ANALYSIS OF THE USER'S INFLUENCE ON RELIABILITY OF PUBLIC CLOUD SERVICES

ANALIZA WPLYWU UŻYTKOWNIKA NA NIEZAWODNOŚĆ USŁUG CHMURY PUBLICZNEJ

Paweł Stąpór, Dariusz Laskowski

Military University of Technology, Warsaw
Wojskowa Akademia Techniczna, Wydział Elektroniki

Abstract: *Universal access to cloud computing services means that users expect services to be provided in a reliable and secure manner. The availability of newer and more efficient end devices raises the question of whether the mobile device used affects an access reliability. In the article the authors taking into account the type of mobile device (laptop, tablet and smartphone) and the access method (WiFi and LTE) check what effect the end device on the reliability of access has.*

Keywords: *public cloud, user influence, reliability*

Streszczenie: *Powszechny dostęp do usług cloud computing sprawia, że użytkownicy oczekują aby usługi były świadczone w sposób niezawodny i bezpieczny. Dostępność coraz to nowszych i wydajniejszych urządzeń końcowych nasuwa pytanie czy to z jakiego urządzenia mobilnego korzystamy ma wpływ na niezawodność dostępu. W artykule autorzy sprawdzają biorąc pod uwagę rodzaj urządzenia mobilnego (laptop, tablet i smartfon) oraz metodę dostępu (WiFi i LTE) jaki wpływ na niezawodność dostępu ma urządzenie końcowe.*

Słowa kluczowe: *chmura publiczna, wpływ użytkownika, niezawodność*

ANALYSIS OF THE USER'S INFLUENCE ON RELIABILITY OF PUBLIC CLOUD SERVICES

1. Introduction

Last years proved great dynamic of developing technologies related to the cloud computing environment. The multitude of open source and paid solutions makes hardware and software manufacturers outdo each other to make their product as efficient and as unreliable as possible. Public cloud services available to the average user of mobile devices enable, among others, storing files, using applications requiring increased computing power. Currently, any smartphone user can store files in the cloud. On the Android system it will be i.e. Google Drive or Dropbox, in Windows - OneDrive or in iOS iCloud. The limitation of these applications is the size of an available space for data collection in cloud computing (CC). The annual report Digital in 2017: Global Overview published by *We Are Social and Hootsuite*¹⁾ shows that in January 2017 there were 7.476 billion people in the world, of whom 50% (3.773 billion) have an access to the Internet, and 46% (3.448 billion) an access to mobile Internet using smartphones. Observing traffic on websites, we can see that there has been a significant increase for traffic generated by smartphones and now equals 50% of all traffic (an increase of 30% compared to the previous year). However, for laptops, PCs and tablets, there was a drop by 20% in the current level to 45% and 5% to the current 5% of total traffic. According to the report in the world (considering only an adult part of the population) 81% of the population uses smartphones, 73% laptops or desktop computers and 39% use tablets. This report shows that the current society is really a "digital society" that every step is taken in contact with mobile devices and services available on the Internet, including the services of CC.

The user can get an access to public cloud services in many ways. Newer standards offer a "higher" bandwidth and the available equipment is "more" efficient. It is therefore reasonable to investigate which access method is the most reliable and ensures the highest level of security. A device used by a particular user also seems to be important. By comparing access times and synchronization times from different devices, it will be possible to examine whether the user equipment's technical parameters affect the reliability of the selected CC service using the same access method.

2. Research methodology

Based on the literature [1,2,3], the user's existence environment was developed [Fig. 1] which has been used in studies of its impact on the reliability of public cloud services.

¹⁾ <https://wearesocial.com/uk/special-reports/digital-in-2017-global-overview>

Fig. 1 Environmental conditions of user existence

The architecture used for the research has been depicted in the figure (Fig 2). It allows users access to CC services using a connection compliant with the 802.11n and LTE standards. The devices used in the study are popular and representative devices such as: a laptop (Lenovo ThinkPad 13), a tablet (Lenovo TAB 4) and a smartphone (Xiaomi Redmi 4X). All devices have network cards compliant with the 802.11n standard and LTE modem. The only exception is a laptop, which was additionally equipped with the Huawei E3372 LTE modem. The research was carried out using the LTE connection of one mobile Internet provider in order to obtain objective results. The distance of devices from LTE and WiFi network transmitters was the same for all tested devices.

