vyp.: Sistemnyy analiz, upravlenie i informatsionnye tekhnologii [Bulletin of the National Technical University "KhPI": a collection of scientific papers. Thematic issue: System analysis, management and information technology]. Kharkov, NTU "KhPI" Publ., 2015, no. 15(1124), pp. 106–111.

Надійшла (received) 09.12.2020

Відомості про авторів / Сведения об авторах / About the Authors

Нікуліна Олена Миколаївна (***Никулина Елена Николаевна***, ***Nikulina Olena Mykolaivna***) – д-р техн. наук, доцент, професор кафедри програмної інженерії та інформаційних технологій управління Національного технічного університету «Харківський політехнічний інститут», Харків, Україна; ORCID: https://orcid.org/0000-0003-2938-4215; e-mail: elniknik02@gmail.com

Северин Валерій Петрович (***Северин Валерий Петрович***, ***Severyn Valerii Petrovich***) – д-р техн. наук, професор, професор кафедри системного аналізу та інформаційно-аналітичних технологій Національного технічного університету «Харківський політехнічний інститут», Харків, Україна; ORCID: https://orcid.org/0000-0002-2969-6780; e-mail: severinvp@gmail.com

Коцюба Ніна Вікторівна (***Коцюба Нина Викторовна***, ***Kotsiuba Nina Viktorivna***) – асистент кафедри програмної інженерії та інформаційних технологій управління Національного технічного університету «Харківський політехнічний інститут», Харків, Україна.; ORCID: https://orcid.org/0000-0002-0017-7426; e-mail: kotsuba.nv@gmail.com

Никулина Елена Николаевна – д-р техн. наук, доцент, профессор кафедры программной инженерии и информационных технологий управления Национального технического университета «Харьковский политехнический институт», Харьков, Украина; ORCID: https://orcid.org/0000-0003-2938-4215; e-mail: elniknik02@gmail.com

Северин Валерий Петрович – д-р техн. наук, профессор, профессор кафедры системного анализа и информационно-аналитических технологий Национального технического университета «Харьковский политехнический институт», Харьков, Украина; ORCID: https://orcid.org/0000-0002-2969-6780; e-mail: severinvp@gmail.com

Коцюба Ніна Вікторівна (***Коцюба Нина Викторовна***, ***Kotsiuba Nina Viktorivna***) – ассистент кафедры программной инженерии и информационных технологий управления Национального технического университета «Харьковский политехнический институт», Харьков, Украина; ORCID: https://orcid.org/0000-0002-0017-7426; e-mail: kotsuba.nv@gmail.com

Nikulina Olena Mykolaivna – Doctor of Technical Sciences, Associate Professor, Professor of Department Software Engineering and Management Information Technologies National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0003-2938-4215; e-mail: elniknik02@gmail.com

Severyn Valerii Petrovich – Doctor of Technical Sciences, Professor, Professor of Department System Analysis and Information-Analytical Technologies National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0002-2969-6780; e-mail: severinvp@gmail.com

Kotsiuba Nina Viktorivna – Assistant of Department Software Engineering and Management Information Technologies National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0002-0017-7426; e-mail: kotsuba.nv@gmail.com

UDC 004.93 **DOI: 10.20998/2079-0023.2020.02.12**

K. S. KHABARLAK, L. S. KORIASHKINA

MOBILE ACCESS CONTROL SYSTEM BASED ON RFID TAGS AND FACIAL INFORMATION

RFID tags see a widespread use in modern security systems, including home intercoms, access control cards, contactless credit cards, biometric passports. Here we focus on a single application, namely access control systems. Currently they have either high cost or low security guarantees. Hence, the developments focusing on improving access control security while lowering the cost is a rapidly developing field. The purpose of this work is to create an alternative access control scheme, where card scanners are replaced with passive RFID tags, and all of the communication is done via user's smartphone Wi-Fi. Based on the analysis of existing approaches to the development of access control systems, it was concluded that use of mobile systems is the most promising due to their expandability and presence of a large number of sensors, such as NFC, camera etc. In the proposed model RFID tags are mounted near a turnstile or a smart door. Tag reading and programming is done via NFC chip directly on an Android or iOS mobile device, which allows for a significant price cut for such a system implementation. A detailed description of a tag writing procedure with the data required to perform it is provided. To enhance security, together with smartphone-based authorization we require the user to provide his photograph while entering a secure gate. The photograph is then displayed on a monitoring dashboard side-by-side with his registration picture, so that the two can then be matched against each other. The developed client-server application offers administrative system used to configure gate access policies and monitor entrances with filters by access time, user and gate. Besides that, we propose a mobile application that allows gate registration and serves as a door unlock key. The access control model that we suggest reduces installation costs required, as it is fully wireless and uses cheap autonomous RFID-tags as its main component. We expect the presented application to be easy in adaptation to customer needs and to existing security systems.

