Acta Informatica Pragensia, 2015, 4(1): 44–51
DOI: 10.18267/j.aip.59
Peer-reviewed paper

Context Sources and their Processing in Company Security

Libor Měsíček*

Abstract

This article deals with the problem of critical employees' oversight. In the article is proposed set of processes which can with cooperation with Data Mining and Ambient Intelligence, in some cases, predict behaviour and movement of monitored objects/people based on reasoned context from set of different sources. The difference between prediction and observed reality can be evaluated and based on rules and gathered information about context can be taken action to prevent security breach and damages to the company. At the end a case scenario is presented which demonstrate behaviour of the system and possible options how the system can prevent damages to assets.

Keywords: Ambient Intelligence, Context, Security, Process, Surveillance, Security Management.

1 Introduction

Threats to the security of a company are as old as companies. In the past there were mainly threats in the form of physical document theft or destruction, information smuggling or selling to competitors or just a simple break into companies' building and stealing or damaging valuable equipment. The number of ways how to interact with the company to harm its position nowadays is much wider. Almost every company has to be connected to the Internet, has local network and servers with sensitive data which must be protected by encryption and in case of a security problem set of pre-set countermeasures.

Ko et al. (2011) pointed out that the weakest part of this chain remains human factor. We can observe similar situation in air traffic, simple data insertion by some office clerks or system administrators using simple passwords into critical company systems, the percentage of wrong action or entries is much higher than success rate of a modern aviation systems and OCR systems. Other connected problem is ontology linked with Ambient Intelligence, generation of device specific user interfaces, automatic code generation, application adaptation and code mobility (Preuveneers et al., 2004).

The main goal of this article is to demonstrate concept of combination of different sources of information to be able to identify context and also security level of an employee and according to this level take appropriate action. Presented model suggests a way how to use already widely spread technologies combined with new techniques to detect unusual behaviour of valuable employee with great importance to the company. The reason why

* Department of Informatics, Faculty of Science, J. E. Purkinje University,
Ceske mladeze 8, 400 96 Usti nad Labem, Czech Republic
✉ l.mesicek@ujep.cz

should this be done is to identify irregularities in the employees' actions and link them with possible security threats. This set of processes could be also used to evaluate behaviour of wider group of employees in order to increase level of security in the company and its ability to defend critical systems. Context aware devices and systems can provide additional layer of security and can add new function into the system.

2 Materials and Methods

Method of analysis and synthesis is mainly used in this article accompanied by Data Mining and Ambient Intelligence. Context in human-computer interaction can be defined from several points of view (e.g. Positivist and phenomenal, location awareness of a device, etc.). Daunish (2004, pp. 19-30) deals with different perspectives related with context definitions. In this article, context will be used as awareness of intentions, plans, situation of a user of the system and his or her needs, probable situation and limitations (e.g. geographical, physical) based on his or her current location and other limitations. Urban theory and use of sensors are described in (Rabari & Storper, 2015).

The idea of analysing user history and creating his or her profile based on it and use them to provide personalized services is mentioned in (Hong, 2009). Proposed processes consist of three steps. First step of the process is data and information collection from different sources. These sources can differ according to the needs of company and purpose of the surveillance. Second step is data evaluation, searching for patterns and prediction of behaviour and movement through space. Last step is comparison of created patterns and information which comes from information sources and searching for important deviation from standard and probable behaviour.

3 Results and Discussion

To be able to construct intelligent system which could detect patterns of the employee it is necessary to have sufficient amount of information from the environment, public information systems or employees' work schedule.

Table 1 shows list of important information inputs used in particular model scenario. Also, inputs connected with Intrusion Detection Systems could be used (Vokorokos, Balas & Mados, 2012). We can see that most of the inputs are linked to companies' environment. Information and metadata from the companies' information systems is important and still underestimated source of knowledge which can be used for several purposes Mesicek and Svoboda (2012).

ID	Input name	Description	Information source	Typical delay of detection
1	Entrance system	Systems based on NFC or RFID technology used for identification of presence of employees ID Card.	Internal system of a company	< 1second
2	Surveillance cameras	Processed information from surveillance cameras around and inside companies' buildings with car ID recognition.	Internal system of a company	<1 second
3	Public transport information system	Information about delays of public transportation system and traffic jams and alternative roads.	Public information systems API	< 5 minutes
4	Employees' work schedule	Employees work schedule with planned meetings, vacations and other important events.	Internal system of a company	N/A
5	Phone	Information about position of employees ' phone, use of auto check-in.	Internal system of a company / API of a third party application	<1 minute
6	Facial expression analysis	Surveillance cameras can not only detect presence of a person but also recognise mood of a person in our case fear or pain (Xu et. al., 2014).	Internal system of a company	<1 minute

Tab. 1. *List of inputs used in the scenario to establish context of employees' behaviour and selected objects. Source Author.*

Information from these sources is transformed in process shown on Figure 1. Difficulty of transformation differs based on particular type of information source. Information from public sources about delays of trains, traffic jams, etc. can be usually use as is, but pictures from cameras must be processed by specialized software and methods (Xu et. al., 2014), after that the output can be used to identify required parameters, e.g. presence of car owned by employee or a human face expression.