In the research, a public cloud was used, i.e. external cloud. This means that all resources, such as hardware and applications, are created by the provider. The service is available to external recipients via the Internet [11]. As a cloud service, ownCloud was launched, which allows you to store files and access them regardless of the network location. An access to resources can be carried out through a web browser and through a dedicated application for mobile devices and computers. The research was carried out using both methods of access to cloud computing resources. This is possible because ownCloud uses TLS to encrypt packets, which must be set up before the transmission starts.

Fig. 2 Test-bed architecture

3. Results

Analyzing the obtained access times to resources it can be noted that both using the Internet browser (Fig. 3) and an application (Fig. 4) the best results were obtained for a laptop. The weakest results (the longest times) in carried research were obtained for the access in which tablets were used. The expected level – 10 seconds, was reached using an access through the WiFi network. In other cases an access time was satisfying or slightly exceeded permissible level while the mobile Internet LTE in tablets was used.

Fig. 3 Times of access to resources from the web browser.

Fig. 4 Times of access to resources from the application.

It is also worth noting that regardless of whether we use the browser or application, the average access times obtained are comparable for individual end devices. The differences that occur are very small, on the order of several hundredths of a second and practically unnoticeable by the user.

Analyzing the synchronization times between the mobile device and the computing cloud, it can be seen that in the case of an internet browser (Fig. 5) shorter synchronization times were obtained when the device was connected via a wireless WiFi network. For most cases the acceptable level has been reached. Taking into account the device, synchronization was the fastest in the laptop - the synchronization time was less than 10 seconds. Only when connecting with a smartphone via the mobile Internet was the permissible level slightly exceeded.

Fig. 5 Average sync times for resources from the web browser.

Fig. 6 Average sync times for resources from the application.

Similar results were obtained in the case of synchronization through the application (Fig. 6). However, for all cases an acceptable level was achieved. For a tablet and smartphone, both access methods achieved similar values of synchronization times - about 10.7 seconds for LTE and about 10.0 seconds for WiFi. Analyzing the results for a laptop, we can see that for this method of synchronization a longer synchronization time of 0.3 seconds was obtained when connecting via mobile Internet, and slightly below the desired synchronization time via a wireless network.

The security of transmitted data has a significant impact on reliability and thus on the access quality. On the basis of the publication [4] it can be concluded that security largely depends on the service user. Despite the fact that the architecture of the test run is encryption using SSL certificate user connecting to the resource using the example. Untrusted points significantly increases the risk of data interception by unauthorized persons. It seems that comparing the two methods of access to the network, it is safer to connect the LTE, because of this mobile Internet provider, they offer additional services to increase transmission security (i.e. the Internet security). It is also more difficult to capture traffic on a mobile cellular network, i.e. more funds are needed in comparison to wireless WLANs. On the other hand, cloud security depends on the cloud manager in whose interest it is to ensure data security and their transmission.

4. Conclusions

Obtained results of measuring the time of access to the service and file synchronization with the use of a smartphone, tablet and laptop show that regardless of an access method - WiFi or LTE - we notice slight differences in the speed of gaining an access. The conducted research shows that which mobile devices the user uses in order to gain an access to cloud resources has an impact on an access time and synchronization, and thus on reliability.

