

Cybersecurity Threats and Mitigation Strategies in E-Procurement Systems: A Case Study of A Local Government (Public Sector)

Stephen Adeniyi Sobulo¹, Funminiyi Olajide²

^{1,2}Nottingham Trent University, Clifton, Nottingham NG11 8NS, United Kingdom

ABSTRACT: Technological advancement has undoubtedly impacted humanity in different ways influencing the way things are done. This has informed the transition of the traditional manual procurement processes to the internet-enabled e-procurement systems which is fast gaining popularity and acceptance across the globe because of the enormous benefits therein. However, cybercriminals, taking advantage of the technology, have become more sophisticated in their antics thereby necessitating the need for the study into the cybersecurity and mitigation methods to make e-procurement systems secured for safe use. This has become pertinent as there have been cyber incident(s) in the public sector service industry that had raised concerns regarding the continued use of e-procurement systems. Especially so because there is not much research in this subject area to give more practical insights in Nigeria and Sub-Saharan African countries.

The research was carried out using the questionnaire designed using the cloud-based JISC Online Surveys to elicit objective data from experienced professionals while two key and strategic professionals were interviewed to harvest accurate and adequate information regarding the implementation of e-procurement systems and the related data security issues. The combination of quantitative data from the questionnaires and the qualitative data from the interview made it possible to gather all relevant data that might be overlooked if only one method was used.

It has been confirmed through this study that pre-engagement security checks on personnel is imperative to reduce the possibility of insider attacks and that organizational policies are needed regarding incident response, the use of peripherals and personal devices within the organization, the regular backup policy and consistent update of Disaster Recovery Plans. Also important is regular personnel capacity building to keep them up to date, especially in security awareness to build a security culture across organizations. Furthermore, it has been confirmed that appropriately configured firewalls (hardware and / or software) would shield an application (website), organizational systems and networks from the DDoS attacks; the introduction of role-based access control in an application will prevent the possibility of unauthorized access to system resources through escalation of user privileges; finally when properly configured, an application can prevent SQLi attack through input validation which can be enhanced to prevent brute force attack; and when strong identification authentication is used, it would be difficult for cybercriminals to successfully use stolen login details to gain unauthorized access to systems or applications. All re-affirming that security must be built into every application (e-procurement) from the design phase to achieve the security goals of confidentiality, integrity, and availability.

KEYWORDS: Cybersecurity, E-Procurement, SQL Injection, DDoS, Public Sector, Risk Mitigation

1. INTRODUCTION:

E-procurement offers organizations worldwide increased efficiency and access to global markets through digitized procurement processes (bidding, evaluation, contracting, payments) (Girgvliani, 2023; Charnor & Quartey, 2024). Its rapid adoption is driven by cost savings and benefits like streamlined processes, efficiency and improved transparency (Abache, 2022). However, cybersecurity threats, particularly in developing economies, create scepticism (Droppe, 2023). Limited research in Nigeria and Sub-Saharan Africa into the implementation of E-procurement systems necessitated this research that is aimed at solving challenges faced by a local government (public sector) referred to as SakovicCorp (Mohungoo, Brown, & Kabanda, 2020), (Abdullahi, Oyewobi, Ganiyu, & Shittu, 2021), (Oseni, 2024).

This study used questionnaires and focus groups to explore cybersecurity issues in e-procurement, identify mitigation strategies, and determine critical success factors for secure system design. Specifically, it focuses on preventing SQL injection attacks (a top OWASP threat) (OWASP, 2025) within a Nigerian public sector's (SakovicCorp's) e-procurement database, addressing challenges that have stalled e-procurement adoption despite its potential. The study also examines DDoS attack mitigation and other success factors for e-procurement implementation.