Keywords: access control system, RFID tags, NFC, mobile access control, security, person identification.

К. С. ХАБАРЛАК, Л. С. КОРЯШКІНА

МОБІЛЬНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ ІЗ ВИКОРИСТАННЯМ RFID МІТОК ТА ІНФОРМАЦІЇ ПРО ОБЛИЧЧЯ

У сучасних системах безпеки RFID-мітки використовуються всюди – у домофонах, пластикових картках систем контролю доступу, безконтактних кредитних картках, біометричних паспортах. У даній роботі ми сфокусуємо увагу на одному застосуванні – системах контролю доступу. Оскільки існуючи комерційні реалізації таких систем характеризуються або ж високою вартістю, або низьким рівнем безпеки, актуальним напрямком наукових досліджень в області комп’ютерних інформаційних технологій є розробки, що сприяють удосконаленню систем безпеки при одночасному їх здешевленні. Метою даної роботи є створення альтернативної схеми системи контролю доступу, у якій замість сканерів використовуються RFID-мітки, а для комунікації через Wi-Fi – тільки мобільний пристрій відвідувача. На основі результатів аналізу існуючих підходів до розробки систем контролю доступу та їх реалізацій, було зроблено висновок про те, що найбільш перспективним є використання мобільних систем в силу їх розширюваності та наявності великої кількості сенсорів – NFC, камера та ін. У запропонованій моделі системи контролю доступу RFID-мітки встановлюються стаціонарно біля турнікету або розумної двері. Програмування та читання міток відбувається чипом NFC мобільного пристрою на платформі Android або iOS, що дозволяє значно зменшити вартість впровадження такої системи. В роботі детально описано процедуру запису міток, а також використовувані при цьому дані. Разом із авторизацією за смартфоном, для забезпечення додаткової безпеки, фотографія користувача, зроблена при вході на фронтальну камеру мобільного пристрою, відображається на панелі моніторингу поряд із його фотографією під час реєстрації для порівняння. Розроблений клієнт-серверний додаток включає не тільки адміністративну систему для налаштування політик доступу до об’єктів та моніторингу із фільтрами за часом доступу, користувачу та двері із міткою, але й мобільний додаток, що дозволяє реєструвати об’єкти та є перепусткою для відкриття дверей. Запропонована модель мобільної системи контролю доступу дозволяє зменшити загальну ціну встановлення такої системи, оскільки вона є бездротовою та використовує недорогі автономні RFID-мітки. Крім того, архітектура розробленого програмного продукту забезпечує легку адаптацію до потреб підприємства або існуючих систем контролю доступу.

Ключові слова: система контролю доступу, RFID-мітки, NFC, мобільний контроль доступу, безпека, ідентифікація особи.

К. С. ХАБАРЛАК, Л. С. КОРЯШКИНА

МОБИЛЬНАЯ СИСТЕМА КОНТРОЛЯ ДОСТУПА С ИСПОЛЬЗОВАНИЕМ RFID МЕТОК И ИНФОРМАЦИИ О ЛИЦЕ

В современных системах безопасности RFID-метки используются повсеместно – домофоны, пластиковые карты систем контроля доступа, бесконтактные кредитные карты, биометрические паспорта. В данной работе мы сфокусируем внимание на одном применении – системах контроля доступа. Поскольку существующие коммерческие реализации таких систем характеризуются либо высокой стоимостью, либо низким уровнем безопасности, актуальным и активно развивающимся направлением научных исследований в области компьютерных информационных технологий являются разработки, способствующие усовершенствованию систем безопасности при одновременном их удешевлении. Целью данной работы является создание альтернативной схемы системы контроля доступа, в которой вместо сканеров используются RFID-метки, а для коммуникации через Wi-Fi – только мобильный телефон посетителя. На основе результатов анализа существующих подходов к разработке систем контроля доступа и их реализаций, был сделан вывод о том, что наиболее перспективным является использование мобильных систем в силу их расширяемости и наличия большого количества сенсоров – NFC, камера и др. В предложенной модели системы контроля доступа RFID-метки устанавливаются стационарно возле турникета или умной двери. Программирование и чтение меток производится чипом NFC мобильного устройства на платформе Android или iOS, что позволяет значительно уменьшить стоимость внедрения такой системы. В работе подробно описана процедура записи меток, а также используемые при этом данные. Вместе с авторизацией по смартфону, для обеспечения дополнительной безопасности, фотография пользователя, сделанная при входе на фронтальную камеру мобильного устройства, отображается на панели мониторинга рядом с его фотографией при регистрации для ее идентификации. Разработанное клиент-серверное приложение включает не только административную систему для настроек политик доступа к объектам и мониторинга с фильтрами по времени доступа, пользователю и двери с меткой; но и мобильное приложение, позволяющее регистрировать объекты и являющееся пропуском для открытия дверей. Предложенная модель мобильной системы контроля доступа позволяет уменьшить общую цену установки такой системы, так как является беспроводной и использует недорогие автономные RFID-метки. Кроме того, архитектура разработанного программного продукта обеспечивает легкую его адаптацию к потребностям предприятия или существующим системам контроля доступа.

