

# ERP SYSTEM SECURITY THROUGH THE EYES OF USERS: EVIDENCE FROM SERBIAN ENTERPRISES

Sanela Arsić<sup>1</sup>, Aleksandra Radić<sup>1</sup>, Đorđe Nikolić<sup>1</sup>

<sup>1</sup>Engineering Management Department, Technical Faculty in Bor, University of Belgrade, Vojske Jugoslavije 12, 19210 Bor, Serbia

DOI: [https://doi.org/10.11118/ecos2026\\_001](https://doi.org/10.11118/ecos2026_001)

## ABSTRACT

Enterprise resource planning (ERP) systems are integrated business platforms characterised by a high need for security, which is a fundamental requirement for efficient operation. Although many vendors include comprehensive security mechanisms in their ERP solutions, user perceptions of security are also crucial for adequate system adoption. This study examines users' perceptions of ERP system security and reliability in relation to demographic characteristics. Analysis of Variance (ANOVA) was used to identify differences in responses. The empirical research included a sample of 206 ERP system users from organisations in Serbia. The ANOVA results show that user perceptions differ significantly by users' level of education, the organisation's industry sector and economic activity, and the frequency and duration of system use. These findings provide valuable insights into variations in perceptions of ERP system security and help identify behavioural patterns influenced by demographic factors.

**Keywords:** ERP systems, security perception, user behaviour, ANOVA, demographic factors

**JEL Code:** M15, O33, D83

## 1 INTRODUCTION

Enterprise Resource Planning (ERP) systems are integrated information platforms that enable the planning, organisation, monitoring, and control of business processes in real time (Hussain *et al.*, 2024). In many industries, ERP is considered essential for conducting business activities, as it allows companies to achieve high performance. Additionally, ERP connects many participants simultaneously, uniting internal and external information flows, the integrity of which is crucial for the company.

Any unauthorised access to the vast amount of data stored in an ERP system can result in significant financial and reputational losses, making the security and reliability of ERP systems among the most critical issues in modern business (Michelberger & Horváth, 2017). A study by Salih *et al.*



This article is licensed under CC BY-SA 4.0 Attribution-ShareAlike 4.0 International license. <https://creativecommons.org/licenses/by-sa/4.0/deed.en>

(2021) found that ERP system security is the most widely cited impacting factor, indicating that security is a critical consideration in examining ERP implementation and usage success.

ERP insecurity can lead to costly consequences for organisations, affecting both operational performance and long-term stability. SAP, one of the leading ERP vendors, reported that in 2021, every 11 seconds a company was hit by ransomware, while the average cost of recovering from a ransomware attack was \$1.85 million (SAP, n.d.). Recently, ERP security has changed dramatically as cybersecurity threats have become more sophisticated, with AI-powered attacks increasing by 95% in 2024 alone (Gangapatnam, 2025).

Current research addresses the technical aspects of ERP security (Boppana *et al.*, 2021; May *et al.*, 2024) and models for their improvement (Atakari, 2024; Annapareddy, 2025; Nittala, 2025). However, the human factor remains the most crucial element for successful system application and use (Almahamid, 2019). Specifically, user perceptions of ERP security are critical for effective system adoption. Perceived security refers to users' perceptions of the reliability and safety of ERP service delivery, the robustness of the system's technical architecture, and the adequacy of its security requirements. Users' attitudes and awareness significantly shape how ERP systems are adopted, used, and safeguarded in everyday operations. Research by Kuo *et al.* (2023) demonstrated that perceived security has a statistically significant impact on ERP users' continued usage intention, indicating that users regard ERP security as an important factor that leads to perceiving ERP as more useful and user-friendly.

Nevertheless, there is a clear need for further research to understand the behavioural issues of ERP users shaped by their psychological beliefs (Salih *et al.*, 2021). Therefore, additional studies are needed to explore the behavioural and cognitive aspects of ERP system introduction in business operations.

The main objective of the study is to provide contemporary insights into differences in ERP users' security perceptions, based on empirical evidence tested using a statistical approach. Such results and implications assist ERP vendors in the process of ERP solution development and ERP consultants in achieving more successful ERP system acceptance during implementation.

Considering all the above, this paper examines ERP security from the users' perspective, emphasising the impact of users' demographic variables on perceived ERP system reliability and security in specific country context. To achieve this aim, an Analysis of Variance (ANOVA) was used to identify differences in users' responses obtained through empirical research, which included a sample of 206 ERP system users from organisations in Serbia.