Comparing all tested devices, we can conclude that more efficient devices will ensure greater reliability of using CC services. When comparing a smartphone with a laptop, it is a difference of the order of seconds in an access or data synchronization. Analyzing access methods in terms of security as a factor having a significant impact on reliability, it should be noted that the mobile Internet access LTE can provide the user with a higher level of security compared to the connection using the 802.11 standard. This is especially noticeable when the user uses an open access point (hotspot), where the highest risk of a hacker attack occurs. However, according to the authors, safety in each case depends mainly on the user's awareness and properly constructed security policies when using CC services. Even the best secured network may not be safe if used improperly. Based on the research and the results obtained, it can be concluded that, despite the high level of quality of CC services provided by the providers, the user also has an impact on the reliability of the service. By choosing more efficient devices and safer access methods, it is possible to increase the level of reliability. However, minor differences that have occurred show that the user will notice a "perceptible" improvement in service provision only in the situation of increased use of cloud computing resources.

5. References

- [1] Barlow R.E., Proschan F., *Mathematical Theory of Reliability*, John Wiley & Sons, 1965.
- [2] Misra K.B., *Reliability Analysis and Prediction*, Elsevier, New York, 1992.
- [3] Ireson W.G., *Handbook of Reliability Engineering and management*, McGraw-Hill, New York, 1996.
- [4] Stąpór P, Laskowski D. Concept of cloud computing implementation as a platform for telemetry systems, *Achives of Transport system Telematics*, Volume 10, Issue 2, 2017.
- [5] Siergiejczyk M., Paś J., Rosiński A.: Issue of reliability–exploitation evaluation of electronic transport systems used in the railway environment with consideration of electromagnetic interference. *IET Intelligent Transport Systems* 2016, vol. 10, issue 9, 2016, pp. 587–593.
- [6] Bujak A., Zajac, P.: *Monitoring of Cargo in Logistic Systems of Transport and Storage, Communications in Computer and Information Science*, Volume 395 CCIS, 2013, Pages 361-369, ISSN: 18650929 ISBN: 978-364241646-0, Springer Verlag.
- [7] Siergiejczyk M., Rosiński A., Krzykowska K.: Reliability assessment of supporting satellite system EGNOS. In: W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, J. Kacprzyk (eds) *New results in dependability and computer systems, given as the monographic publishing series – „Advances in intelligent and soft computing”*, Vol. 224. Springer, 2013. pp. 353-364.

- [8] Rychlicki M., Kasprzyk Z.: Increasing performance of SMS based information systems. In: „Proceedings of the Ninth International Conference Dependability and Complex Systems DepCoS-RELCOMEX”, given as the monographic publishing series – „Advances in intelligent systems and computing”, Vol. 286. Springer, 2014. pp. 373-382.
- [9] Stawowy M., Dziula P.: Comparison of uncertainty multilayer models of impact of teleinformation devices reliability on information quality. In: “Proceedings of the European Safety and Reliability Conference ESREL 2015”, editors: L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio, W. Kröger. CRC Press/Balkema, 2015. pp. 2685-2691.
- [10] Bajda A., et al: Diagnostics the quality of data transfer in the management of crisis situation, Electrical Review 87(9A), pp. 72-78, 2011.
- [11] Mell P., The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, Special Publication 800-145. <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>
- [12] Butlewski, M., Sławińska, M. 2014. Ergonomic method for the implementation of occupational safety systems, Occupational Safety and Hygiene II - Selected Extended and Revised Contributions from the International Symposium Occupational Safety and Hygiene, SHO 2014, pp. 621-626.
- [13] Jasiulewicz-Kaczmarek M., Drożyner P.: Social dimension of sustainable development – safety and ergonomics in maintenance activities, C. Stephanidis and M. Antona (Eds.): Universal Access in Human-Computer Interaction. Design Methods, Tools, and Interaction Techniques for eInclusion, UAHCI/HCI 2013, Part I, LNCS 8009, pp. 175-184. Springer, Heidelberg.
- [14] Lubkowski, P., et al: Provision of the reliable video surveillance services in heterogeneous networks, Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014, CRT Press, A Balkema BOOK, 2015, pp. 883-888, Print ISBN: 978-1-138-02681-0, DOI: 10.1201/b17399-58.
- [15] Lubkowski P., Laskowski D.: Selected Issues of Reliable Identification of Object in Transport Systems Using Video Monitoring Services, Communication in Computer and Information Science, Springer International Publishing AG / Springer Berlin Heidelberg, Switzerland, Volume 471, 2014, pp 59-68, ISSN 1865-0929, ISBN 978-3-662-45316-2 (Print), DOI 10.1007/978-3-662-45317-9_7, 2014.
- [16] Kozakiewicz A., Felkner, A., Furtak, J., Zieliński, Z., Brudka, M., Małowidzki, M.: Secure workstation for special applications, Communications in Computer and Information Science, Volume 187 CCIS, 2011, Pages 174-181, ISSN: 18650929 ISBN: 978-364222364-8, DOI: 10.1007/978-3-642-22365-5_21.

