but rather the system should compute the relative position of the user and the geofence, and in case of an intrusion, an alarm should be set. Euclidean representation of the geofence's protected coverage area, $E$, is defined to be the area of the following circle:

$$E = \pi \cdot r^2 \qquad (1)$$

An annotated map of the Smart Campus of the University of West Attica, Greece, along with the locations of certain passive geofences, is presented in Fig. 1.

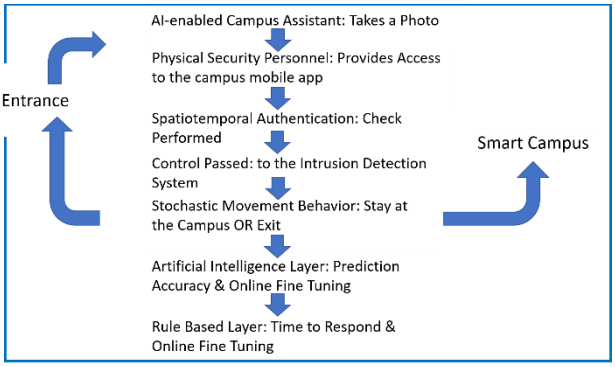


Fig. 2. Adopted system architecture authentication process.

The system should also update and protect such a list of sensitive assets with new unseen examples in the future. The core element of the system architecture active safety is the spatiotemporal fingerprint, which an individual has identically compared with other persons on the campus. This personal fingerprint is created by combining data streams from CCTV camera networks' video and GPS mobility trace within the campus as patented in [5]. An actor to enter the university has three discrete roles: verified personnel, student, or visitor. Specifically, to enter the university, an authentication system is established, which focuses on using an Artificial Intelligence (AI) – enabled campus assistant. The AI-enabled campus assistant takes a photo of each person wishes to enter the university. Consequently, security personnel at the university entrance kindly prompt the individual to download from the cloud and use the university's mobile app, taking a photo of the student. Then the photo of the user is double-checked with the photo taken from the AI-enabled campus assistant. If the two photos are matched and proved identical then the mobile app requires by the users to have their GPS sensor active for as long as they are located in the Smart Campus. The mobile app logs users' traces for future

stochastic movement analysis within the campus, and transmit them to the university cloud upon the exit of the user from the campus. Physical safety is then provided by incorporating an intrusion detection system to track the possible unlawful actions.

Concretely, at this stage, all categories of users can move within the campus. However, the system tracks their spatiotemporal context and moving behavior to provide prediction accuracy and time to the respond services in case of possible malicious action. Specifically, the following security level is to pass control to an AI layer, which monitors the users unobtrusively and triggers an alarm in case of a violation and provides the system's prediction accuracy. In addition, the system can get current output and feedback it in a loop to fine-tune the AI layer, thus improving its efficiency and accuracy. Subsequently, on system optimization, it follows a last safety rule-based layer, which is responsible for providing the system's time to respond in case of an attack and for updating this information to the system's knowledge base within a specific fine-tuning loop.

The proposed system architecture for the authentication process is shown in Fig. 2. The AI-enabled campus assistant has a prominent role in the architecture in providing the adopted system's first stage of spatiotemporal authentication defense.

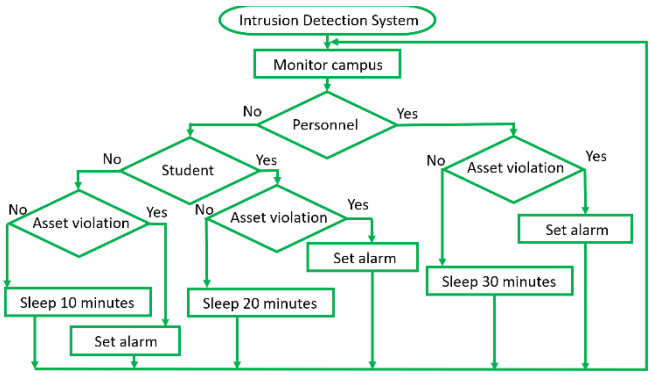


Fig. 3. Proposed intrusion detection system algorithm.