Ключевые слова: система контроля доступа, RFID-метки, NFC, мобильный контроль доступа, безопасность, идентификация личности.

Introduction. Many of the modern enterprises use turnstiles or smart doors with access card scanners, where predominantly RFID cards are used. To provide extra security guarantees schools and universities also employ such systems as being cheap and easy to use. In the same time, they have a serious drawback, namely the card can be easily lost, which means an intruder can access the enterprise unnoticed, that in turn may cause critical consequences such as an accident, sensitive information loss etc. Installing video surveillance cameras may be a partial solution, which allows to detect such an access in a retrospect. However, storing video surveillance during a long timeframe may take a lot of disk space. The most efficient yet expensive approach to solving the problem is an installation of expensive biometric systems recognizing face or fingerprint (the latter can be recognized via the terminal or directly on a special access control card).

Using smartphone’s NFC chip for secure authentication sees an ever-increasing interest. In this paper, we describe a novel access control scheme, which doesn’t use card scanner and offers higher security guarantees when entering a gateway without needing video surveillance cameras.

Review of existing approaches. To begin with, let us describe existing commercial systems, which control the access by means of a personal identifier. Company [1] proposes systems based on using plastic cards or fingerprint. Manufacturer [2] features a more advanced set of products including virtual mobile cards (NFC-based), bank credit card authentication or biometric systems (fingerprint or facial recognition). A comprehensive list of currently available commercial products is presented in [3]. These can be categorized in 1) products supporting only classical plastic card id; 2) products that additionally include support for NFC or Bluetooth Low Energy (if NFC is not available); 3) biometric systems. Unique identifier in NFC compatible systems (point 2 above) is granted either via a global server for all clients (in this case a regular fee is taken) or for free based on a unique id of a smartphone (IMEI) or a SIM-card (IMSI). Identifier can be blocked if requested. Wherein, there may arise at least two cases of unauthorized access to the enterprise, that are impossible to track down: 1) after having lost the mobile device and before locking its id; 2) in case of intentional transfer of a smartphone to third parties. That is to say that such systems are quite vulnerable on its own.

Let us also highlight some of the more advanced systems. In [4] authors note a growing interest in access cards having an extra level of security. Multi technology cards offering embedded fingerprint scanner together with a standard passive RFID tag are said to be an interesting and promising advancement in the field. To supply the scanner, these cards also have an ultra slim battery. Surely, this comes with a higher price.

Next let’s consider research of promising combined systems. Patent [5] contains a description of a biometric system, in which RFID tag holders are also verified via a standalone facial recognition system. This allows to solve additional problems of access control systems like 1) buddy badging, when one person logs two badges, while only one actually enters the gate; 2) tailgating, when several people enter while using the same badge. Let any access violation occur, the door will be locked and a special lighting stack will alert the guards to intrude. A similar system with a different alerting method is proposed by [6] for access control in university hostels.

To sum it all up, all of the abovementioned systems have either almost no defense against card transfer (classical or NFC-based systems) or have a high price (biometric systems including fingerprint and facial recognition, as well as combined systems).

Mobile access control system model. Here we propose to turn the classical access control scheme “upside-down”. Firstly, instead of a RFID card scanner, which has to be connected to a computer or can be embedded into a smart door, we propose using passive RFID tags similar to those found in today’s plastic cards. They can store enough data for our system and are much cheaper. Secondly, instead of plastic cards we suggest employing user’s smartphone. By holding the device near a passive tag, the application we have developed, will be automatically started. All information about gate location to which the tag is attached will also be automatically scanned. Also, to avoid the need of a standalone video surveillance camera installation, we require the user to take a photograph on his frontal camera. After that, information from the tag as well as user’s data, including user id, location and photograph, is sent to the server via a corporate Wi-Fi network. Figure 1 has a comparison of typical access control system (fig. 1, *a*) and the one we propose (fig. 1, *b*). As can be seen from the picture, the proposed system doesn’t need camera or RFID scanner installation, furthermore no wiring is required as all of the communication is done using smartphone’s Wi-Fi connection.