- [17] Kulesza R., Zieliński, Z.: Diagnosis resolution of processors' network using the comparison method, *Przegląd Elektrotechniczny*, Volume 86, Issue 9, 2010, Pages 157-162, ISSN: 00332097.
- [18] Nowakowski, T., Werbińska-Wojciechowska, S.: Uncertainty problem in decision support system for means of transport maintenance processes performance development, *Journal of Konbin*, Volume 23, Issue 1, September 2012, Pages 173-192, ISSN: 18958281, DOI: 10.2478/jok-2013-0047.
- [19] Zieliński Z., Furtak J., Chudzikiewicz J., Stasiak A., Brudka, M.: Secured workstation to process the data of different classification levels, *Journal of Telecommunications and Information Technology*, Volume 2012, Issue 3, 2012, Pages 5-12, ISSN: 15094553.

***MSc. Paweł Stąpór** is a graduate and PhD student at the Faculty of Electronics at the Military University of Technology. He is interested in ICT networks, in particular mobile networks and new technological solutions. Mainly focused on the security, reliability and quality of access to network resources from different locations. (Share 50%)*

***PhD. Eng. Dariusz Laskowski** is a graduate of the Faculty of Electronics of the Military University of Technology. He deals with multi-aspect analysis of eye phenomena in heterogeneous services and networks offered by data transmission. It focuses on safety, maintenance, quality of life and technological security. (Share 50%)*

ANALIZA WPLYWU UŻYTKOWNIKA NA NIEZAWODNOŚĆ USŁUG CHMURY PUBLICZNEJ

1. Wstęp

Ostatnie lata to czas dynamicznie rozwijających się technologii związanych ze środowiskiem chmur obliczeniowych (CC). Mnogość rozwiązań open source'owych jak i płatnych sprawia, że producenci sprzętu i oprogramowania prześcigają się w tym, aby to ich produkt był jak najwydajniejszy i jak najmniej zawodny. Usługi chmur publicznych dostępne dla przeciętnego użytkownika urządzeń mobilnych umożliwiają m.in. przechowywanie plików, korzystanie z aplikacji wymagających zwiększonej mocy obliczeniowej. Obecnie każdy użytkownik smartfona może przechowywać pliki w chmurze. W systemie Android będzie to np. Google Drive czy Dropbox, w systemie Windows – OneDrive czy w iOS iCloud. Ograniczeniem w przypadku tych aplikacji jest rozmiar dostępnej przestrzeni do gromadzenia danych w CC.

Z corocznego raportu *Digital in 2017: Global Overview*² opublikowanego przez serwisy We Are Social i Hootsuite wynika, że w styczniu 2017 roku na świecie było 7,476 mld ludzi, z czego aż 50% (3,773 mld) posiada dostęp do Internetu, a 46% (3,448 mld) łączy się z mobilnych Internetem za pomocą smartfonów. Patrząc na ruch na stronach internetowych możemy zauważyć, że odnotowano znaczący wzrost dla ruchu generowanego przez smartfony i obecnie wynosi 50% całego ruchu (wzrost o 30% w porównaniu z poprzednim rokiem). Natomiast dla laptopów, komputerów PC oraz tabletów zanotowano spadek kolejno o 20% do obecnego poziomu 45% i o 5% do aktualnych 5% ogólnego ruchu. Według raportu na świecie (biorąc pod uwagę tylko dorosłą część populacji) 81% ludności używa smartfonów, 73% laptopów lub komputerów desktopowych oraz 39% korzysta z tabletów. Powyższy raport pokazuje, że obecne społeczeństwo to tak naprawdę „cyfrowe społeczeństwo”, które na każdym kroku ma kontakt z urządzeniami mobilnymi oraz usługami dostępnymi przez Internet, w tym usługami CC.

