UDC: 336.74:004.738.5
DOI: 10.5937/AnEkSub2001135P
Review article

Анали Економског факултета у Суботици – The Annals of the Faculty of Economics in Subotica
Vol. 56, No. 43, pp. 135-149
Received: 30/08/2019
Accepted: 21/03/2020

Loss of privacy in electronic payment systems[1]

Губитак приватности података у електронским системима плаћања

Aleksandra Pešterac[*]
University of Kragujevac, Faculty of Economics, Kragujevac, Republic of Serbia,
apesterac@kg.ac.rs
Nenad Tomić
University of Kragujevac, Faculty of Economics, Kragujevac, Republic of Serbia,
ntomic@kg.ac.rs

Abstract: The emergence of new information technologies, such as the Internet of Things, the fifth generation of mobile Internet, artificial intelligence, Big Data, machine learning and blockchain, has led to significant changes in the social and business environment. The potential for exponential growth in such conditions is also recognized in the field of electronic payment systems. The development of the Internet of Things, as a global technical infrastructure that connects objects by adding microprocessors and communications software to them, has become an important basis for the further progress of electronic payment systems. In the process of further improvements, the system faces the great challenge of protection against the unauthorized use, modification or destruction of data. An even greater challenge is the potential abuse of users' personal data by business entities or government agencies. The paper focuses on the challenges of protecting the privacy of users of electronic payment systems in a smart environment.

Keywords: Internet of Things, Big Data, privacy, electronic payments.
JEL classification: E42, L86, O33

Сажетак: Појава нових информационих технологија као што су Интернет ствари, пета генерација мобилног Интернета, вештачка интелигенција, обрада велике количине података, машинско учење и блокчеин, довели су до значајних промена у начину функционисања друштвеног и пословног окружења. Потенцијал за експоненцијални раст у таквим условима препознат је у области електронских система плаћања. Развој Интернет ствари, као глобалне техничке инфраструктуре која додавањем микропроцесора и комуникационих софтвера стварима врши њихово повезивање, постао је важна основа даљег напретка електронских система плаћања. У поступку даљег унапређења, систем се нашао пред великим изазовом заштите од неовлашћеног коришћења, модификације или уништења података. Још већи изазов представља потенцијална злоупотреба приватности личних података корисника, од стране пословних ентитета или државних органа. Решења се траже у проналажењу компромиса између приватности (платилац) и сигурности (прималац) различитих страна. Рад се фокусира на изазове очувања приватности података корисника електронских система плаћања у паметном окружењу.

Кључне речи: Интернет ствари, велики подаци, приватност, електронско плаћање
JEL класификација: E42, L86, O33

[1] The paper presents a result of the project number III 47009 supported by The Ministry of Education, Science and Technological Development of the Republic of Serbia.

[*] Corresponding author

Introduction

The new technological transformation brings about the need for change in the approach to basic business principles. The tremendous advances in the deployment of wireless communications systems in recent years have increased the usage of mobile devices and the concept of customer service delivery anywhere, at any time. In this context, connecting users to the Internet is no longer the highest form of information and communication technologies (ICT) application, as the efforts are made towards connecting the physical and virtual worlds. There are tendencies to connect all aspects of the human environment, which can be used to monitor processes or automate activities into a virtual whole, with the aim of providing services via Internet (Tsiatsis et al., 2019, p. 9).

The Internet of Things (IoT) concept was created as a product of the global connection of people with devices and objects from the environment. It has created new opportunities for the development of electronic payment systems. Connecting devices, machines and objects through the installation of microprocessors and forming a permanent communication link will allow automatic execution of routine transactions. The large amounts of data generated by smart devices provide the basis for a new approach to data processing and management, known as Big Data. At the same time, the question of storage, protection and possible misuse of the obtained data arises. The subject of paper is the key challenges in ensuring the privacy and security for data created by electronic payment systems customers. The aim of the paper is to advance the theoretical understanding of privacy of electronic payment systems customers in a modern information environment.

The first part of the paper will explain in more detail the concepts of the Internet of Things and the Internet of Values, along with the key features and risks they carry. The huge amount of data created by the interaction of people and devices leads to the need for their analysis by the Big Data method, which will be the focus of the second part of the paper. The impact of these concepts on privacy of electronic payment systems customers, as well as possible future implications, will be analyzed in the third part of the paper.