Adding tags to the system. As is known, RFID (Radio Frequency Identification) tag is a device that can store a small amount of data, usually below 888 bytes (while there exist modifications with higher memory capacity, they are rate). The tags are classified into active, which contain an embedded energy source (battery). Their advantage is in high acting distance (up to 100m). And passive – this is the type of tag used in intercoms, biometric passports, contactless credit cards and classical access control systems. Such tags are cheaper that active, but can work only on a short distance ranging from several centimeters to meters depending on a standard and working frequency. Because in passive tags the microchip has no built-in power source, an electromagnetic coil is installed instead. A device for reading and programming the tag (including a smartphone) creates an electromagnetic field inducting a current in the tag by the Faraday’s law [6].

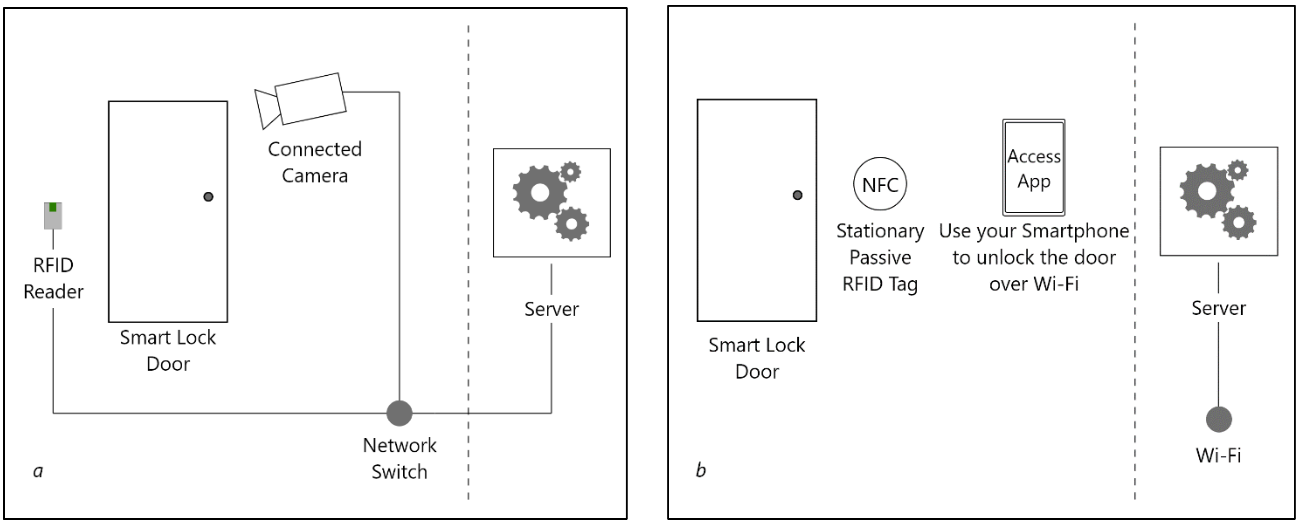


Fig. 1. *a* – typical access control system; *b* – our system

Smartphones contain a so-called NFC chip (Near Field Communication) to read and program RFID tags. It should be noted, that not all of existing tags on the market are compatible with NFC. Three main tag types, supporting NFC include: MIFARE Classic ®, MIFARE Ultralight ® and NTAG ®. The latter two have the best support among mobile devices [7], and NTAG has the largest capacity. Thus, in our product we support two its main modifications: NTAG213 (144 bytes) and NTAG216 (888 bytes) [8]. Besides the described writable memory, the tag also contains serial number, an option to enable write password protection and an irreversible switch to read-only mode.

In our system tag programming is supposed to happen on a device of an enterprise security administrator with a use of a special account. The first step is to fill data about the gate to which the tag is going to be attached. The data includes unique object name and its location. In response to tag registration request, server generates a unique unsigned integer id for the gate, which together with server identifier is written on the tag. In order to avoid data rewrite by third party applications or intentional data corruption, tag programming is protected via tag programming password (as we have described earlier, this capability is built into the chosen RFID tag standards). The password is global for the given organization and is automatically sent from the server. Given the described information, the administrator should bring the device to the tag at a distance of 1–3 cm for the programming to take place. If the tag is already password protected, then the operator should enter old password and take the device to the tag again. Then the administrator needs to setup user access policies for the registered tag in a special server-side administrative application (which we will describe in the next section).