Użytkownik może uzyskać dostęp do usług chmury publicznej na wiele sposobów. Coraz to nowsze standardy oferują „większe” przepustowości, a dostępny sprzęt jest „bardziej” wydajny. Zasadnym zatem staje się zbadanie, która metoda dostępu jest najbardziej niezawodna i zapewnia najwyższy poziom bezpieczeństwa. Istotnym wydaje się także urządzenie, z którego korzysta użytkownik. Porównując czasy dostępu oraz czasu synchronizacji z różnych urządzeń, możliwe będzie zbadanie czy parametry techniczne urządzenia użytkownika mają wpływ na niezawodność wybranej usługi CC przy wykorzystywaniu tego samego sposobu dostępu.

² <https://wearesocial.com/uk/special-reports/digital-in-2017-global-overview>

2. Metoda badawcza

Na podstawie literatury [1,2,3] opracowano środowisko egzystencji użytkownika (rys. 1) który został wykorzystany w badaniach wpływu jego na niezawodność usług chmury publicznej

Rys. 1 Uwarunkowania środowiska egzystencji użytkownika

Architektura wykorzystana do badań została zobrazowana na rysunku (rys. 2). Umożliwia ona dostęp użytkownika do usług CC przy wykorzystaniu połączenia zgodnego ze standardem 802.11n oraz LTE. Urządzenia użyte w badaniu to popularne i reprezentatywne urządzenia typu: laptop (Lenovo ThinkPad 13), tablet (Lenovo TAB 4) i smartphone (Xiaomi Redmi 4X). Wszystkie urządzenia posiadają karty sieciowe zgodne ze standardem 802.11n oraz modem LTE. Wyjątek stanowi laptop, który został dodatkowo wyposażony w modem LTE Huawei E3372. Badania wykonano wykorzystując połączenie LTE jednego providera Internetu mobilnego w celu uzyskania obiektywnych wyników. Odległość urządzeń od nadajników sieci LTE oraz WiFi była jednakowa dla wszystkich badanych urządzeń.

W badaniach wykorzystano chmurę publiczną (ang. public cloud), czyli tzw. chmura zewnętrzna. Oznacza to, że wszystkie zasoby, takie jak sprzęt i aplikacje, są tworzone przez dostawcę. Usługa jest dostępna dla odbiorców zewnętrznych poprzez Internet [11]. Jako usługę chmurową uruchomiono ownCloud, która umożliwia przechowywanie plików i dostęp do nich niezależnie od lokalizacji sieciowej.

Dostęp do zasobów może być realizowany przez przeglądarkę internetową oraz przez dedykowaną aplikację na urządzenia mobilne oraz komputery. Badania przeprowadzono z użyciem obydwu sposobów dostępu do zasobów chmury obliczeniowej. Wykorzystując oprogramowanie Wireshark na podstawie przechwyconych pakietów zmierzono czasy dostępu oraz synchronizacji. Jest to możliwe do zrealizowania, ponieważ ownCloud wykorzystuje do szyfrowania pakietów protokół TLS, który przed rozpoczęciem transmisji musi zestawić połączenie, tzw. three-way handshake, a po zakończeniu połączenie jest rozłączane. W celu zwiększenia dokładności badań, każde z pomiarów zwielokrotniono, a do analizy wzięto uśrednione wyniki. Do synchronizacji został wykorzystany plik w formacie pdf o rozmiarze 1,14 MB, jest to rozmiar odpowiadający kilkunastostronicowemu dokumentowi.

Rys. 2 Architektura test-bedu.

