Jožef Stefan Institute, Ljubljana, Slovenia

Jamova cesta 39, POB 3000, SI - 1001 Ljubljana, Slovenia / www.ijs.si
Tel.: +386 1 477 3900 / Fax: +386 1 453 5400

Center for technology transfer and innovation
Tel.: +386 1 477 3224, Fax.: +386 1 423 54 00; email: tehnologije@ijs.si

TECHNOLOGY OFFER

Intelligent High-Security Physical Access Control

that learns from experience to distinguish authentic entries from the impostor ones and to detect an unusual behaviour

Slovenian research institute has developed an intelligent access control system that learns from experience to distinguish authentic entries from the impostor ones and to detect an unusual behaviour of the regular users. The system improves efficiency of an arbitrary access control in surveillance and security demanding applications. Researchers are looking for partners interested in integration of the system into their products, joint further development and commercialization of the solution.

Aim of an arbitrary automated physical access control system is to restrict entrance to a certain room, building or a wider perimeter to authorized persons. Various access control systems include different types of credentials for the authorization such as PIN, access cards or biometrics (e.g. fingerprint). Different types of credentials have different levels of security and are suitable for different purposes. However, any of the known credentials (including biometrics) are prone to security vulnerabilities and can be breached quite easily once the security mechanism is figured out. For example, an arbitrary card based access control system does not recognize the obvious misuse of the credential of the unauthorized person (e.g. in case somebody uses the entry access card which belongs to other person or in case of a false verification of the identity by a biometric device such as fingerprint reader.

Our Intelligent High-Security Physical Access Control system learns from usual behaviour of the users and detects unusual (incorrect) entry or exit attempts. The used attributes for learning are for example, the time in the day, the specific day of the week, the specific date in relation to the month (e.g. each first Monday in a month) etc. Each date also relates to a specific user in a specific way – e.g. normal working days, vacations, reported sick leaves etc. The third relation deals with previous entries in a specific time period, e.g. the last hour or on each Monday. The data features include timing of entries of the person himself or in relation to any other access of any other person. For example, appropriate input data features and examples enable finding patterns such as person #1 and person #2 always enter at the same door inside a one minute
interval. Also the combination of entries at different doors (e.g. use of different access points) gives the system more information and therefore facilitates the verification of users.
To summarize: in contrast to an ordinary access control system, our system differentiates between "proper" access of "fit" employees and all other attempts of access, e.g. due to fake card, stolen identity or other security vulnerabilities of an arbitrary access control system.

Advantages / Invention

- detection of unusual user behaviour (entry/exit) by applying machine learning methods
- distinguishing of regular entries from faulty or fake ones (e.g. due to identity theft or security breach of a system)
- the system can be used as a stand alone application or as an add-on to an arbitrary access control system in surveillance and security demanding applications
- easy integration with existing security systems

- graphical representation of the results of unusual behaviour help security personnel to understand and efficiently fine tune the detection of an unusual behaviour
- easy integration with video surveillance systems in order to improve the efficiency and analysis of the captured events, e.g. each event can be easily analysed and properly treated
- possible implementation in time attendance systems (e.g. for detection of false evidence of working hours)

The system can be used as a stand alone application or as add-on to an arbitrary physical access control system or time attendance system (e.g. RFID card or biometric based) in surveillance and security demanding applications. The system can be easily integrated with video surveillance systems. The system ads anoother level of security and functionality to arbitrary existing access control systems.

The authors of the system are

internationally recognized experts in the fields of ambient intelligence, machine learning and data mining, language and speech technologies, computational intelligence and agent and multiagent systems.

Intellectual property

Secret know-how.

Stage of development

The solution has been field tested and integrated with a commercial of-the –shelf biometric access control system in a nuclear reactor facility with high-security demands.

Target sectors for commercialization / application

We are looking for:
- partners for further joint development, field testing and commercialization of the e-Dorman system.

- **partner able to further commercialize the system, potentialy connected with door and locking mechanisms producers** interested in integration of the system into their solutions or introduction of the solution as a new independent product on the market;
- companies with good contacts and business orientation in building construction industry, security system integrators and architecture companies, able to introduce the e-Dorman system as a niche security solution for homes and appartments.

CONTACT DETAILS

Robert Blatnik, M.Sc.
Center for Technology Transfer and Innovation,
Jozef Stefan Institute,
Jamova cesta 39, SI-1000 Ljubljana
http://tehnologije.ijs.si
Phone: +386 1 477 31 37
Fax: +386 1 251 39 85
E-mail: robert.blatnik@ijs.si