The paper is organised as follows. After the Introduction, the Theoretical Background reviews previous literature and highlights its main findings, while Hypotheses Formulation section proposes the study research hypotheses. The Research Method section details data collection and the methodology used to process the data. The Results and Discussion section presents the main results and considers the findings. The Conclusion summarises the implications and limitations and outlines the future research agenda.

## 2 THEORETICAL BACKGROUND

Integrating an enterprise's diverse functions through the implementation of a unique ERP system offers numerous benefits. However, during the implementation process, enterprises may encounter several challenges, such as customisation, data migration, user training, and integration with existing systems (Siraj *et al.*, 2024). From the user's perspective, ERP security is not merely a technical constraint but a functional framework. As users operate across departmental boundaries, including finance, procurement, production, and logistics, the seamless integration of access controls and approval workflows is vital (Shish, 2025). Due to the increasing complexity and sophistication of cyber threats, ERP implementation poses a greater risk to the integrity and functionality of these systems.

Among the most significant threats are malware attacks, which can lead to data corruption or theft, as well as phishing and other forms of social engineering that exploit human weaknesses to gain unauthorised access. Distributed denial-of-service attacks can overload a system and cause downtime, while zero-day attacks exploit vulnerabilities for which security patches are not yet available, making them particularly dangerous. The most sophisticated attacks enable perpetrators to maintain a long-term presence in the network and systematically compromise data (Efe, 2024). Insufficient preparation and neglect of security in ERP projects can lead to failure, as key controls are often left until the end of implementation, when budgets are exceeded and deadlines missed. This practice results in significant system vulnerabilities. Morrisson (2020) states that this approach stems from the misconception that ERP is exclusively an IT project, whereas in reality it requires the engagement and responsibility of the entire enterprise.

This highlights the need to emphasise the importance of the user's role in ERP security. The main goal of ERP security is to reduce the risk of information loss, ensure compliance with state and corporate standards, protect the privacy of internal data, and preserve its integrity (Efe, 2024). ERP system security can be defined as the degree to which the ERP system is regarded as secure for data storage, data exchange, and other business operations (Salih *et al.*, 2021).

Although technical protection measures are important, contemporary literature increasingly emphasises that the human factor is the weakest, yet most important, link in the chain of defence (Triplett, 2022). In current discourse on ERP systems, security is no longer viewed solely through the lens of cryptographic algorithms and technical barriers, but as a complex socio-technical phenomenon centred on human behaviour. Users' awareness and attitudes directly shape how ERP systems are used and protected in daily work (Kuo *et al.*, 2023; Shish, 2025).

Examining ERP system security within the context of Serbian enterprises is particularly important given the heterogeneous levels of digital maturity, organisational practices, and user competencies present in transition economies. While ERP systems are increasingly adopted by organisations in Serbia, variations in implementation quality, user training, and security governance may influence how security and reliability are perceived by end users.

Regarding ERP security in Serbian enterprises, this issue represents a unique combination of strict legal regulations, accelerated digitisation (such as the introduction of e-invoices), and a specific mentality regarding data storage. A particular feature of Serbia is the mandatory use of the Electronic Invoice System, which has introduced new security challenges, such as the requirement that the connection between the local ERP and the national portal must be encrypted and protected by digital certificates to avoid the risk of interception.

Traditionally, most Serbian enterprises have preferred on-premise ERP systems and local data storage. However, this trend is changing, with an increasing number of companies adopting cloud ERP. Nevertheless, research by Ivanović and Marić (2021) shows that over 50% of surveyed

companies wish to switch to cloud ERP technology, but 40% of respondents agree that the major barrier is the problem of data security and safety.

Such insights are essential for designing more effective security policies, user training programmes, and system configurations that align with users' expectations and behaviours. By focusing on the Serbian context, this study contributes to the broader literature by providing context-sensitive evidence on ERP system security from the users' perspective in an underexplored empirical setting.