Internet of Things

The Internet of Things starts with the formation of intelligent infrastructure, which connects objects and people through a computer network. It enables both humans and machines to universally coordinate resources through remote monitoring and control (Brock, 2001, p. 5). It is a virtual world made up of elements capable of making decisions, which are constantly interacting. Adding processors to some of the objects in the human environment transforms them into "smart objects". Developments in this field are largely due to the advancement of Machine-to-Machine (M2M) communication, which has made it possible to connect devices with autonomous communication capability without human intervention (Kimani et al., 2019, p. 36). These devices have the ability, not only to collect information from users but also to further exchange information (Borgia, 2014, p. 1).

Numerous industries, from healthcare, through manufacturing, commerce and transportation, have transformed their services based on the use of smart devices. More than 46 billion devices are expected to be connected worldwide by 2021 (Tsiatsis et al., 2019, p. 31). According to the authors' forecasts, by the year 2020, returns of $ 7.1 billion are expected worldwide from the use of the IoT (Lund et al., 2014). At the same time, with the expansion of IoT devices, the world faces numerous challenges in maintaining data security and privacy.

Unlike traditional networks that are provided with complex, multiple factors of security protocols, IoT systems require the use of lightweight security algorithms to maintain a balance between security and resource consumption such as - battery life, memory status, or processor load (Makhdoom et al. 2018, p. 253). Therefore, the overall architecture of the IoT environment is comprised of devices characterized by unique recognition, low processing power and memory capacity, which further leads to a limited ability to process data (Khan & Salah, 2018, p. 396). Despite these features, connecting devices through gateways that link one protocol to another creates the ability to transfer large amounts of data. Data creation can occur in any part of the IoT environment, whether it is a "smart" device, the Internet, or any of the online spaces (such as Cloud). Hou, Qu, & Shi (2018) point out that over the past two years, 90% of the world's data has been generated at a rate of 250,000 gigabytes per second, which is roughly equivalent to 150 million books. Information security is largely focused on finding specific solutions for the virtual space where data moves from IoT devices to the border of Internet.

With the increasing technical and technological progress there is a suppression of the risk of system malfunctioning and an increase in the risk of fraud. Within the IoT, the risk of fraud originates from the application of non-standardized technology that increases the vulnerability of the entire system. Attacks that may occur are directed to the privacy and confidentiality of the user's data. In order to provide greater information security, Weber (2010) outlines the following requirements:

- Attack Resistance - The system should avoid single points of failure and adapt to the key nodes where failure occurs;
- Data authentication - The downloaded addresses and object information must be authenticated;
- Access control - information providers must be able to implement control of access to databases;
- Client privacy - steps should be taken to ensure that only the information provider is able to draw conclusions by observing a customer-specific search system.

The IoT concept is the basis of future business communication. However, adequate utilization of the payment infrastructure is required to fully exploit the potential that will be created through the networking of people and devices. Integrating payments into the IoT will provide a higher form of communication connectivity, called Internet of Value (IoV). The key idea within the IoV is to build an adequate technical and technological basis for safe and fast transfer of value. This is not just about monetary value, but also about the transfer of dematerialized securities, contracts or intellectual property. The transfer should take place without the need for a third party, at no additional cost in comparison to those that would have incurred the transfer of ordinary information.

Building an adequate infrastructure involves striking a balance between high security requirements and acceptable costs. It is thought that blockchain technology could satisfy both requirements. A blockchain technology creates databases made up of a series of blocks such that each new block is cryptographically linked to the previous one (Minoli & Occhiogrosso, 2018, p. 255). The transmitted information are parts of the chains of blocks, with each block storing a set of transactions at a specified time. Reliability is enhanced by the possibility of verification, audit and monitoring from the first transaction that occurs in the system (Reyna et al., 2018, p. 176). This also achieves a high level of transparency that helps in building trust with clients.