## IV. Intrusion Detection Algorithm

The proposed architecture focuses on the physical safety of the university, which is performed by unobtrusive monitoring of engaged individuals. An intrusion detection system is retrofitted that enables monitoring individuals on predetermines time intervals. Data gathered from the system are stored in the knowledge base for further use, such as matching real-time information with invoked stochastic data to trigger a security alert. However, such a monitoring system cannot be scaled horizontality to include many individuals, since it would cause loss of computational power due to state-space explosion of the physical objects being detected across the campus. To overcome such problem, users are classified in three separate classes, which are: (1) campus verified personnel, (2) an individual is a student at the university, and (3) a certain individual is a visitor of the university. Then the intrusion detection system monitors assigned personnel, students, and visitors at different temporal scales to avoid collapse of the surveillance system.

The system triggers a security alarm when an unauthorized user is detected within a prohibited zone. This is achieved in case the system chooses to actively awake on certain temporal scale trigger. On the occurrence of such a trigger, the system monitors an individual, either if she is a campus personnel or a student, or a visitor. The system is able to invoke the photo of the user from the university mobile app, check it with the photo captured by the nearest CCTV camera and also evaluate the GPS trace of the mobile phone to assure that the user fingerprint is verified. In this point, there is a change in control flow of the system. In case the system is triggered by a staff member it is checked if that user is within the spatial geofence allowed to be, and if not, then the alarm is actively set. In case the system is triggered by a student or a visitor an alarm is actively set at once.

When the alarm is set to true, the first action is that the targeted spatial area around the asset is evacuated immediately (i.e., building or car parking evacuation) according to clear directions given by campus speakers and assistance provided by the security personnel guards. The second action is to give the control to the security personnel for further investigation, which should be either to engage the individual in case of a human error (i.e., if it is proven to be a mistake), or to call the police for any subsequent lawful action.

The developed intrusion detection flow control algorithm is presented in Fig. 3, focusing on the classification of users to three discrete classes and the state-space control of the system in case of unlawful behavior.

## V. Experiments

The experimental section of the proposed architecture is evaluated with specific metrics, such as the systems' prediction accuracy of a true alarm versus a false alarm, which is examined as part of the AI layer of the architecture. Please recall that this layer performs stochastic self-optimization and follows in flow control the intrusion detection system and the movement behavior layer, which is responsible for monitoring the user activity. In addition, experiments also examine the system's rule-based layer and response time to an actual attack. This layer also has the potentiality to be self-optimized through experience, and it follows the AI layer in the stack hierarchy. Evaluation metrics are defined subsequently with their mathematical formulas.

### A. Evaluation metrics

- **Prediction accuracy**, $a$, is defined as a fraction with numerator the sum of true positive alarms, $t_p$, plus the true negative alarms, $t_n$, and denominator the sum of true positive alarms, $t_p$, plus false positive alarms, $f_p$, plus true negative alarms, $t_n$, plus false negative alarms, $f_n$. It is obvious that $a$ is a net number in the interval, $a \in [0,1]$, such as:

$$a = \frac{t_p + t_n}{t_p + f_p + t_n + f_n} \tag{2}$$

- **Time to respond**, $t$, is defined as the sum of sleep time period where the attack is performed, $p$, (i.e., time monitoring period the user has violated the passive spatial geofence, such information is stored in the knowledge base and get invoked when the system awakes) plus time period required by the system to set an alarm, $s$, such as:

$$t = p + s \tag{3}$$

### B. Performed experiments

To experiment with the proposed system, we accepted certain assumptions, such as the data incorporated in the research were generated by real data with the addition of Gaussian white noise to produce synthetic data streams [14]. White noise transforms the synthetic data distribution to be

composed of variables, which are independent and identically distributed with a mean zero. However, stochastic processes are composing the ground truth that the produced datasets are integrated due to the fact that these datasets are based on real data. Actually, this property of the stochastic data is required to test the trends of the synthetic data streams without loss of generality (i.e., by avoiding deterministic behavior). To perform accurate experiments and observe realistic results, certain parameters should be defined and fine-tuned.