Cybersecurity Threats and Mitigation Strategies in E-Procurement Systems: A Case Study of A Local Government (Public Sector)

The World Bank emphasizes public procurement's importance to national economies, highlighting the need to address challenges like data breaches, which have risen sharply with e-procurement adoption (Oshoma, Raji, & Yusuf, 2024), (WEF, 2025), (WorldBank, 2025). The fact that these systems handle sensitive data increases the risk of significant losses (UNDP, 2024). In addition, fraud is rampant in public procurement, particularly in developing economies (Iwerebor, et al., 2024; Charnor & Quartey, 2024) thereby fuelling resistance to the adoption of E-Procurement (Egwim, Dike, & Nmecha, 2024). Furthermore, cyberattacks, including DDoS attacks and website disruptions, further threaten e-procurement (Issabayeva, Yesseniyazova, & Grega, 2019), (PYMNTS, 2019), (Droppe, 2023). The Global Cybersecurity Outlook 2025 indicate a surge in attacks (WEF, 2025), necessitating proactive security measures and user training (Turyatamba & Turyasingura, 2024). Given that human error contributes to over 90% of breaches (Thakur, Barker, & Ali, 2024), (Tikanmäki & Ruoslahti, 2024) such trainings are crucial (Moh, 2025).

2. LITERATURE REVIEW

This literature review examines cybersecurity issues and mitigation strategies for e-procurement systems, aiming to inform the development of a secure system for a developing country's public sector, comparable to those in advanced nations. E-procurement, facilitated by growing global internet access of 67.9% in 2025 (Statista, 2025) and 115% increase in internet users in Sub-Saharan Africa from 2016 to 2021 (WorldBank, 2024) offers numerous benefits like expanded market access, efficiency, and transparency, contributing to economic growth (Stephens & Valverde, 2018), (Masudin, Aprilia, Nugraha, & Restuputri, 2021), (Sánchez-Rodríguez, Martínez-Lorente, & Hemsworth, 2020), (Kemp, 2021), (Abache, 2022; Egwim, Dike, & Nmecha, 2024). However, sophisticated cybercrime poses a significant threat, causing substantial financial losses (Hurst, 2021), (WEF, 2025).

E-procurement offers benefits like reduced overhead and wider product access (Sánchez-Rodríguez, Martínez-Lorente, & Hemsworth, 2020), (Gadour, 2024), (Egwim, Dike, & Nmecha, 2024), but cybersecurity concerns hinder adoption, especially in public sectors (Inusah, Kazaz, & Ulubeyli, 2025), (Droppe, 2023). Furthermore, as reported by Inusah et al. (2025), implementation challenges include low leadership commitment, poor funding, inadequate resources, data breaches, and outdated technology (Naeem, 2021), (Mohungoo, Brown, & Kabanda, 2020), (Naeem, Sulaimani, & Anwar, 2021), (WorldBank, 2024). Additionally, the increase in the frequency and sophistication of cyberattacks is also a factor (Rowell, 2021), (Inusah, Kazaz, & Ulubeyli, 2025), (WEF, 2025).

E-Procurement Systems and Cybersecurity: Cybersecurity protects digital assets from unauthorized access and corruption (Inusah, Kazaz, & Ulubeyli, 2025), (IBM, 2021), (Turyatamba & Turyasingura, 2024). Notwithstanding, cybersecurity concerns impede e-procurement adoption (Mohungoo, Brown, & Kabanda, 2020) due to the valuable data stored, making these systems attractive targets. Furthermore, the ever-increasing data breaches has continued to fuel these concerns (Alex, 2021), (Kerner, 2025), (WEF, 2025).

Therefore, there is a need to adopt appropriate mitigation strategies such as input validation, cryptography, authentication, access control, adoption of multi-factor authentication (MFA), biometrics, data masking, encryption, and tokenization (Kilincer, Ertam, & Sengur, 2021), (Looker, 2021), (Inusah, Kazaz, & Ulubeyli, 2025). These should be integrated from the design phase for effective and efficient security (Chapple, Stewart, & Gibson, 2021). Additionally, blockchain and AI offer further protection (Okon, et al., 2024), (Banafa, 2019), (Gunasekara, Sridarran, & Rajaratnam, 2021), (Girgvliani, 2023). It is noteworthy that training and capacity building are crucial (UNDP, 2024), (Moh, 2025), given that over 90% of cyberattacks are attributed to human errors (Thakur, Barker, & Ali, 2024), (Tikanmäki & Ruoslahti, 2024), (Omweri, 2024).