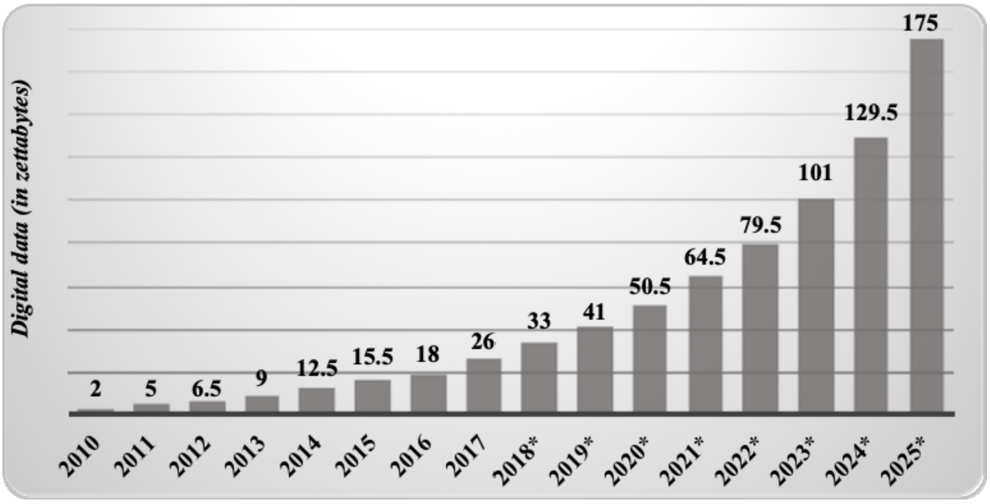
The blockchain mechanism was originally intended for transfer of financial values. This is also supported by key features such as speed, low cost and reliable transaction transfer. Blockchain is increasingly mentioned in the literature as a tool for addressing security and privacy issues of the IoT, owing to its decentralized architecture, fault tolerance, and cryptographic security features, such as pseudonym, data integrity, and authentication, (Minoli & Occhiogrosso, 2018, p. 251). Therefore, embedding blockchain in applications is considered a good way to form a secure payment system. The challenge that arises is the daily growth of such databases. Consequently, formation of too big databases can have adverse effects on performance (e.g., increasing synchronization time for new users) (Reyna et al., 2018, p. 175).

2. Electronic payment systems in a Big Data world

The vast amount of data generated by IoT devices and social networks can be used to create the information needed to make decisions. However, standard data management tools cannot adequately and quickly analyze received inputs (Alam et al., 2014, pp. 446). There is a mass of data, the use of which makes sense only with very short time delay, which practically requires real-time analysis. This means that business entities are facing an increasing volume of data whose heterogeneity and dynamics of emergence create additional problems (Lukić, 2014, p. 227). The revised approach to data management is referred to as Big Data in the literature (Ghani et al., 2019). By using new software solutions for processing, storing and connecting data, companies can find hidden schemes and patterns. Based on new information, it is possible to personalize the offer not only to groups but also to each customer individually. Torrecilla & Romo (2018) highlight two major advantages of the Big Data concept. The first one relates to the fact that businesses collect potentially valuable customer information at low cost. The second one relates to the adoption of more successful and better decisions by governing bodies, since such decisions are made in accordance with research based on the collected data.

There are estimates that the total amount of digital data created globally will increase from about 30 zettabytes, as estimated for 2018, to 175 zettabytes by the end of 2025 (Chart 1). The rapid growth has also been attributed to the continued growth in the number of Internet connections and social networks users, the migration from analogue to digital television and the spread of information-sensitive technologies, such as surveillance cameras, microphones, radio frequency identification readers and wireless communications networks (Gantz & Reinsel, 2013).

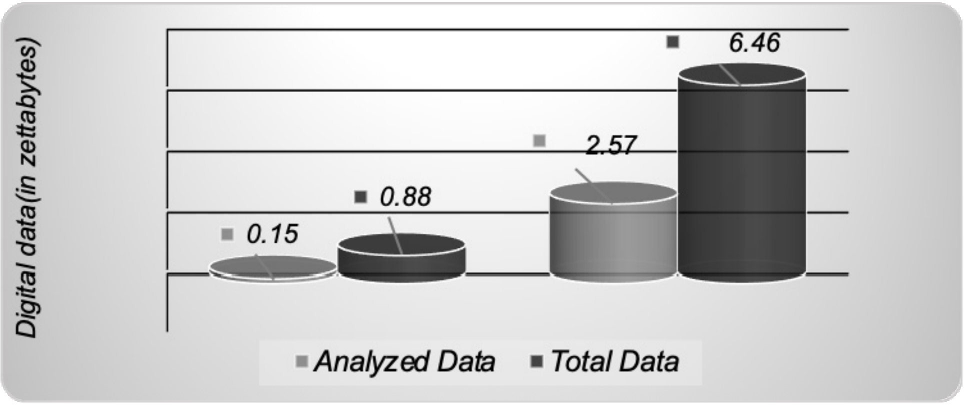
Chart 1: Trend of global creation of digital data