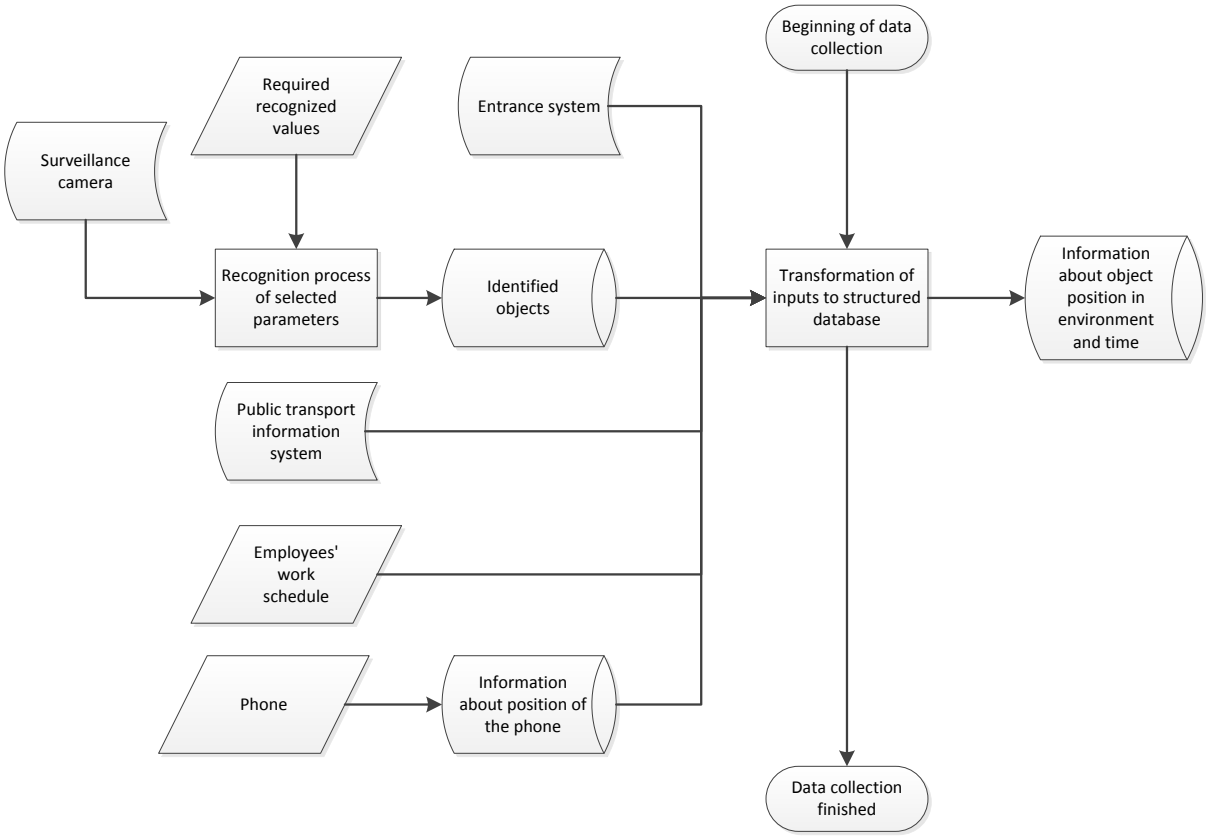

Fig. 1. *Process of inputs procession and insertion to object time database. Source Author.*

In the database of objects we must keep at least information about object ID, name, position, time, category of record (whether is it estimated position, e.g. planned meeting of the employee next week at a restaurant or position of the object in the past or present).

Once is available information where selected object were, where they are and where some of them should be in the future it is possible to use Data Mining and Ambient Intelligence to reason current security status of the employee.

Result of this step should provide information about the usual behavior, its probability distribution in time, patterns of movement and interaction with companies' information systems. Figure 2 briefly describes process of this reasoning.