### 3 HYPOTHESES FORMULATION

To support the study's objectives, this section presents hypotheses drawn from previous research. The hypotheses were primarily based on previous international ERP and information systems literature, as empirical studies specifically examining perceived ERP security and reliability in the Serbian context are limited. Furthermore, examining these relationships in Serbia is particularly relevant, as transition economies may differ from others. Consequently, the study replicates previous findings and contextualises them within a less frequently investigated context. The proposed hypotheses will be tested to determine how perceptions differ by users' age, education level, organisation's industry sector, economic activity, company size, user experience, and frequency of system use.

Previous research found that males dominate information systems adoption (Kusumaningtyas & Suwanto, 2015). McGill and Thompson (2021) reported that women perceive lower levels of information security and privacy than men, and behaviours requiring greater technical skill are less frequently adopted by female users. Therefore, this study proposes the following hypothesis H1:

***H1. There is a statistically significant difference in perceived ERP security and reliability between males and females.***

Earlier studies identified a positive relationship between age and information system use, as older individuals have limited knowledge and training regarding computers (Elsadaani, 2013). Additionally, younger people adopt IS more readily than older generations (Kusumaningtyas & Suwanto, 2015). Based on this, the study proposes the following hypothesis H2:

***H2. There is a statistically significant difference in perceived ERP security and reliability based on ERP users' age.***

Olatokun (2009) found that education level is linked to the technology usage gap. Previous literature (Davis, 1989; Venkatesh & Bala, 2008) indicates that perceptions of ERP system acceptance are often influenced by education. Therefore, this study proposes the following hypothesis H3:

***H3. There is a statistically significant difference in perceived ERP security and reliability based on ERP users' education level.***

Despite industry specialisation, manufacturing and services remain the two main economic activities and may represent distinct groups of ERP system users. Previous literature (Ruivo *et al.*, 2017) suggests that manufacturing and service industries have different processes and types of data stored in the system (Ifinedo, 2012), which can affect perceptions of ERP security. Based on this, the study proposes the following hypothesis H4:

***H4. There is a statistically significant difference in perceived ERP security and reliability based on the industry sector background of ERP users.***

Abu Afifa *et al.* (2023) examined users' attitudes towards ERP use in the financial, service, and manufacturing sectors. The study found that ERP adoption is higher in manufacturing than in service and financial sectors. Mishra *et al.* (2022) also highlighted distinct cybersecurity issues in enterprises with different economic activities. Thus, this study proposes H5:

***H5. There is a statistically significant difference in perceived ERP security and reliability based on the economic activity background of ERP users.***

Regarding company size, Johansson *et al.* (2015) demonstrated that as enterprise size increases, the complexity and scale of ERP security issues also become more significant. The challenge of managing user permissions, ensuring regulatory compliance, and maintaining system integrity is greater in larger enterprises (Mishra *et al.*, 2022). Accordingly, this study proposes the following hypothesis H6:

***H6. There is a statistically significant difference in perceived ERP security and reliability based on the company size in which ERP users are employed.***

Previous literature indicates that user experience with an ERP system positively affects perceived system security (Bhattacharjee, 2001). Greater exposure to an ERP system increases users' security awareness and understanding of their responsibilities in maintaining system security (Seneviratne & Colombage, 2023). Therefore, this study proposes the following hypothesis H7:

***H7. There is a statistically significant difference in perceived ERP security and reliability based on ERP users' experience.***

The frequency of ERP system use is positively correlated with users' perceptions of security and reliability (Workman *et al.*, 2009). It influences user familiarity with the system and the trust developed through repeated interaction. Based on this, the study proposes the following hypothesis H8:

***H8. There is a statistically significant difference in perceived ERP security and reliability based on the frequency of system use by ERP users.***

## 4 RESEARCH METHOD

To assess user beliefs and attitudes regarding the acceptance and use of ERP systems, an empirical survey was conducted in 2024. Data were collected through an online questionnaire created in Google Forms and distributed via the LinkedIn network to ERP users employed in enterprises operating in Serbia. Participants were informed that their responses would be used exclusively for scientific research purposes.

The distributed questionnaire consisted of two parts. The first part included users' demographic questions, while the second comprised items related to ERP system acceptance and use. The questionnaire used in this study was adapted from Sternad Zabukovšek *et al.* (2019) and covered a wide range of constructs examining drivers influencing ERP system usage, such as perceived usefulness, ease of use, work compatibility, and external factors. Respondents rated their agreement on a five-point Likert scale, where 1 indicated the lowest level of agreement and 5 the highest. Among the items included under external factors was a statement addressing the reliability and security of ERP systems, as this is an important aspect of successful ERP implementation and continued use.