Source: https://www.statista.com/statistics/949144/worldwide-global-datasphere-real-time-data-annual-size/

The same authors showed that in 2013, monitoring and analyzing of only 18% of the United States' total amount of digital data produced some benefit in creating information. It is predicted that this percentage would be much higher in the future, as much as 40% of total data - see Chart 2.

Chart 2: Share of analyzed data in total data



Source: Gantz, J., & Reinsel, D. (2013). The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the Far East (IDC iView)

Electronic payments provide the basis for the application of modern data management tools. With the exception of the electronic money, transactions with all other electronic payment systems are finalized through the standard payment infrastructure. This means that all transactions via credit cards, mobile digital wallets or some other system, such as PayPal, are made by transferring funds from a current account or a credit card account in a bank. Companies that manage payment systems can collect a large amount of customer information which they can use to profile them. A customer's digital identity in addition to various online information such as usernames, passwords, PINs and access codes includes a wide range of offline features that can be tracked (e.g. age, residence, income) (Eastin et al., 2016, p. 215).

Data management requires some knowledge, storage space, and software solutions. Many companies either cannot meet these requirements or do not have a direct relationship with customers, so they cannot collect data. Therefore, monetization of the collected data is a very important aspect of ICT companies' business. The best example is Facebook, which makes money based on data users willingly share. In addition to demographic data, the interests of users are of great importance, both those that are explicitly listed and those that social network algorithms perceive from interacting with other users. In this way, Facebook creates a psychological profile of every user, which is the basis for offering new content. Companies looking to leverage the powerful tools that Facebook has at disposal pay to distribute their content to users.

A significant problem in ensuring digital security at present is legal uncertainty regarding the regulatory definition of the concept and disclosure of the content of such an objective phenomenon as "the digital form of existence of information, the exchange and operation of it" (Aryamov et al., 2019, p. 2). The concern for the information privacy is enhanced by examples of personal data leaks from databases of

ICT companies, financial institutions and the public sector. Eastin et al. (2016) identify the following determinants that influence the raising awareness of data privacy - data collection settings, data control, unauthorized secondary use, improper access, location monitoring. Greater concern also leads to the strengthening of the individual's interest in protecting personal information. The conflict of interest that arises between privacy protection and public benefit makes it difficult to collect personal information, even when government agencies appear as data collectors (Lee et al., 2019, p. 294). Although it seems difficult, a clear line can be drawn between privacy and data protection. While data protection is one of the segments of privacy within which the collection, use and dissemination of private information occurs, privacy as a broader term also includes various forms of intrusive behavior (wiretapping, concealment, physical surveillance, interception of mail, etc.) (Anić et al. 2018, p. 17).

3. Concept of privacy in electronic payment systems

Today, much of the communication takes place on the Internet, leaving traces that reveal the interests, traits, intentions and beliefs of individuals (Acquisti et al., 2015, p. 509). Electronic communication has enabled the collection and non-transparent management of personal data by other individuals, businesses and governments. Therefore, individuals are often unaware who has access to their data and what he or she can do with them. Defining the concept of privacy, Buchanan et al. (2006) have pointed to some of the following dimensions:

- *Informational privacy* - the right of an individual to determine how, when and how much information he or she will share with others;
- *Privacy accessibility* – it overlaps with informational privacy in cases when taking over or the intention to retrieve information involves accessing to an individual. It also applies to cases where physical access is compromised (e.g. intrusion by spam or computer viruses);
- *The physical dimension of privacy* - the degree to which a person is physically accessible to others;
- *Expressive privacy* – one's ability to protect the area for expressing identity and personality through speech or activity while enhancing the intrinsic ability to build interpersonal relationships;
- *The social-communication dimension of privacy* - an individual's ability to control social contacts.