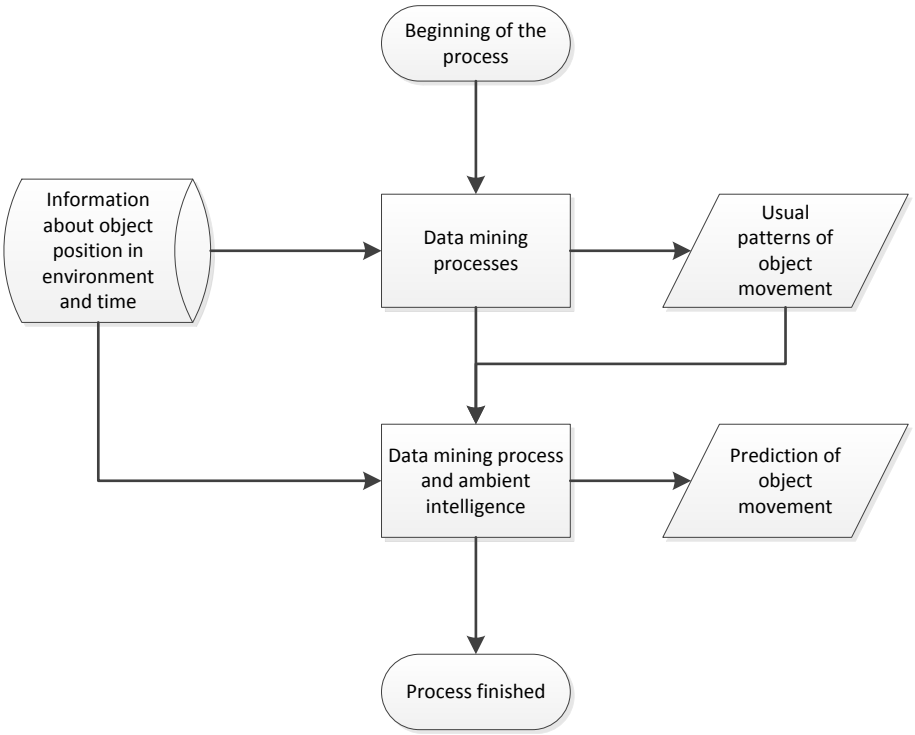

Fig. 2. *Use of gathered information for reasoning patterns and prediction of future movement. Source Author.*

Example of the output should be information that employee arrives to work by his car on Mondays between 8:35 and 8:45 with probability of 0.7. When there is traffic jam at particular part of his route from home he will arrive with 15 minutes delay with probability of 0.6. On Tuesdays he usually uses a train because of regular heavy jams and the train is usually five minutes delayed on arrival (but we can use Public information system with information about current delay of used train), then he has to walk for five minutes, so on Tuesdays his probable arrival is from 8:45 to 8:50 with 0.8 probability, but if he has any planned work meeting in the city center he will arrive after the meeting is finished (this can be checked in his calendar and scheduled meetings).

Once we have information about usual patterns of movement and interaction of selected employee we can use it for prediction of his or her behavior, and the most importantly potentially dangerous situations.

The success rate of the prediction should be measured in short- and mid-term.

$$success\ rate = \frac{number\ of\ successfull\ predictions}{number\ of\ all\ prediction} \times 100\% \qquad \textbf{(1)}$$

We can easily find out that some employees keep their routines almost perfectly, but some behave unexpectedly and this way of security oversight cannot be applied on them (this group has usually free work hours or can work from remote places).

For group of employees which tend to behave according model prediction is possible to use security level setting according how they behave in real world and what is the usual behavior.

Process of comparison is described at Figure 3.