Furthermore, to examine the influence of demographic factors on perceived ERP system security and reliability, an Analysis of Variance (ANOVA) was applied. This statistical analysis was performed using the IBM SPSS v.25 software package.

The ANOVA test is a statistical technique used to determine whether there are statistically significant differences between the means of multiple groups for a selected dependent variable. In this study, ANOVA is used to examine whether users' perceptions of ERP system security and reliability differ significantly across demographic groups such as gender, age, education, industry sector, economic activity, company size, user experience, and frequency of use with ERP systems.

By enabling the comparison of several groups, ANOVA provides an appropriate methodological framework for identifying demographic factors that may influence variations in perceived ERP system security and reliability, thereby directly supporting the study's objective.

## 5 RESULTS AND DISCUSSION

The sample of 206 ERP users from enterprises operating in Serbia has been gathered to conduct the analysis. Demographic characteristics of the research sample are described in Table 1.

This empirical research included more males (56.3%) than females (43.7%). Most ERP users were aged 30–39 (49.0%) and held either a BSc (43.2%) or MSc (42.2%) degree. In terms of industry sector, 65% of respondents were from manufacturing. The sample displayed industry heterogeneity regarding the distribution of enterprises' economic activity. Most ERP users work for large enterprises, defined as companies with more than 250 employees. Regarding user experience, most users have used ERP systems for 3 to 5 years (51.0%) and use them daily (83.5%).

This paper explores the impact of demographic variables of ERP users on perceived ERP system reliability and security. To achieve this, an ANOVA test was performed, and the results are presented in Table 2.

**Tab. 1** Demographic characteristics of the research sample (N = 206)

| Variables         | Category                    | Percentage % |
|-------------------|-----------------------------|--------------|
| Gender            | Male                        | 56.3         |
|                   | Female                      | 43.7         |
| Age               | 20-29                       | 20.4         |
|                   | 30-9                        | 49.0         |
|                   | 40-49                       | 25.2         |
|                   | 50-59                       | 5.3          |
| Education         | High school                 | 7.3          |
|                   | Higher education            | 5.8          |
|                   | BSc                         | 43.2         |
|                   | MSc                         | 42.2         |
|                   | PhD                         | 1.5          |
| Industry sector   | Manufacturing               | 65.0         |
|                   | Service                     | 35.0         |
| Economic activity | IT industry                 | 15.0         |
|                   | Automotive industry         | 17.5         |
|                   | Industrial selling          | 11.7         |
|                   | Banking                     | 2.4          |
|                   | Pharmaceutical industry     | 9.7          |
|                   | Production                  | 11.7         |
|                   | Aviation industry           | 1.9          |
|                   | Mining and metallurgy       | 13.1         |
|                   | Energy industry             | 2.4          |
|                   | Telecommunications industry | 3.9          |
|                   | Food and beverage industry  | 10.7         |
| Company size      | Less than 10 employees      | 1.9          |
|                   | 11-50 employees             | 5.3          |
|                   | 51-250 employees            | 18.9         |
|                   | Above 250 employees         | 73.8         |
| User experience   | Less than 1 year            | 5.8          |
|                   | 1-3 years                   | 26.7         |
|                   | 3-5 years                   | 51.0         |
|                   | More than 5 years           | 16.5         |
| Frequency of use  | Every day                   | 83.5         |
|                   | 1-2 times a week            | 4.9          |
|                   | Several times a week        | 7.8          |
|                   | 1-2 times a month           | 3.9          |

**Tab. 2** ANOVA test results

| Hypothesis | Demographic characteristic | Significance |                       | Hypothesis remark |
|------------|----------------------------|--------------|-----------------------|-------------------|
|            |                            | F            | p                     |                   |
| H1         | Gender                     | 1.472        | 0.226 <sup>n.s.</sup> | Rejected          |
| H2         | Age                        | 0.503        | 0.681 <sup>n.s.</sup> | Rejected          |
| H3         | Education                  | 3.284        | 0.012 <sup>**</sup>   | Accepted          |
| H4         | Industry sector            | 6.041        | 0.015 <sup>**</sup>   | Accepted          |
| H5         | Economic activity          | 2.440        | 0.007 <sup>**</sup>   | Accepted          |
| H6         | Company size               | 2.084        | 0.103 <sup>n.s.</sup> | Rejected          |
| H7         | User experience            | 3.791        | 0.005 <sup>*</sup>    | Accepted          |
| H8         | Frequency of use           | 2.734        | 0.030 <sup>*</sup>    | Accepted          |

Notes: \*statistically significant at 0.01 level; \*\*statistically significant at 0.05 level; n.s. Not significant.