Informational privacy has been at the center of academic interest for more than two decades. At the very beginning of electronic business, the focus was on e-commerce and building an adequate e-payment infrastructure. Over time, customers became aware that their personal information are being used, which influenced the development of strategies regarding the protection of informational privacy. However, despite concerns, not only that personal data sharing have not ceased, but the volume and variety of shared data have increased over time. The distinction between attitudes and behavior in the literature has been characterized as a privacy paradox (Acquisti, et al., 2015; Anić et al., 2018). The authors explain the emergence of this phenomenon in the volatility of individuals' attitudes toward privacy, where change is influenced by the prevailing costs and benefits of a particular situation (Acquisti, 2004; Acquisti, et al., 2015; Eastin et al., 2016). Smith, Dinev and Xu (2011) state that when assessing such a situation, customers consider three types of benefits they can gain by disclosing personal information: financial rewards, personalization, and the benefits of social adjustment. Cost-benefit calculation, in services that are loaded with compromising informational privacy, has been referred to in the literature as the privacy calculation (Anić et al., 2018, p. 31).

On one hand, the problem is that customers often do not realize the value of privacy until they lose it. On the other hand, they are often suggested that privacy is a brake on the development of safer and more efficient systems. For example, it is stated that the system would be more resistant to identity theft if customers were willing to share more personal information. If a customer logs on to a network from a geographical location where he has never been present before, or sends a payment to a recipient on another continent, the system could recognize the illogicality and respond by asking for additional confirmations, sending an email alert or blocking an account. Although at first glance it seems like an ideal solution, it implies that the system would need to monitor customer's physical movement and analyze the amounts of payments and identities of recipients.

The question is what a company that poses so much data wants or can do with it. One option is to create personalized payment services in the form of microcredit for individual participants. Selling data to internet marketers is another option, as these companies could prepare personalized offers based on the experience of previous payments. Finally, a company with a large amount of payment information would probably be under a lot of pressure from the authorities to make the data available. After the terrorist attacks in the early 21st century, the Western states repeatedly passed laws that gave their governments the power to usurp citizens' privacy in order to maintain public security.

However, an essential problem is the interpretation of public safety. While citizens believe that the goal is to find financiers and participants in terrorist acts, states actually have a basis to follow anyone who is labelled suspicious. In practice, just because terrorists buy large quantities of artificial fertilizer to make explosives, anyone who buys artificial fertilizer and is not a farmer can be labelled suspicious. In addition to further data collection, such individuals may face account blocking or asset forfeiture. The problem comes from the large amount of processed data, in which some facts can coincidentally match with predefined patterns of dangerous behavior. Instead of raising public safety, sacrificing privacy can actually reduce the security of individuals and expose them to problems, as in the example above.

It is often stated that cash is suitable for the informal economy and terrorist financing and should therefore be withdrawn. While this is true, the fact is that criminals and terrorists have been able to find ways to fund their activities without cash. An example is the continuous existence of the Islamic State, a terrorist organization that has operated in multiple countries in the Middle East and gathered tens of thousands of followers from around the world. The organization has always been well-armed and equipped, often with the newest off-road vehicles from the world's largest manufacturers, but its financial flows have never been revealed (Engel, 2015). In preparation for the 2015 terrorist attack in Paris, attackers used pre-paid payment cards to pay for logistics material (Guarascio, 2015). Such cards are anonymous and do not require customer's name when issued. In other words, criminals and terrorists find a way to stay out of reach of authorities despite the strictness of regulations, while in fact conscientious citizens lose some of their personal freedoms.

The electronic payment system starts from decentralized structure, which contrasts with the existing hierarchically ordered and a centralized structure, which has an inherent reliance on credible payment intermediaries (Lukić & Živković, 2018, p.164). Therefore, withdrawing cash will not reduce the ability to perform undesirable actions. On the contrary, the disappearance of cash can only destabilize economies (Tomić & Todorović, 2018, p. 316). On one hand, a fully electronic payment system would enable states to fully control economic life, creating an unprecedented space for abuse and corruption. Funds could be blocked or confiscated to both individuals and companies that appear to be ineligible for any reason. The power to make decisions with such far-reaching consequences quickly and easily would inevitably lead to abuses. On the other hand, a large number of customers would be unprepared for absence of cash and switching to fully electronic payments. The readiness of the system itself and technical perfection would also be an issue.