The data written to the tag is stored in a special binary format called NDEF (NFC Data Exchange Format), that is implemented on Android via a special NdefMessage message type, containing a set of data records, called NdefRecord [9]. In our system we write:

1) global unique server identifier (server GUID), which we use to verify that the user registered in one organization will not try to get access to another one. It should be noted that a distinctive feature of GUID generation is its high randomness, meaning that its collisions are nearly impossible [10];

2) unsigned integer, representing gate id inside the organization;

3) a special Android Application Record (AAR) [9] used to launch the application instantly, when the device is held near the tag. The only requirement here is that the device should be unlocked. It is of no importance if any application is already running (either our or third party);

4) a similar record for iOS devices, containing the so-called Universal Link.

Having calculated each field's size (table 1), it can be noted, that each one of the considered RFID tag standards has enough memory for the developed system.

It is noteworthy that Apple iOS smartphones did not contain NFC chip for a long time [7], and even after its appearance NFC use was limited to Apple Pay functionality only. Currently, NFC development APIs are being rapidly added to the iOS operating system. Since iOS 11.0 it is possible to read RFID tags, and iOS 13.0 has introduced a tag write capability [11]. New devices also feature support for background tag reading [12]. That is a feature mostly analogous to the AAR, with a difference in that the application is not launched automatically, but a notification is presented to the user, inviting him to launch it. As we have already mentioned, the iOS launch record is written in Universal Link format [13]. Thereby, while we have developed the mobile application for Android devices only (at least for now), all of the functionality is available on both mobile platforms.

Table 1 – Data written on the RFID tag

Content	Size (bytes)	Description
Server ID	16	GUID
Secure gate ID	4	Unsigned integer
Android Application Record	42	Depends on application name length
iOS Universal Link	58	Depends on application name length
Overall	120	

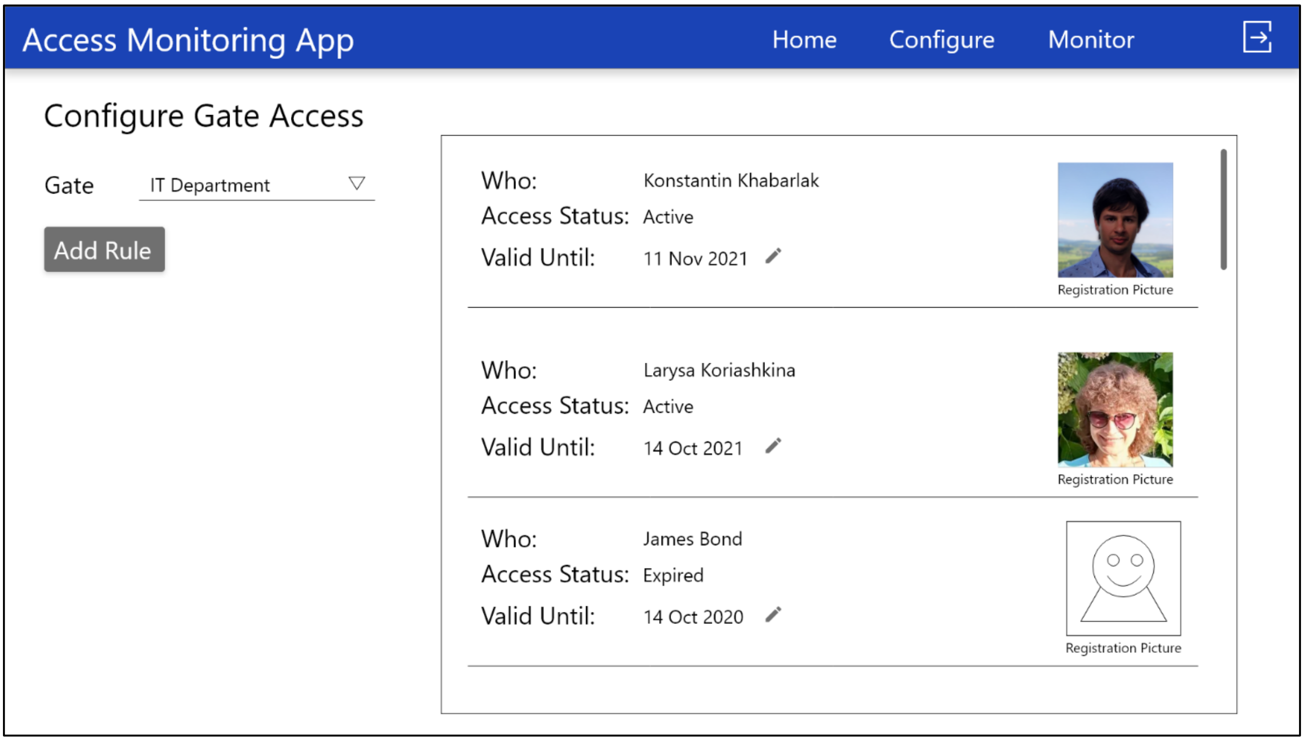
Server-side control system. The main instrument for administrator is a server-side control panel, implemented in a form of a web-site. Administrative account is needed to access the panel. In there the administrator can register a new smartphone user. Entering first and last name, as well as person's photograph is sufficient to complete the process. It should be noted that it is the administrator's responsibility to guarantee the correctness of the entered data. Here the configuration of gate access policies is also available. In a separate monitoring tab of the control panel latest accesses can be viewed.