Gender has not been found to have a statistically significant impact on the perceived security and reliability of ERP systems, leading to rejection of H1. Earlier studies (such as Broos, 2005) emphasised that, in the past, women were more anxious about using computers. Some recent studies (Mohamed & Ahmad, 2012; McGill & Thompson, 2021) have indicated differences in information security and privacy perceptions regarding gender. However, these studies explored privacy concerns and security perceptions in relation to social networks or internet technologies used for personal purposes. Moreover, users, regardless of gender, may perceive that ERP vendors have already implemented adequate security measures, diminishing the salience of security concerns in their perceptions. In the context of Serbia, the absence of statistically significant gender differences can be explained by the fact that the use of ERP systems in organisations is largely mandatory and directly related to daily work tasks.

The results also suggest that respondents' age does not have a statistically significant effect on the perceived security and reliability of ERP systems. Therefore, proposed hypothesis H2 is also rejected. ERP system security mechanisms, such as access control, encryption, and activity logging, are mostly invisible to users and are built in at the system level (Atakari, 2024). Therefore, users, regardless of age, do not have direct insight into the technical aspects of security, but form their perceptions based on general work experience and system stability. Furthermore, digital competencies are increasingly less dependent on age, as ERP systems have been present in business practice for many years. This may reduce differences between younger and older users in terms of understanding and trust in information systems. Similarly, the absence of differences between younger and older users can be attributed to the fact that ERP systems have been present in Serbia for some time, particularly in small and medium, and large enterprises, which constitute the dominant structure in this study sample.

Users' education has been found to have a statistically significant impact on the perceived security and reliability of ERP systems, leading to acceptance of H3. The literature suggests that perceptions of ERP system acceptance are often influenced by individual user characteristics, including education (Davis, 1989; Venkatesh & Bala, 2008). Specifically, a higher level of education can lead to a better understanding of how security measures support system stability, which positively

affects perceptions of reliability and safety. For example, Sternad Zabukovšek *et al.* (2019) report that more educated users demonstrate a higher degree of trust in ERP systems, as they are better able to recognise long-term benefits and understand system complexity. To gain deeper understanding, an ANOVA post hoc test was employed. The results indicate that the most pronounced difference is observed between ERP users with a high school degree and those with an MSc degree (mean difference = -0.531; standard error = 0.188;  $p = 0.042$ ). This finding supports existing literature in information security, which suggests that higher levels of education are associated with greater awareness of security risks and a more accurate understanding of protective mechanisms (Ifinedo, 2012). Furthermore, this difference may also be influenced by the increasing integration of ERP-related content and formal training in higher education curricula. However, this remark should be treated with caution, as the present study did not examine whether participants had undergone formal ERP, cybersecurity, or digital skills training, nor did it assess the quality or intensity of such training.

Industry sector has a statistically significant impact on the perceived security and reliability of ERP systems, resulting in acceptance of H4. The literature indicates that in manufacturing environments, ERP system outages are directly linked to financial losses and supply chain disruptions, reinforcing the importance of security and reliability in user perception (Wagner & Monk, 2008). In contrast, in the service sector, ERP systems often manage large volumes of customer data, financial transactions, and contractual relationships, where issues of confidentiality, privacy, and data protection are prioritised. Studies show that users in the service sector more frequently associate ERP system security with the protection of sensitive information and compliance with regulatory requirements, shaping a different perception of security compared to the manufacturing sector (Ifinedo, 2012).

Similarly, the economic activity of the enterprise has a statistically significant impact on perceived security. In industries such as finance, healthcare, or telecommunications, ERP systems process highly sensitive data such as financial transactions and personal and health information. Therefore, security requirements are stricter and user awareness of potential risks is greater (Trunina *et al.*, 2018). In contrast, in industries like mining and metallurgy, the focus is often on operational reliability and system availability, as even short-term ERP system outages can cause production downtime and supply chain disruptions (Ranitović *et al.*, 2013). Therefore, proposed hypothesis H5 is accepted.