3. Wyniki

Analizując uzyskane czasy dostępu do zasobów można zauważyć, że zarówno przy użyciu przeglądarki internetowej (rys. 3) jak i dedykowanej aplikacji (rys. 4) uzyskano najlepsze wyniki dla laptopa. Najgorsze wyniki (najdłuższe czasy) w przeprowadzonych badaniach uzyskano dla dostępu przy pomocy tabletu. W przypadku dostępu przez sieć WiFi został osiągnięty pożądany poziom wynoszący 10 sekund. Dla pozostałych przypadków czas dostępu jest na poziomie akceptowalnym bądź nieznacznie został przekroczony poziom dopuszczalny – dostęp przez Internet mobilny LTE z wykorzystaniem tabletu.

Rys. 3 Czasy dostępu do zasobów z poziomu przeglądarki internetowej.

Rys. 4 Czasy dostępu do zasobów z poziomu aplikacji.

Warto również zauważyć, że niezależnie czy używamy przeglądarki czy aplikacji uzyskiwane średnie czasy dostępu są porównywalne dla poszczególnych urządzeń końcowych. Różnice jakie występują są bardzo niewielkie, rzędu kilkunastu setnych części sekundy i praktycznie niezauważalne przez użytkownika.

Analizując czasy synchronizacji pomiędzy urządzeniem mobilnym a chmurą obliczeniową można zauważyć, że w przypadku przeglądarki internetowej (rys. 5) krótsze czasy synchronizacji uzyskano przy połączeniu urządzenia przez sieć bezprzewodową WiFi.

Dla większości przypadków został osiągnięty poziom dopuszczalny. Biorąc pod uwagę urządzenie synchronizacja najszybciej przebiegała w laptopie – czas synchronizacji poniżej 10 sekund. Jedynie przy połączeniu smartfonem przez Internet mobilny został nieznacznie przekroczony poziom dopuszczalny.

Rys. 5 Uśrednione czasy synchronizacji zasobów z poziomu przeglądarki internetowej.

Rys. 6 Uśrednione czasy synchronizacji zasobów z poziomu aplikacji.

Podobne wyniki uzyskano w przypadku synchronizacji poprzez aplikację (rys. 6). Jednak dla wszystkich przypadków został osiągnięty poziom dopuszczalny.

Dla tabletu i smartfona w obu metodach dostępu uzyskano zbliżone wartości czasów synchronizacji – około 10,7 sekundy dla LTE i około 10,0 sekundy dla WiFi. Analizując wyniki dla laptopa możemy zauważyć, że dla tego sposobu synchronizacji uzyskano dłuższy o 0,3 sekundy czas synchronizacji przy połączeniu przez Internet mobilny, oraz nieznacznie poniżej poziomu pożądanego czas synchronizacji poprzez sieć bezprzewodową.

Znaczny wpływ na niezawodność, a tym samym na jakość dostępu ma bezpieczeństwo transmitowanych danych. Na podstawie publikacji [4] można wywnioskować, że bezpieczeństwo w znacznej mierze zależy od użytkownika usługi. Pomimo tego, że w badanej architekturze uruchomione zostało szyfrowanie za pomocą certyfikatu SSL użytkownik łącząc się z zasobami przy pomocy np. niezaufanych punktów znacząco zwiększa ryzyko przechwycenia danych przez osoby niepowołane. Wydaje się, że porównując dwa sposoby dostępu do sieci, bezpieczniejszym jest połączenie LTE, z racji tego dostawcy Internetu mobilnego oferują dodatkowe usługi zwiększające bezpieczeństwo transmisji (np. ochrona Internetu). Trudniej jest również przechwycić ruch w mobilnej sieci komórkowej, tzn. potrzeba większych środków w porównaniu z bezprzewodowymi sieciami WLAN. Z innej strony bezpieczeństwo chmury zależy od zarządzającego chmurą w którego interesie jest zapewnić bezpieczeństwo danych oraz ich transmisji.