TABLE I. EXPERIMENTAL PARAMETERS

| Parameter | Value |
|---|---|
| Smart Campus coverage area (square kilometers) | 62.58 |
| Number of entrances | 2 |
| Number of AI-enabled campus assistants | 2 |
| Number of assets | 8 |
| Coverage area of passive geofences (square meters) | 33.64 |
| Number of physical security personnel | 10 |
| Number of campus personnel | 412 |
| Number of students | 2508 |
| Number of visitors | 134 |
| Temporal monitoring period of personnel (minutes) | 30 |
| Temporal monitoring period of students (minutes) | 20 |
| Temporal monitoring period of visitors (minutes) | 10 |
| Alarm set temporal interval (minutes) | $(0, 1]$ |
| Number of repeated attacks experimental iterations | 1000 |

*1) System fine-tuning* assume that sleeping times of each separate category of users are initialized with certain temporal values within given intervals. Concretely, there is a training phase where these time variables are converged to almost constant values. Specifically, personnel sleep time, in minutes, is initialized in the interval $[20, 40]$, while students' sleeping time is within the interval of $[10, 30]$ minutes. In addition, sleeping time of visitors is initally set up in the following interval $(0, 20]$ minites. After the training phase for certain iterations of the experiment, such sleep times have converged in the following values: (1) personnel spleep time is set to 30 minutes, (2) student sleep time is set to 20 minutes, while (3) visitor sleep time is converged to 10 minutes. Subsequently, a time period required by the system to set an alarm after an asset violation is fine-tuned to take values within the interval $(0, 1]$ minutes. This time variance in latency is explained because of the system's workload, which may have an instant reaction or require some time to report the incident due to network traffic load of data transmission from the point of asset violation reference to the central system's server location.

*2) Experimental parameters* incorporated contain: (1) the total coverage area of the University of West Attica campus, (2) number of entrances to the campus, (3) number of AI-enabled campus assistants, (4) number of assets to be protected, (5) coverage area of spatial passive geofences, (6) number of physical security personnel, (7) number of campus personnel, (8) number of students, (9) number of visitors, (10) temporal monitoring period of personnel, (11) temporal monitoring period of students, (12) temporal monitoring period of visitors, (13) alarm set temporal interval, and (14) number of attack iterations the experiment repeated to minimize statistical error and bias of the synthetic data. Table I, presents the experimental parameters along with their assigned values to perform the experiments.

*3) Experimental results* of the prediction accuracy, $a$, are presented in Fig. 4. These results are performed with the invocation of AI layer when a malevolent behavior is tracked and the system is required to take further actions. In addition, it is presented the experimental outcomes of the time to respond, $t$, for the cases of personnel, students and visitors are presented in Fig. 5, Fig. 6, and Fig. 7, respectively. These experiments are performed with the involvement and self-optimization of the system's rule-based layer. Results are promising for the adoption of the proposed spatiotemporal system architecture by other Smart Campuses, aiming to provide unobtrusive safety and a sustainable ecosystems.

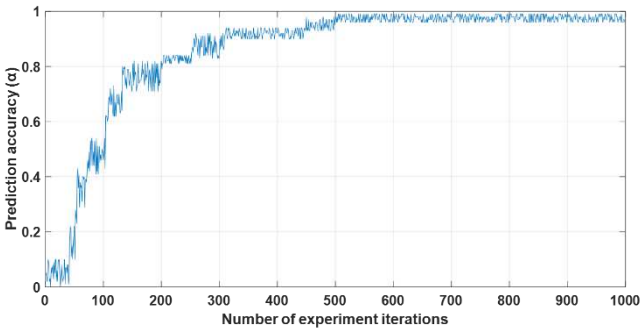


Fig. 4. Prediction accuracy of the system observed in the experiment.