The statistically significant impact of the industrial sector and economic activity is due to the structure of the Serbian economy, where manufacturing, metal processing, mining, and the energy sector continue to play a significant role, with ERP system interruptions directly causing operational and logistical problems. Conversely, the service sector, banking, telecommunications, and healthcare institutions are increasingly dependent on data protection and regulatory compliance, especially following the intensified digitalisation of financial and administrative processes.

Company size has not been found to have a statistically significant impact on perceived ERP system security and reliability, leading to rejection of H6. ERP users, whether they work in small, medium, or large companies, generally have a similar level of exposure to the system's security functionalities. Furthermore, company size is primarily relevant for managers' strategic and technical decisions regarding the selection and implementation of the ERP system (Lutfi *et al.*, 2024), while users form their perceptions of security and reliability based on their use of the system, its stability, and availability, rather than on wider organisational resources or structure.

User experience has a statistically significant impact on the perceived security of ERP systems, as supported by previous literature suggesting that, with longer use, users develop procedural

knowledge and routines, which reduce cognitive effort and increase the perception of system stability (Bhattacharjee, 2001). To gain deeper insights, post hoc analysis was performed, and results indicated that the most pronounced difference is between ERP users with 1–3 years of experience and those with more than five years of experience (mean difference = -0.436; standard error = 0.146;  $p = 0.027$ ). This supports the statement that experienced users are more likely to evaluate the security of ERP systems based on repeated positive experiences and have greater exposure to various situations when working with an ERP system, including system errors, security procedures, access controls, and the organisation's response to incidents. Therefore, proposed hypothesis H7 is accepted.

The frequency of using an ERP system has a statistically significant impact on perceptions of security and reliability (H8 is accepted), as it influences user familiarity with the system and the trust that develops through repeated interaction. Furthermore, research in information security shows that greater exposure to the system increases users' security awareness and understanding of their role in protecting the system (Workman *et al.*, 2009). This also confirms the results of post hoc analysis, showing the most pronounced difference is between ERP users who use ERP every day and those who use ERP 1–2 times per month (mean difference = 0.797; standard error = 0.261;  $p = 0.014$ ).

User experience and the frequency of ERP use are particularly relevant in Serbia, where the level of digital transformation among companies varies. The adoption of these systems has increased employees' exposure to digital business processes, which may lead to greater awareness of the importance of security, reliability and data protection in information systems. Furthermore, e-invoicing in Serbia should not necessarily be interpreted as directly improving users' digital competence. Rather, it has significantly increased employees' exposure to digital business processes and information systems, thereby making issues such as cybersecurity, data protection, and system reliability more visible in everyday work activities.

## 6 CONCLUSION

This study examined ERP system security from the users' perspective, focusing on how demographic characteristics influence perceptions of system reliability and security in Serbian enterprises. Using ANOVA on a sample of ERP users, the research provides empirical evidence of variations in perceived ERP security across different user groups, addressing an underexplored aspect of ERP security research.

The findings show that users' perceptions of ERP system security and reliability differ significantly according to education level, industry sector, economic activity, user experience, and frequency of system use. In contrast, no statistically significant differences were found for gender, age, or company size. These results suggest that perceptual differences are more strongly influenced by users' cognitive, experiential, and contextual characteristics than by basic demographic attributes. More educated and experienced users, as well as those who interact with ERP systems more frequently, tend to evaluate system security more positively, likely due to greater familiarity with system functionality and security mechanisms.

From a theoretical perspective, this study reinforces the view that ERP system security should be understood as a socio-technical construct rather than a purely technical attribute. From a practical standpoint, the results highlight the importance of tailoring security-related training, communication, and support mechanisms to different user groups. These implications are particularly relevant in the context of Serbia, where enterprises are undergoing digital transformation characterised by

heterogeneous levels of digital maturity, different level digital competencies, and varying levels of ERP adoption across industries. Therefore, improving continuous user support, and awareness-raising activities may be essential for strengthening confidence in ERP systems and reducing security-related uncertainty among employees.

Despite its contributions, this study has several limitations. The research is based on self-reported perceptions, which may not fully reflect actual system security or user behaviour. Future research could extend this work by incorporating longitudinal designs, comparative cross-country analyses, or additional behavioural variables such as security awareness, training intensity, or organisational security culture. Such approaches would provide a deeper understanding of how user perceptions of ERP security evolve over time and across different organisational and institutional contexts.