In addition to withdrawing cash, there are some other tendencies that can further compromise customers' privacy. On June 18, Facebook released a white paper on intentions to develop its own cryptocurrency, Libra, with a consortium of financial and technological companies. The document states that transaction accounts will not be associated with a user's personal identity (libra.org). However, the fact that the digital wallet - called Calibra - will be integrated into Facebook Messenger and WhatsApp applications suggests that the company plans to integrate its users' financial and personal information. Users can be offered to separate digital wallets from social networks accounts, with promises that integration prevents unauthorized access to funds. One should not expect that Facebook would miss the opportunity to integrate those data. An insight into the history of transactions would create an incomparably greater potential for monetization of users' privacy. It is known that Facebook have sold collected data to third parties in the past, as well as having ceded them to state intelligence agencies. Therefore, integrating social networks data with personal transaction history would be a great danger for each individual.

The Shazam mobile application is a good example of machine learning. Based on the sounds collected by the mobile phone's microphone, the application is able to recognize the song the user is listening and to provide basic information about it. The internet is the largest megastore of today - Amazon - has announced it will start using an application that will identify photographed pieces of clothes and provide a buyer with a link (Hanbury, 2019). It should be expected that the algorithm remembers what kind of clothes users are searching for, and then start to independently suggest similar items to them. However, this is not the biggest problem with machine learning. In the case of withdrawal of cash, governments could theoretically have an insight into all performed transactions, as they would all be initiated electronically. If part of the transactions were to be carried out anonymously using pre-paid cards or electronic money, participants would not be able to be identified. However, machine learning based software could consider the origin, time of day, day of the week, transaction amount and content of the purchase, and compare them to known patterns of identified users. In case the software works perfectly, no transaction would be anonymous. In the case of imperfections, users would be at risk of being misidentified and classified as suspicious.

Another problem is the lack of awareness of the information volume shared with others. Cellary and Rykowski (2015) distinguish financial transactions occurring within the Visible versus the Invisible Internet. Substantial differences in the functioning and sharing information influenced this of classification. Visible Internet connects individuals who, on their own initiative, initiate certain actions (opening an application, prompting for a specific action, etc.) using computers and software to access the network. Users are aware what information about them can be collected and who collects them, although even then they cannot know for what purpose they will be used. In the Invisible Internet, procedures are being unconsciously initiated using IoT connections, whereby users cannot detect how many devices are connected and what information is collected. When it comes to financial transactions, the differences are also obvious. While services are paid directly or indirectly in the Visible Internet, requiring payment participants to be identified, services in the Invisible Internet are offered at random, most often by geographical location (Cellary & Rykowski, 2015, p. 3).

The presentation so far was about the possibility of deliberate and planned misuse of users' personal data. Equally dangerous is the inadvertent data management, or their poor protection in storage. Databases that have no cryptographic security, located on servers connected to the Internet, have a great chance of being usurped. Attacks on databases can occur from outside, by hacking groups, or from the inside, by malicious employees. If the payment authentication information is usurped, users could lose financial resources in addition to privacy. Some examples of usurping large amounts of data are (Johnson et al., 2018):

- Target Corporation – in 2008 and 2013, payment information of over 100 million users leaked to the public;
- Sony Online Entertainment – the intrusion on private networks in 2014 resulted in 102 million compromised user accounts;
- JP Morgan Chase – In 2014, hackers gained access to personal information related to 76 million personal accounts and 7 million small business accounts;
- Home Depot - compromised data of more than 56 million credit and debit card users.

The potential violation of privacy by using IoT could be far greater than in the current conditions of Internet communication (Tomić & Todorović, 2017, p. 102). In order to provide personalized services that fully meet the needs of an individual, it is necessary to collect a large amount of private information. In an effort to reach a compromise between personalization and privacy, Cellary and Rykowski (2015) propose a license-plate approach. Similar to the vehicle authentication in a smart environment, the license - plate approach assumes that a trusted third-party issues digital tags, as public administration offices do in the real world. With the help of a digital tag, the smart environment operator obtains the information needed to personalize the service under client-defined conditions. In each iteration, a different identifier would be used, avoiding thus the usage of previously collected information.