To setup gate access policies, the tags needed must have already been registered via the mobile application as it was previously described. Then the administrator can select the tag to configure from the drop-down list (fig. 2) to add, view or edit existing accesses. To enhance the security each access record should have an expiration date set, after which the access will automatically be disabled (if access is not extended by the administrator). Based on the expiration date a corresponding status (active or expired) is shown.

After the initial setup, the main panel that we expect to be used is the monitoring panel, where we propose a number of features (fig. 3): 1) an ability to view access records in real time or by time filter (for example, during or outside the working hours); 2) filter by the tag to which an access attempt has been made; 3) filter by user; 4) also, an option to display denied accesses only can be selected. Each of the filters can be left empty if need. It should be noted, that while currently we use face information only to be able to track the actual person that tried to pass the gate manually (by a human being), in future we suggest extending such a system via mobile face recognition as described in [14].

Backend and third-party services integration. Along with the above described user-facing parts, we also have a server backend used to communicate with a mobile application via REST API. Also, we have implemented a SignalR [15] endpoint for third-party services integration. In our system we do not propose turnstile or smart door systems, so we expect the end-users to be able to quickly adapt their existing door or turnstile systems via the provided API. The SignalR itself is a set of libraries for server-side as well as mobile and web integrations, which as we hope, will allow for a seamless implementation of our system into existing infrastructure.

Conclusions. Client-server application has been presented in the paper, which includes: 1) administrative system to configure gate access policies and monitoring with filters by access time, user and RFID-tagged gate; 2) mobile application made to register gates and being a key to unlock the doors. The implementation of the developed system will allow to lower the cost of access control systems in schools, universities and enterprises by not only replacing stationary RFID scanner by a cheap tag, but also by not requiring video surveillance camera installation. The latter is not needed as it’s enough for the