### Acknowledgements

The research presented in this paper was carried out with the financial support of the Ministry of Education, Science and Technological Development of the Republic of Serbia within the framework of financing scientific research work at the University of Belgrade, Technical Faculty in Bor, in accordance with the contract with registration number 451-03-34/2026-03/ 200131.

### REFERENCES

- ABU AFIFA, M. M., VO VAN, H., LE HOANG VAN, T. 2023. Blockchain adoption in accounting by an extended UTAUT model: empirical evidence from an emerging economy. *Journal of Financial Reporting and Accounting*. 21(1), 5-44.
- ALMAHAMID, S. 2019. The influence of ERP system usage on agile capabilities: examining the mediating role of users' psychological empowerment in Jordanian commercial banks. *Information Technology & People*. 32(6), 1633-1656.
- ANNAPAREDDY, V. N. 2025. The Intersection of Big Data, Cybersecurity, and ERP Systems: A Deep Learning Perspective. *Journal of Artificial Intelligence and Big Data Disciplines*. 2(1), 45-53.
- ATAKARI, C. 2024. A Deep Learning-Based Security Model for ERP-Integrated IoT in National Defense Manufacturing Environments. *International Journal of Emerging Trends in Computer Science and Information Technology*. 5(3), 90-98.
- BHATTACHERJEE, A. 2001. Understanding information systems continuance: An expectation-confirmation model. *MIS Quarterly*: 351-370.
- BOPPANA, S. B., MOORE, C. S., BODEPUDI, V., JHA, K. M., MAKHA, S. R., SADARAM, G. 2021. AI And ML Applications In Big Data Analytics: Transforming ERP Security Models For Modern Enterprises. *SSRN Electronic Journal*. 30(S2), 98-117.
- BROOS, A. 2005. Gender and information and communication technologies (ICT) anxiety: Male self-assurance and female hesitation. *CyberPsychology & Behavior*. 8(1), 21-31.
- DAVIS, F. D. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*: 319-340.
- EFE, A. 2024. Risk modelling of cyber threats against MIS and ERP applications. *Pamukkale Üniversitesi İşletme Araştırmaları Dergisi*. 11(2), 502-530.
- ELSAADANI, M. A. 2013. Exploring the relationship between teaching staff age and their attitude towards information and communications technologies (ICT). *International Journal of Instruction*. 6(1), 2015-226.
- GANGAPATNAM, K. 2025. Securing the Digital Core: Cybersecurity Challenges and Strategies in SAP ERP Systems. *Journal of Computer Science and Technology Studies*. 7(3), 270-276.