Conclusion

Maintaining data privacy in the modern digital age is a real challenge. The following dilemma arises: smart devices or security, that is, how much can people trust a service provider if one considers the potential risk of fraud? This type of risk is especially pronounced with electronic payment systems. Although all payment systems experience security issues, the specific features of electronic payment systems in the IoT environment have increased the risk of user's data abuse. The risk of fraud comes from the use of non-standardized technology, which increases the vulnerability of the entire system. The vast amount of data that goes through payment systems can provide insight into consumer spending patterns, as well as a potential mechanism to identify and prevent fraud.

The digital age is erasing the boundaries of information privacy slowly. Creating a secure electronic payment system in a smart environment requires protection against unauthorized access to the network and user data. Expectations for IoT in the future are high, especially with regard to micro and pico payments, whose expansion is becoming more certain. But it must also be remembered that these expectations can remain unfulfilled unless the way for overcoming challenges is provided. It is important that the biggest turning point in the field of data protection is expected from the integration of IoT with blockchain technology, which can provide a reliable channel for transmitting information. The inclusion of blockchain technology in the electronic payment systems architecture in the IoT environment is a recommendation for all future research.

Theoretical analysis in the paper provides an opportunity to fully understand the threat to privacy in contemporary conditions. The results show that it is crucial for electronic payment systems to improve the level of financial transaction security as new technology evolves. Regulatory changes in the domain of privacy are necessary, not only for the area of unauthorized downloading data, but also for their further processing. The world needs a global consensus on what data should be considered as private and what rules should be applied to collecting, storing, distributing and processing it. The question is no longer what the best way for protecting privacy is, but when privacy does not need to be protected, and when protection is imperative at all costs.

References

Acquisti, A. (2004). Privacy in Electronic Commerce and the Economics of Immediate Gratification. In: Proceedings of the 5th ACM Conference on Electronic Commerce-EC ’04. USA, New York: ACM. Doi: https://doi.org/10.1145/988772.988777

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509–514. Doi: https://doi.org/10.1126/science.aaa1465

Alam, J.R., Sajid, A., Talib, R. & Niaz, M. (2014). A Review on the Role of Big Data in Business. International Journal of Computer Science and Mobile Computing, 3(4), 446-453.

Anić, I-D., Budak, J., Rajh, E., Recher, V., Škare, V., Škrinjarić, B., Žokalj, M. (2018). The Extended Model of Online Privacy Concern. Zagreb: The Institute of Economics.

Aryamov, A., Grachova, V., Chuchaev, I., & Malikov, V. (2019). Digital asset as an object legal regulation. Ekonomika, 65(2), 1-11. Doi:https://doi.org/10.5937/ekonomika1902001A

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. Computer Communications, 54, 1–31. doi: https://doi.org/10.1016/j.comcom.2014.09.008

Brock, D. L. (2001). Whitepaper - The Electronic Product Code (EPC) - A Naming Scheme for Physical Objects. Retrieved June 22, 2019, from https://wenku.baidu.com/view/46155a4733687e21af45a95e.html

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2006). Development ofmeasures of online privacy concern and protection for use on the Internet. Journal of the American Society for Information Science and Technology, 58(2), 157–165. Doi: https://doi.org/10.1002/asi.20459

Cellary, W., & Rykowski, J. (2015). Challenges of Smart Industries – Privacy and payment in Visible versus Unseen Internet. Government Information Quarterly, 1-7. Doi: https://doi.org/10.1016/j.giq.2015.08.005

Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. Computers in Human Behavior, 58, 214–220. Doi: https://doi.org/10.1016/j.chb.2015.12.050

Engel, P. (2015, October 7) These Toyota trucks are popular with terrorists — here's why, Business Insider. Available at: https://www.businessinsider.com/why-isis-uses-toyota-trucks-2015-10

Gantz, J., & Reinsel, D. (2013). The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the Far East (IDC iView). Retrieved July 5, 2019, from https://www.emc.com/leadership/digital-universe/2012iview/index.htm

Ghani, N. A., Hamid, S., Targio Hashem, I. A., & Ahmed, E. (2019). Social media big data analytics: a survey. Computers in Human Behavior, 101, 417-428. Doi: https://doi.org/10.1016/j.chb.2018.08.039