Configure Gate Access

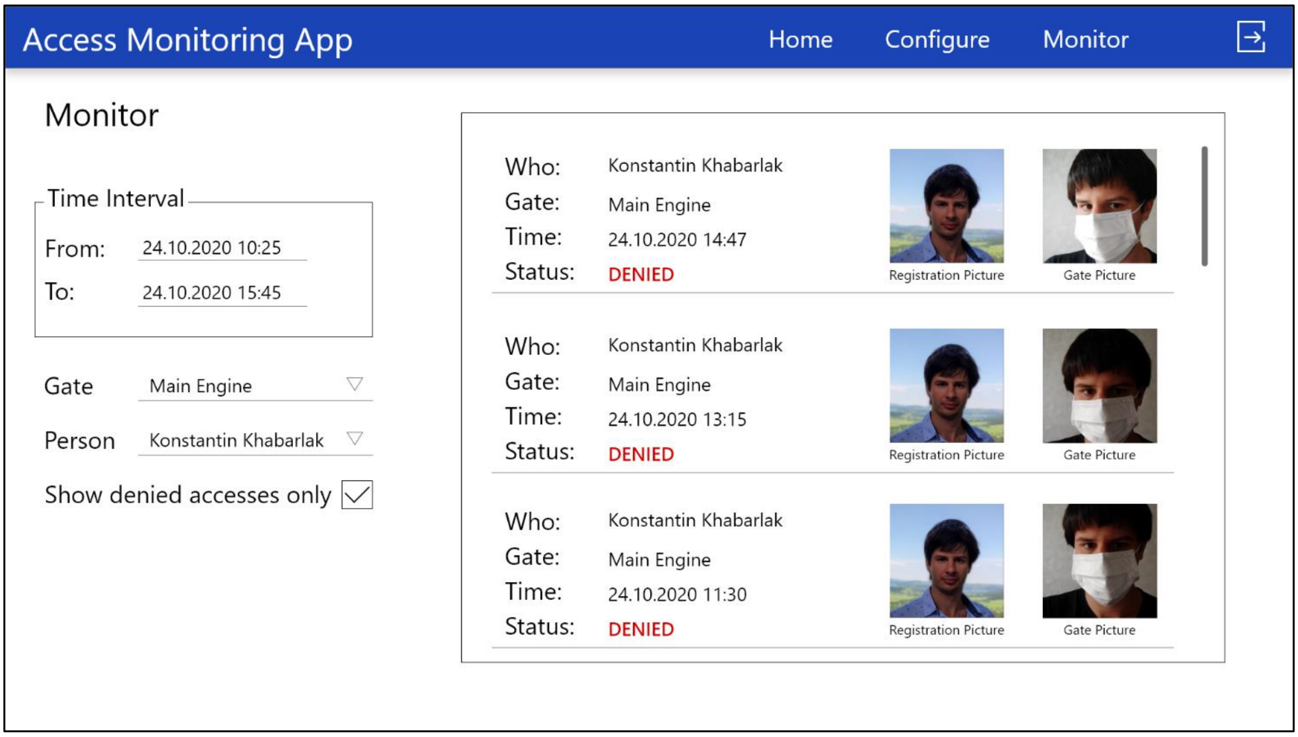
Gate: IT Department ▽

Who: Konstantin Khabarlak
Access Status: Active
Valid Until: 11 Nov 2021

Who: Larysa Koriashkina
Access Status: Active
Valid Until: 14 Oct 2021

Who: James Bond
Access Status: Expired
Valid Until: 14 Oct 2020

Fig. 2. Configuration tab of the proposed access control system



Monitor

Time Interval
From: 24.10.2020 10:25
To: 24.10.2020 15:45

Gate: Main Engine ▽

Person: Konstantin Khabarlak ▽

Show denied accesses only ☑

Who: Konstantin Khabarlak
Gate: Main Engine
Time: 24.10.2020 14:47
Status: DENIED

Who: Konstantin Khabarlak
Gate: Main Engine
Time: 24.10.2020 13:15
Status: DENIED

Who: Konstantin Khabarlak
Gate: Main Engine
Time: 24.10.2020 11:30
Status: DENIED

Fig. 3. Monitoring tab of the proposed access control system

user to take a photograph on his mobile phone when unlocking the door. We hope, that the proposed application will make a contribution to the development of more secure and less expensive access control systems.

We see an implementation of a mobile face recognition system as one of the next steps to enhance the proposed application.

References

1. *Защита информации. Контроль доступа. Учёт рабочего времени.* URL: http://www.ualock.kiev.ua/index.htm (accessed: 23.10. 20).
2. *Системы безопасности PERCo*. URL: https://www.perco.ru/ (accessed: 23.10.20).
3. *Мобильный доступ — использование смартфона в системах контроля доступа*. URL: https://habr.com/ru/company/intems/blog/433872/ (accessed: 12.10.20).
4. *Карты контроля доступа*. URL: http://www.techportal.ru/glossary/karti-kontrolya-dostupa.html (accessed: 12.10.20).
5. Kail K., Williams C., Kail R. *Access control system with RFID and biometric facial recognition.* U.S. Patent No. 11/790,385. 2007.
6. Farooq U. et al. RFID based security and access control system //*International Journal of Engineering and Technology*. – 2014. – Т. 6. – №. 4. – С. 309. doi: 10.7763/IJET.2014.V6.718
7. *NFC Compatibility*. URL: https://www.shopnfc.com/en/content/7-nfc-compatibility (accessed: 12.10.20).
8. *NFC Tag Specs – Tag NFC*. URL: https://www.tagnfc.com/en/info/11-nfc-tags-specs (accessed: 12.10.20).
9. *NFC basics*. URL: https://developer.android.com/guide/topics/connectivity/nfc/nfc (accessed: 13.10.20).
10. *What is GUID?* URL: http://guid.one/guid (accessed: 24.11.20).
11. *Core NFC | Apple Developer Documentation*. URL: https://developer.apple.com/documentation/corenfc (accessed: 23.10.20).
12. *Adding Support for Background Tag Reading | Apple Developer Documentation*. URL: https://developer.apple.com/documentation/corenfc/adding_support_for_background_tag_reading (accessed: 23.10.20).
13. *Allowing Apps and Websites to Link to Your Content | Apple Developer Documentation*. URL: https://developer.apple.com/documentation/xcode/allowing_apps_and_websites_to_link_to_your_content (accessed 23.10.20).
14. Khabarlak K., Koriashkina L. *Fast Facial Landmark Detection and Applications: A Survey* //ResearchGate preprint. – 2020. doi: 10.13140/RG.2.2.32735.07847
15. *Real-time ASP.NET with SignalR | .NET*. URL: https://dotnet.microsoft.com/apps/aspnet/signalr (accessed: 23.10.20).