## VI. DISCUSSION

In this section will be performed analysis and discussion on the observed experimental results. As presented in Fig. 4, prediction accuracy, $a$, is depicted as a curve, which in the initial experiment iteration is almost near to zero while in time passing increments progressively and after approximately $450^{th}$ repetitions, converges to values close to 1. This is explained because at the beginning of the experiments, there is no prior knowledge of malicious behavior at the system's AI layer, which is responsible for this action, thus leading the system to have low prediction accuracy values. Progressively, the factors of the fraction in Eq. 2 are learnt step by step until the system becomes more aware of the campus activity. Examining scholastically Eq. 2, it is revealed that the factors as trained as follows: (1) true positives, $t_p$, are expressed as the number of users who are proved to be malicious, (2) true negatives, $t_n$, is the quantity expresses that certain users is obvious to be legal, (3) false positives, $f_p$, is the number of users who although initially are judged as malicious, actually are proved to be legal, and finally (4) false negatives, $f_n$, is the quantity of the users initially judged to be legal however time passing is proved to be malicious. Actually, the last case of false negatives, $f_n$, is the most difficult to be proved since at first it seems there is no evidence by cameras instant snapshots to decide if a user is legal or malicious. However, due to the spatiotemporal authentication fingerprint attribute of the system it is performed stochastic analysis of data collected in the past (i.e., stored in the knowledge base) by processing and matching the places and temporal information of the subject being located recently, which provides the required evidence to make the correct decision regarding user's behavior.

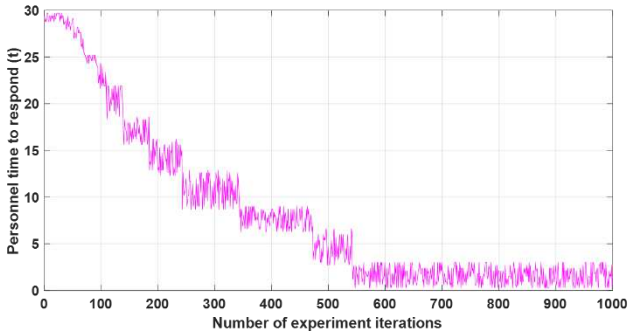


Fig. 5. Personnel time to respond achieved by observed system data.

Time to respond, $t$, results for personnel, students and visitors are presented in Fig. 5, Fig. 6, and Fig. 7, respectively, which is performed by the incorporation of the rule-based layer of the system. Please also recall from Eq. 3, that for all the user categories the alarm set time, $s$, is set in the interval $(0, 1]$ minutes, while time monitoring period, $p$, is varied according to certain user category. Specifically, in each figure, the temporal information can be observed, required by the system to respond to an upcoming attack (i.e., time to respond, $t$). Results observed in Fig. 5 can be explained as a snapshot of the time system requires to respond, $t$, for case of personnel users, which varies in the interval, $(0,30]$ minutes. Please note that the time to respond curve is decreasing from a maximum value of almost 30 minutes to values near zero. The curve converges after the $480^{th}$ experiment iteration, which means that the system is trained sufficiently to track malevolent behavior after this temporal point. In addition, it can be also observed that the curve of prediction accuracy is increased as the personnel time to respond curve is decreased, which is also a proof of the system's maturity. Moreover, the curve implies that the system can awake and monitor the GPS locations along with the photos of the personnel users and match this information with the passive geofence locations and the system's knowledge base. So, over time, if an attack is being performed it will be captured promptly to trigger the safety personnel guards for further assistance.

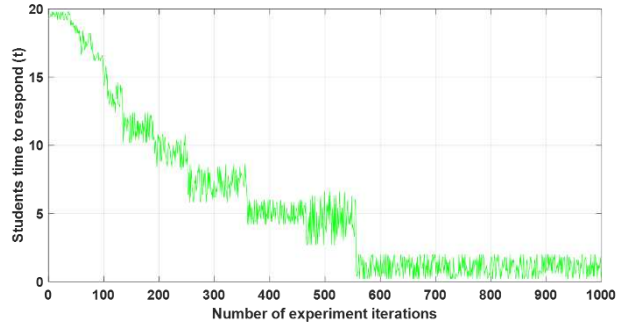


Fig. 6. Students population time to respond observed by the system.

Respectively, the same procedure is performed in the case of monitoring a student user, which is differentiated by the previous user category to the time required by the system to respond, $t$, to an upcoming attack shown in Fig. 6. Specifically, the system awakes and takes a snapshot of current student mobility in the campus while time interval is defined to be $(0,20]$ minites, which means that an attack might take place within that period. Also note that the time to respond curve is decreasing from a maximum value of almost 20 minutes to nearly zero values. In addition, the curve converges after the $460^{th}$ experiment iteration, which indicates that after that temporal value the system is trained sufficiently to capture illegal behavior. Subsequently, it can be observed that the curve of prediction accuracy is increased as the students time to respond curve is decreased, which is also an indication that the system converges in a stable condition. Additionally, the time to respond curve implies that the system awakes on time and monitors the GPS locations along with the student users' photos, and matches this information with the passive geofence locations and the system's knowledge base. Stochastically, the system is able to be proactive and in case that an attack might be performed it will be captured immediately by the safety personnel, which will process the event according to certain legal actions.