4. Podsumowanie i wnioski

Uzyskane wyniki pomiaru czasu dostępu do usługi oraz synchronizacji plików z wykorzystaniem smartfona, tabletu oraz laptopa pokazują, że niezależnie od metody dostępu – WiFi czy LTE – zauważamy niewielkie różnice w szybkości uzyskania dostępu. Przeprowadzone badania pokazują, że to z jakich urządzeń mobilnych korzysta użytkownik w celu uzyskania dostępu do zasobów chmury obliczeniowej ma wpływ na czas dostępu oraz synchronizacji, a tym samym na niezawodność. Porównując wszystkie badane urządzenia możemy stwierdzić, że wydajniejsze urządzenia zapewnią większą niezawodność korzystania z usług CC. Przy porównaniu smartfona z laptopem jest to różnica rzędu pojedynczych sekund w dostępie czy synchronizacji danych. Analizując metody dostępu pod względem bezpieczeństwa, jako czynnika mającego znaczący wpływ na niezawodność, należy zauważyć, że dostęp przez Internet mobilny LTE może zapewnić użytkownikowi wyższy poziom bezpieczeństwa w porównaniu do połączenia z wykorzystaniem standardu 802.11. Szczególnie jest to zauważalne w przypadku, gdy użytkownik korzysta z otwartego punktu dostępowego (hotspot), gdzie występuje najwyższe ryzyko ataku hackerskiego. Jednak wg autorów bezpieczeństwo w każdym z przypadków w głównej mierze zależy od świadomości użytkownika oraz właściwie skonstruowanych polityk

bezpieczeństwa przy używaniu usług CC. Nawet najlepiej zabezpieczona sieć, może nie być bezpieczna, jeśli będzie niewłaściwie użytkowana.

Na podstawie przeprowadzonych badań i otrzymanych wyników można stwierdzić, że pomimo wysokiego poziomu jakości świadczonych usług CC przez providerów, użytkownik także ma wpływ na niezawodność świadczenia usługi.

Wybierając wydajniejsze urządzenia oraz bezpieczniejsze metody dostępu możliwe jest zwiększenie poziomu niezawodności. Jednak niewielkie różnice jakie wystąpiły pokazują, że użytkownik zauważy „odczuwalną” poprawę świadczenia usługi dopiero w sytuacji zwiększonego wykorzystywania zasobów chmury obliczeniowej.

5. Literatura

- [1] Barlow R.E., Proschan F., Mathematical Theory of Reliability, John Wiley & Sons, 1965.
- [2] Misra K.B., Reliability Analysis and Prediction, Elsevier, New York, 1992.
- [3] Ireson W.G., Handbook of Reliability Engineering and management, McGraw-Hill, New York, 1996.
- [4] Stąpór P., Laskowski D. Concept of cloud computing implementation as a platform for telemetry systems, Archives of Transport system Telematics, Volume 10, Issue 2, 2017.
- [5] Siergiejczyk M., Paś J., Rosiński A.: Issue of reliability–exploitation evaluation of electronic transport systems used in the railway environment with consideration of electromagnetic interference. IET Intelligent Transport Systems 2016, vol. 10, issue 9, 2016, pp. 587–593.
- [6] Bujak A., Zajac, P.: Monitoring of Cargo in Logistic Systems of Transport and Storage, Communications in Computer and Information Science, Volume 395 CCIS, 2013, Pages 361-369, ISSN: 18650929 ISBN: 978-364241646-0, Springer Verlag.
- [7] Siergiejczyk M., Rosiński A., Krzykowska K.: Reliability assessment of supporting satellite system EGNOS. In: W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, J. Kacprzyk (eds) New results in dependability and computer systems, given as the monographic publishing series – „Advances in intelligent and soft computing”, Vol. 224. Springer, 2013. pp. 353-364.
- [8] Rychlicki M., Kasprzyk Z.: Increasing performance of SMS based information systems. In: „Proceedings of the Ninth International Conference Dependability and Complex Systems DepCoS-RELCOMEX”, given as the monographic publishing series – „Advances in intelligent systems and computing”, Vol. 286. Springer, 2014. pp. 373-382.