- HUSSAIN, M. K., SIDDIQUE, A., KAZMI, H., OBAIDULLAH, N. 2024. Factors Affecting User Acceptance of ERP Systems in SMEs. *Bulletin of Multidisciplinary Studies*. 1(1), 01–13.
- IFINEDO, P. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*. 31(1), 83–95.
- IVANOVIĆ, T., MARIĆ, M. 2021. Application of modern Enterprise Resource Planning (ERP) systems in the era of digital transformation. *Strategic Management – International Journal of Strategic Management and Decision Support Systems in Strategic Management*. 26(4), 28–36.
- JOHANSSON, B., ALAJBEGOVIC, A., ALEXOPOULOU, V., DESALERMOS, A. 2015,. Cloud ERP adoption opportunities and concerns: the role of organizational size. In: *2015 48<sup>th</sup> Hawaii international conference on system sciences*. pp. 4211–4219. IEEE.
- KUO, C. S., KANG, Y., YANG, H. L. 2023. Investigating the determinants of continuance intention on cloud ERP systems adoption. *Advances in Mechanical Engineering*. 15(4), 16878132231165973.
- KUSUMANINGTYAS, N., SUWARTO, D. H. 2015. ICT adoption, skill and use differences among small and medium enterprises managers based on demographic factors. *Procedia-Social and Behavioral Sciences*. 169, 296–302.
- LUTFI, A., ALQUDAH, H., AL-DAOUD, K. I., ZAQEEBA, N., ALRAWAD, M., ALMAIAH, M. A. 2024. Technology factors and ERP system efficiency in the Jordanian industrial firms: does company size matter? *Humanities and Social Sciences Communications*. 11(1), 1–13.
- MAY, R., BIERMANN, C., KENNER, A., KRÜGER, J., LEICH, T. 2024. A product-line-engineering framework for secure enterprise-resource-planning systems. *Procedia Computer Science*. 239, 1619–1626.
- MCGILL, T., THOMPSON, N. 2021. Exploring potential gender differences in information security and privacy. *Information & Computer Security*. 29(5), 850–865.
- MICHELBERGER, P., HORVÁTH, Z. 2017. Security aspects of process resource planning. *Polish Journal of Management Studies*. 16(1), 142–153.
- MISHRA, A. P., DUBLISH, M., KUMAR, D. 2022. Cyber security application in ERP implementation. *J. Pharm. Negat. Results*. 13, 2507–2522.
- MOHAMED, N., AHMAD, I. H. 2012. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*. 28(6), 2366–2375.
- MORRISSON, M. K. 2020. Best practice models for enterprise resource planning implementation and security challenges. *Journal of Business*. 8(2), 55–60.
- NITTALA, E. P. 2025. Zero Trust Security Models in AI-Integrated ERP Platforms for Defense-Grade Business Continuity. *International Journal of AI, BigData, Computational and Management Studies*. 6(2), 75–84.
- OLATOKUN, W. M. 2009. Analysing socio-demographic differences in access and use of ICTs in Nigeria using the capability approach. *Issues in Informing Science & Information Technology*. 6, 479–496.
- RANITTOVIĆ, P., TEPIĆ, G., MATIĆ, B., SREMAC, S., VUKADINOVIĆ, V. 2013. Functional dependency between the logistics security system and the MySAP ERP in metallurgy. *Metalurgija*. 52(4), 545–548.
- SALIH, S., HAMDAN, M., ABDELMABOUD, A., ABDELAZIZ, A., ABDELSALAM, S., ALTHOBAITI, M. M. *et al.* 2021. Prioritising organisational factors impacting cloud ERP adoption and the critical issues related to security, usability, and vendors: A systematic literature review. *Sensors*. 21(24), 8391.
- SAP. 2024. ERP security in a cybercrime world. SAP. [Accessed: 24 December 2025] <https://www.sap.com/resources/erp-security>
- SENEVIRATNE, S. C., COLOMBAGE, L. 2023. The impact of User-Characteristics and Organizational-Characteristics on End-user Satisfaction with Enterprise Resource Planning (ERP) systems. *International Journal of Financial, Accounting, and Management*. 5(1), 75–95.

- SHISH, Z. H. 2025. Securing ERP Systems: The Role Of Information Security Analysts In US Textile And Manufacturing Enterprises. *International Journal of Business and Economics Insights*. 5(3), 459–493.
- SIRAJ, T., HAQUE, R., CHOWDHURY, S., ISLAM, N., BISWAS, B., CHOWDHURY, K. H. 2024. Analyzing challenges in enterprise resource planning (ERP) implementation in a safety inspection company: An IVT2IF DEMATEL approach. *Optimality*. 1(2), 205–223.
- STERNAD ZABUKOVŠEK, S., KALINIC, Z., BOBEK, S., TOMINC, P. 2019. SEM-ANN based research of factors' impact on extended use of ERP systems. *Central European Journal of Operations Research*. 27(3), 703–735.
- TRIPLETT, W. J. 2022. Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*. 2(3), 573–586.
- TRUNINA, I., VARTANOVA, O., SUSHCHENKO, O. and ONYSHCHENKO, O. 2018. Introducing ERP System as a Condition of Information Security and Accounting System Transformation. *International Journal of Engineering & Technology*. 7(4.3), 530–536.
- VENKATESH, V., BALA, H. 2008. Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*. 39(2), 273–315.
- WAGNER, B., MONK, E. 2008. *Enterprise resource planning*. Course Technology Press.
- WORKMAN, M. 2009. How perceptions of justice affect security attitudes: Suggestions for practitioners and researchers. *Information Management & Computer Security*. 17(4), 341–353.

### Contact information

Sanela Arsić: e-mail: sarsic@tfbor.bg.ac.rs

Aleksandra Radić: e-mail: aradic@tfbor.bg.ac.rs

Đorđe Nikolić: e-mail: djnikolic@tfbor.bg.ac.rs