Subsequently, in Fig. 7 it is presented the behavior of the system on taking a snapshot of university physical traffic for the case of visitor users' category. Please note that the time to respond, $t$, by the system threshold in this case is within the interval, $(0,10]$ minutes, because visitors are monitored more strictly since they are not part of the campus personnel or even part of student population. Please note that the time to respond curve is decreasing from a maximum value of almost 10 minutes to values approaching zero. The curve converges after the $440^{th}$ experiment iteration, which indicates that after this temporal point the system is trained well to track malicious user behavior. Concretely, it can be observed that the curve of prediction accuracy is increased as the visitors time to respond curve is decreased, which is also an indication that the system is mature enough to transit from sleep to awake mode on time and monitor the GPS locations along with the photos of the visitor users while matching this information with the passive geofence locations and the knowledge base supported by the system's core software. On time passing if an actual attack is being tracked it will be treated appropriately by the system, which will pass the control to the safety personnel guards for consecutive legal actions.

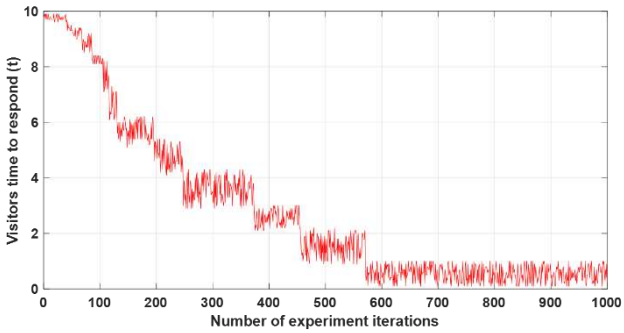


Fig. 7. Visitors time to respond achieved by the system's observation.

## VII. Conclusions and Future Work

Securing unobtrusively a Smart Campus infrastructure from inappropriate user action is a rational need, which is currently required by contemporary sustainable universities. In this paper, we used spatiotemporal authentication fingerprint data analytics as a key enabling technology to a support a certain secure system architecture. Such an architecture incorporates CCTV camera networks and GPS traces provided by users' mobile phones. On entrance to the campus, users are instructed through the expert physical security guards' personnel to: (1) take a photo of themselves by the AI-enabled campus assistants, and (2) download from the cloud the university's mobile app, which verifies their personal photo with their spatiotemporal data. Such data are provided on consent of the users to have their mobile phone's GPS sensors active for as long as they will be located in the campus. An unobtrusive surveillance system monitors the users either they are: (1) university personnel, (2) students, or (3) visitors. An intrusion detection system is proposed, which is able to infer if a user has legal or malicious behavior upon entrance to a passive spatial geofence. Prediction accuracy and

time to respond evaluation metrics are defined to measure the efficiency of the system. The system undergoes a fine-tuning phase to train the system parameters to be effective. Such parameters are trained by the AI layer and the rule-based layer of the infrastructure, which are responsible for the prediction accuracy convergence as well as the system's time to respond awareness of each users' category. Certain experiments have been performed to achieve optimal results in the area of user behavior tracking and prediction, based of spatiotemporal authentication fingerprint data sources stored in the systems knowledge base.