- [9] Stawowy M., Dziula P.: Comparison of uncertainty multilayer models of impact of teleinformation devices reliability on information quality. In: "Proceedings of the European Safety and Reliability Conference ESREL 2015", editors: L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio, W. Kröger. CRC Press/Balkema, 2015. pp. 2685-2691.
- [10] Bajda A., et al: Diagnostics the quality of data transfer in the management of crisis situation, *Electrical Review* 87(9A), pp. 72-78, 2011.
- [11] Mell P., The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, Special Publication 800-145. <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>
- [12] Butlewski, M., Sławińska, M. 2014. Ergonomic method for the implementation of occupational safety systems, *Occupational Safety and Hygiene II - Selected Extended and Revised Contributions from the International Symposium Occupational Safety and Hygiene, SHO 2014*, pp. 621-626.
- [13] Jasiulewicz-Kaczmarek M., Drożyner P.: Social dimension of sustainable development – safety and ergonomics in maintenance activities, C. Stephanidis and M. Antona (Eds.): *Universal Access in Human-Computer Interaction. Design Methods, Tools, and Interaction Techniques for eInclusion, UAHCI/HCI 2013, Part I, LNCS 8009*, pp. 175-184. Springer, Heidelberg.
- [14] Lubkowski, P., et al: Provision of the reliable video surveillance services in heterogeneous networks, *Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014, CRT Press, A Balkema BOOK*, 2015, pp. 883-888, Print ISBN: 978-1-138-02681-0, DOI: 10.1201/b17399-58.
- [15] Lubkowski P., Laskowski D.: *Selected Issues of Reliable Identification of Object in Transport Systems Using Video Monitoring Services, Communication in Computer and Information Science, Springer International Publishing AG / Springer Berlin Heidelberg, Switzerland, Volume 471*, 2014, pp 59-68, ISSN 1865-0929, ISBN 978-3-662-45316-2 (Print), DOI 10.1007/978-3-662-45317-9_7, 2014.
- [16] Kozakiewicz A., Felkner, A., Furtak, J., Zieliński, Z., Brudka, M., Małowidzki, M.: *Secure workstation for special applications, Communications in Computer and Information Science, Volume 187 CCIS*, 2011, Pages 174-181, ISSN: 18650929 ISBN: 978-364222364-8, DOI: 10.1007/978-3-642-22365-5_21.

- [17] Kulesza R., Zieliński, Z.: Diagnosis resolution of processors' network using the comparison method, *Przegląd Elektrotechniczny*, Volume 86, Issue 9, 2010, Pages 157-162, ISSN: 00332097.
- [18] Nowakowski, T., Werbińska-Wojciechowska, S.: Uncertainty problem in decision support system for means of transport maintenance processes performance development, *Journal of Konbin*, Volume 23, Issue 1, September 2012, Pages 173-192, ISSN: 18958281, DOI: 10.2478/jok-2013-0047.
- [19] Zieliński Z., Furtak J., Chudzikiewicz J., Stasiak A., Brudka, M.: Secured workstation to process the data of different classification levels, *Journal of Telecommunications and Information Technology*, Volume 2012, Issue 3, 2012, Pages 5-12, ISSN: 15094553.

Mgr inż. Paweł Stąpór jest absolwentem Wydziału Elektroniki Wojskowej Akademii Technicznej. Interesuje się sieciami teleinformatycznymi, w szczególności sieciami mobilnymi oraz nowymi rozwiązaniami technologicznymi. Głównie koncentruje się na bezpieczeństwie, niezawodności i jakości dostępu do zasobów sieciowych z różnych lokalizacji. (Udział 50%)

Dr hab. inż. Dariusz Laskowski jest absolwentem wydziału Elektroniki Wojskowej Akademii Technicznej, gdzie obecnie pracuje. Zajmuje się wieloaspektową analizą zjawisk wpływających na prawidłową realizację usług w systemach i sieciach heterogenicznych oferujących transmisję danych. Koncentruje się na niezawodności, bezpieczeństwie, jakości oraz przetrwaniu obiektów technicznych pod kątem ich praktycznego zastosowania w sieciach heterogenicznych. (Udział 50%)