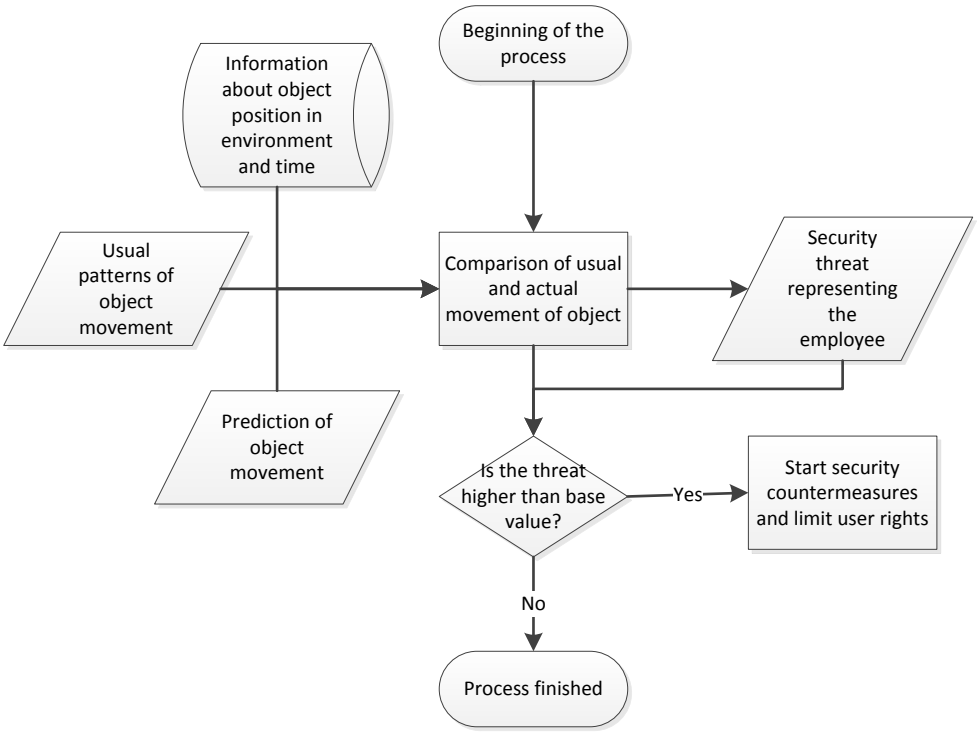

Fig. 3. *Comparison process of predicted and actual behavior and security threat level evaluation of current employee. Source Author.*

In case there is unusual movement, actions or difference between detected positions of companies' employee and his or her phone and ID card there should be started security countermeasures to prevent damages caused by possible, and in this case probable, stolen or forgotten phone and ID card. For example, there is information from the phone that it's moving along the train tracks but the employee should have left the train several train stops before these stations and his ID card was used recently to open his office. Conclusion of the system should be that either the employee is in the train and his ID card was stolen or the employee is in his office and he just lost his phone. Neither of these options is safe. The first one requires lock down of all endangered systems and presence of security guard or police in employees' office to detain possible burglar. The second described option requires silent remote locking and encrypting the content of the phone and preventive suspension of access to the information system. Set of sources of information and reaction can be of course much wider, it depends on companies' needs, requirements and options.

4 Conclusion

Context has become one of important parts of modern information systems. People use smart devices (e.g. power cords, fridge, watch, wrist band or mobile phone whit shared calendar and personal data) and some of them carry everywhere they go. We are observed by cameras, have RFID chips in our wallets and this all could be used as relatively cheap source of information about our behaviour and plans. Once we have these sources we can apply Ambient Intelligence and other methods and tools to reason probable behaviour of one specific person. Purpose of this article is to introduce concept of resources combination and its use for companies' security improvement.

Presented processes show example how to harvest selected sources of information and how to use them to prevent unwanted situation regarding companies' security. It is important to

detect undesired situations to improve critical companies' systems level of security and apply sufficient countermeasures.

Brief example showed one possible scenario how could be used detection of situation context. Presented scenario shows that it is feasible to reason information about employees based on mix of available data sources. After the information is compared with behaviour patterns, probability distribution, predictions etc. with certain reliability could be possible to say what the security threat the employee and his or her authorization rights could be.

Company which handles sensitive information with restricted access should implement algorithms which are able to track key employees (with theirs knowledge and agreement) and in case the company detects some abnormality (e.g. impossible speed of movement, unexplained access to dozens customers records, etc.) the action must be taken to prevent any additional damage.

References

Dourish, P. (2004). What we talk about when we talk about context. *Personal and Ubiquitous Computing*, 8(1), 19-30.

Hong, JY., Suh, EH., Kim, J., & Kim, S. (2009). Context-aware system for proactive personalized service based on context history. *Expert Systems with Applications,* 36(4), 7448-7457.

Ko, H., Marrieros, G., An, K., Vale, Z. Kim, T., & Choi, J. (2011). Contexts-Management Strategy with Security Consideration in Urban Computing based on urban design. In *2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing* (pp.65-72). Seoul: Korean Bible University.

Mesicek, L., & Svoboda, J. (2012). Composition of ICT Project Teams from Social Network Analysis Point of View. In *Proceedings of the 13th European Conference on Knowledge Management* (pp. 1462-1470). Cartagena.

Preuveneers, D., Van den Bergh, J., Wagelaar, D., Georges, A., Rigole, P., Clerckx, T., Berbers, Y., Coninx, K., Jonckers, V., De Bosschere, K. (2004). Towards an extensible context ontology for ambient intelligence. In Proceedings on Ambient Intelligence, (pp. 148-159). Eindhoven: Springer.

Rabari, C., & Storper, M. (2015). The digital skin of cities: urban theory and research in the age of the sensored and metered city, ubiquitous computing and big data. *Cambridge Journal of Regions Economy and Society*, 8(1) pp. 27-42.

Vokorokos, L., Balas, A., & Mados, B. (2012). Intrusion Detection Architecture Utilizing Graphics Processors. *Acta Informatica Pragensia,* 1(1), 50-59*.* doi: 10.18267/j.aip.5

Xu, C., Hu, Q. H., Xu, G. Q., & Feng, Z. Y. (2014). An approach to facial expression analysis with multi-model interactions. *International Journal of Computer Mathematics*, 91(11), 2329-2340.