Future work focuses on adopting active spatiotemporal geofences, which will interact with the environment at their own pace in case of an emerging attack violation. Concretely, in current research, it is assumed that the attackers act for their own will without having any connection or even an attack plan shared between them. In the future asynchronous physical treats will be examined as part of an integrated malicious attack behavior to Smart Campus sensitive assets. Moreover, it will be analyzed and designed a series of AI-enabled prediction models to perform stochastic spatiotemporal inference on a larger scale of real malevolent incidents. Such AI-enabled applications will incorporate big data analytics' methods to deal with the vast amount of heterogeneous data sources generated within the university. Such models will also exploit the advantages of federated learning technology to achieve that surveillance code will be executed locally as well as distributedly in the edge of the campus network to reduce traffic data latency. Last but not least, the functionality of the system will be expanded by incorporating social networking engineering to capture illegal user activity from outside attackers and users who have not giving consent to authenticate lawfully like the other university's users (i.e., cases where malevolent users are not enter by the university gate but rather jump the physical fences or enter through holes or even enter the campus by any kind of physical and/or social camouflage). Such users are characterized by the avoidance to collaborate with the security personnel and by not giving consent to the AI-enabled campus assistants. These malicious actors will also use evasive methods against the Smart Campus mobile app use by the rest of the campus population to get legally assigned with an appropriate spatiotemporal authentication fingerprint. Such behavior is of great interest on providing observed research results to experts to study in more depth the phycological nature profile and activity of outlaw individuals in a well-being and green Smart Campus ecosystem.

## REFERENCES


[1] A. Abdullah, M. Thanoon, and A. Alsulami, "Towards a Smart Campus Using IoT: Framework for Safety and Security System on a University Campus", in Advances in Science, Technology and Engineering Systems Journal (ASTESJ), vol. 4, no. 5, pp. 97 – 103, September 2019.

[2] 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", in International Journal of Geo-Information, vol. 7, no. 385, pp. 1 – 29, Sepember 2018.

[3] O. Bates, and A. Friday, "Beyond Data in the Smart City: Repurposing Existing Campus IoT", in IEEE Pervasive Computing, vol. 16, no. 2, pp. 54 – 60, June 2017.

[4] T. Anagnostopoulos, "Spatiotemporal Authentication", E.U. Patent 17172573.2, Filled on: May. 23, 2017, E.U. Patent No. 3,407,232, Granted on: July. 28, 2021.

[5] T. Anagnostopoulos, "Spatiotemporal Authentication", U.S. Patent 15/976,517, Filled on: May. 10, 2018, U.S. Patent No. 10,824,713, Granted on: November. 3, 2020.

[6] T. Saba, A. Rehman, R. Latif, S. M. Fati, M. Raza, and M. Sharif, "Suspicious Activity Recognition Using Proposed Deep L4-Branched-Actionnet With Entropy Coded Ant Colony System Optimization", IEEE Access, vol. 9, pp. 89181 – 89197, June 2021.

[7] R. Hasan, R. Hasan, and T. Islam, "InSight: A Blietooth Beacon-based Ad-hoc Emergency Alert Syste for Smart Cites", in Proc. IEEE CCNC, Las Vegas, NV, USA, January 2021.

[8] L. Wang, C. Yao, Y. Yang, and X. Yu, "Research on a Dynamic Virus Propagation Model to Improve Smart Campus Security", in IEEE Access, vol. 6, pp. 20663 – 20672, Mar. 2018.

[9] F. Concone, P. Ferraro, and G. L. Re, "Towards a Smart Campus Through Participatory Sensing", in Proc. IEEE SMARTCOMP, Taormina, Italy, 2018, pp. 393 – 398.

[10] A. U. Rehman, A. Z. Abbasi, and Z. A. Shaikh, "Building a Smart University Using RFID Technology", in Proc. IEEE ICCSSE, Hubei, China, 2008, pp. 641 – 644.

[11] J. E. Ferreira, J. A. Visintin, J. Okamoto, and C. Pu, "Smart services: A case study on smarter public safety by mobile app for University of Sao Paulo", in Proc. IEEE SmartWorld-SCALCOM-UIC-ATC-CBDCom-IOP-SCI, San Francisco, CA, USA, 2017, pp. 1 – 5.

[12] H. Pinggui, and C. Xiuqing, "Design and Impementation of Campus Security System Based on Internet of Things", in Proc. IEEE ICRIS, Huai'an, China, 2017, pp. 86 – 89.

[13] T. Anagnostopoulos, P. Kostakos, A. Zaslavsky, I. Kantzavelou, N. Tsotsolas, I. Salmon, J. Morley, and R. Harle, "Challenges and Solutions of Surveillance Systems in IoT-Enabled Smart Campus: A Survey", IEEE Access, vol. 9, pp. 131926 – 131954, September 2021.

[14] R. M. Howard, "White noise: A time domain basis", in Proc. IEEE ICNF, Xi'an, China, 2015, pp. 1 – 4.