Global data sphere real time data total size worldwide from 2010 to 2025. (2019). https://www.statista.com/statistics/949144/worldwide-global-datasphere-real-time-data-annual-size/ (Accessed on: 23th July 2019)

Guarascio, F. (2015, November 21) The EU is stepping up controls on Bitcoin and prepaid cards to help block terrorist funding, Business Insider. Available at: https://www.businessinsider.com/r-eu-steps-up-controls-on-bitcoin-pre-paid-cards-to-curb-terrorist-funds-2015-11

Hanbury, J. (2019, Jun 6) Amazon is launching the Shazam for fashion, which finds clothes you want simply by analyzing a photo, Business Insider. Available at: https://www.businessinsider.com.au/amazon-launches-shazam-for-clothes-2019-6

Hou, J., Qu, L., & Shi, W. (2018). A Survey on Internet of Things Security from Data Perspectives. Computer Networks, (148), 295-306. Doi: https://doi.org/10.1016/j.comnet.2018.11.026

Johnson, V. L., Kiser, A., Washington, R., & Torres, R. (2018). Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services. Computers in Human Behavior, 79, 111–122. Doi: https://doi.org/10.1016/j.chb.2017.10.035

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. Doi: https://doi.org/10.1016/j.future.2017.11.022

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber Security Challenges for IoT-based Smart Grid Networks. International Journal of Critical Infrastructure Protection, 25, 36-49. Doi: https://doi.org/10.1016/j.ijcip.2019.01.001

Lee, H., Wong, S. F., Oh, J., & Chang, Y. (2019). Information privacy concerns and demographic characteristics: Data from a Korean media panel survey. Government Information Quarterly, 36(2), 294-303. Doi: https://doi.org/10.1016/j.giq.2019.01.002

Libra Association Members. (2019). White Paper - An Introduction to Libra. Retrieved July 28, 2019, from https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/LibraWhitePaper_en_US.pdf

Lund, D., MacGillivray, C., Turner, V., & Morales, M. (2014). Worldwide and Regional Internet of Things (IoT) 2014–2020 Forecast: a Virtuous Circle of Proven Value and Demand. International Data Corporation (IDC). Retrieved July, 8, 2019, from https://studylib.net/doc/13054228/worldwide-and-regional-internet-of-things--iot--2014–2020

Lukić, J. (2014). The impact of information and communication technology on decision making process in the Big Data Era. Megatrend revija, 11(2), 221-233. Doi: https://doi.org/10.5937//MegRev140221L

Lukić, V., & Živković, A. (2018). The consequences of digital revolution in monetary realm. Anali Ekonomskog fakulteta u Subotici, (39), 157-170. Doi: https://doi.org/10.5937/AnEkSub1839157L

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2018). Blockchain's adoption in IoT: The challenges, and a way forward. Journal of Network and Computer Applications, (125), 251-279. Doi: https://doi.org/10.1016/j.jnca.2018.10.019

Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. Internet of Things, (1-2), 1-13. Doi: https://doi.org/10.1016/j.iot.2018.05.002

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, (88), 173–190. Doi: https://doi.org/10.1016/j.future.2018.05.046

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. MIS Quarterly, 35(4), 989-1015. Doi: https://doi.org/10.2307/41409970

Tomić, N., & Todorović, V. (2017). The future of payments in the Internet of Things. Internet and Development Perspectives. Paper presented at Sinteza 2017 - International

Scientific Conference on Information Technology and Data Related Research. Doi: https://doi.org/10.15308/Sinteza-2017-97-104

Tomić, N., & Todorović, V. (2018) Challenges of transition to cashless society. Contemporary issues in Economics, business and management – EBM 2018 [proceedings of the international scientific conference], Kragujevac: Faculty of Economics, 313-320.

Torrecilla, J. L., & Romo, J. (2018). Data learning from big data. Statistics & Probability Letters, (136), 15–19. Doi: https://doi.org/10.1016/j.spl.2018.02.038

Tsiatsis, V., Karnouskos, S., Höller, J., Boyle, D., & Mulligan, C. (2019). Origins and IoT Landscape. In book: Internet of Things, 2nd edition, 9–30. Doi: https://doi.org/10.1016/B978-0-12-814435-0.00013-4

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23–30. Doi: https://doi.org/10.1016/j.clsr.2009.11.008