References (transliterated)

1. *Zashchita informatsii. Kontrol' dostupa. Uchot rabochego vremeni [Information Protection. Access Control. Time Tracking].* Available at: http://www.ualock.kiev.ua/index.htm (accessed 23.10. 20).
2. *Sistemy bezopasnosti PERCo [PERCo Security Systems].* Available at: https://www.perco.ru/ (accessed 23.10.20).
3. *Mobil'nyy dostup — ispol'zovaniye smartfona v sistemakh kontrolya dostupa [Mobile access - using a smartphone in access control systems]*. Available at: https://habr.com/ru/company/intems/blog/433872/ (accessed 12.10.20).
4. *Karty kontrolya dostupa [Access Control Cards]*. Available at: http://www.techportal.ru/glossary/karti-kontrolya-dostupa.html (accessed 12.10.20).
5. Kail K., Williams C., Kail R. *Access control system with RFID and biometric facial recognition*. U.S. Patent No. 11/790,385. 2007.
6. Farooq, Umar, et al. *RFID based security and access control system*. International Journal of Engineering and Technology 6.4 (2014): 309. doi: 10.7763/IJET.2014.V6.718
7. *NFC Compatibility*. Available at: https://www.shopnfc.com/en/content/7-nfc-compatibility (accessed 12.10.20).
8. *NFC Tag Specs – Tag NFC.* Available at: https://www.tagnfc.com/en/info/11-nfc-tags-specs (accessed 12.10.20).
9. *NFC basics*. Available at: https://developer.android.com/guide/topics/connectivity/nfc/nfc (accessed 13.10.20).
10. *What is GUID?* Available at: http://guid.one/guid (accessed 24.11.20).
11. *Core NFC | Apple Developer Documentation.* Available at: https://developer.apple.com/documentation/corenfc (accessed 23.10.20).
12. *Adding Support for Background Tag Reading | Apple Developer Documentation*. Available at: https://developer.apple.com/documentation/corenfc/adding_support_for_background_tag_reading (accessed 23.10.20).
13. *Allowing Apps and Websites to Link to Your Content | Apple Developer Documentation*. Available at: https://developer.apple.com/documentation/xcode/allowing_apps_and_websites_to_link_to_your_content (accessed 23.10.20).
14. Khabarlak K., Koriashkina L. *Fast Facial Landmark Detection and Applications: A Survey* //ResearchGate preprint. – 2020. doi: 10.13140/RG.2.2.32735.07847
15. *Real-time ASP.NET with SignalR | .NET*. Available at: https://dotnet.microsoft.com/apps/aspnet/signalr (accessed 23.10.20).

Received 30.11.2020

Відомості про авторів / Сведения об авторах / About the Authors

Хабарлак Костянтин Сергійович – аспірант кафедри системного аналізу та управління Національного технічного університету «Дніпровська політехніка», Senior Backend Developer в IT-компанії SOLVVE; м. Дніпро, Україна; ORCID: https://orcid.org/0000-0003-4263-0871; e-mail: Khabarlak.K.S@nmu.one

Коряшкіна Лариса Сергіївна – кандидат фізико-математичних наук, доцент кафедри системного аналізу та управління Національного технічного університету «Дніпровська політехніка»; м. Дніпро, Україна; ORCID: https://orcid.org/0000-0001-6423-092X; e-mail: Koriashkina.L.S@nmu.one

Хабарлак Константин Сергеевич – аспирант кафедры системного анализа и управления Национального технического университета «Днепровская политехника», Senior Backend Developer в ИТ-компании SOLVVE; г. Днепр, Украина; ORCID: https://orcid.org/0000-0003-4263-0871; e-mail: Khabarlak.K.S@nmu.one

Коряшкина Лариса Сергеевна – кандидат физико-математических наук, доцент кафедры системного анализа и управления Национального технического университета «Днепровская политехника»; г. Днепр, Украина; ORCID: https://orcid.org/0000-0001-6423-092X; e-mail: Koriashkina.L.S@nmu.one

Khabarlak Kostiantyn Serhiyovych – PhD student at the department of System Analysis and Control, Dnipro University of Technology; Senior Backend Developer at SOLVVE IT-Company; Dnipro, Ukraine; ORCID: https://orcid.org/0000-0003-4263-0871; e-mail: Khabarlak.K.S@nmu.one

Koriashkina Larysa Sergiyivna – PhD, Associate Professor at the department of System Analysis and Control, Dnipro University of Technology; Dnipro, Ukraine; ORCID: https://orcid.org/0000-0001-6423-092X; e-mail: Koriashkina.L.S@nmu.one