Approaches to Cybersecurity: Key cybersecurity approaches include: Access Control (RBAC, MAC, DAC) (Chapple, Stewart, & Gibson, 2021), (University of Hawai'i, 2021), (Martin, 2019), (Lashkov, 2018); Identity and Authentication, Cryptography, Firewalls and Data Masking (Islam, 2024), (Chapple, Stewart, & Gibson, 2021), (National Cyber Security Centre, 2018), (Weisman, 2021), (Qiu, Gui, & Zhao, 2020).

Regulations on Data Protection: Data protection regulations, like the UK's Data Protection Act 2018 (based on GDPR) and Nigeria's Data Protection Regulation (NDPR) (NITDA, 2019), mandate security measures to prevent unauthorized data access. Compliance requires integrating these measures into e-procurement systems from the design stage (GOV.UK, 2018).

E-Procurement Systems and Cyberattacks: E-procurement systems are attractive targets due to the valuable data they handle (bank details, IP, bid data). Common attacks include DDoS, SQL injection (SQLi), ransomware, man-in-the-middle, and supply chain attacks (PYMNTS, 2019), (Droppe, 2023).

Prevention of SQLi Attack: SQLi, a top OWASP threat, allows attackers to access sensitive data (OWASP, 2025), (Alenezi, Nadeem, & Asif, 2021). Protecting against SQLi requires robust security practices implemented from the design phase (Chapple, Stewart, & Gibson, 2021), (Kaur & Kaur, 2014). Mitigation strategies include input validation, Web Application Firewalls (WAFs),

Cybersecurity Threats and Mitigation Strategies in E-Procurement Systems: A Case Study of A Local Government (Public Sector)

regular software updates, principle of least privilege, prepared statements / stored procedures, and whitelisting / blacklisting (UC Berkeley, 2025), (Alenezi, Nadeem, & Asif, 2021), (Chapple, Stewart, & Gibson, 2021).

Countermeasures of DDoS Attacks: A Distributed Denial-of-Service (DDoS) attack prevents authorised users from accessing a system by flooding it with traffic from several compromised devices (bots) (Cloudflare, 2025), (Silva, 2021). When directed by the attacker, these bots, which are managed by a command-and-control server, produce enormous amounts of bandwidth. However, DDoS mitigation requires differentiating legitimate from malicious traffic, a complex task (Cloudflare, 2025). Therefore, a layered approach is recommended, including: blackhole routing; rate limiting; firewall/router configuration; Anycast network diffusion (often outsourced); ISP rerouting (Ferrillo, 2016), (Weisman, 2021A); network redundancy (Irwin, 2020), (Isberto, 2021) hybrid IDPS (Shah, Khan, & Ahmad, 2021), (Weisman, 2021); honeypots (Santhosh, 2024); and specialized hardware (Gartner, 2025).

E-Procurement Systems in the Public Sector: E-procurement offers significant benefits to the public sector (government and publicly funded services) (Ebong, 2020), (Egwim, Dike, & Nmecha, 2024), (Inusah, Kazaz, & Ulubeyli, 2025) particularly in developing economies, where it can combat corruption, increase transparency, and improve value for money (Gadour, 2024), (Fourie & Malan, 2021), (Turyatamba & Turyasingura, 2024). E-procurement training for public sector staff is essential due to the substantial procurement budgets (Turyatamba & Turyasingura, 2024), (Boafo, Ahudey, & Darteh, 2020), (Ebong, 2020). Although successful in developed nations, public sector e-procurement adoption lags in many developing economies, including Nigeria (Mohungoo, Brown, & Kabanda, 2020).

Critical Success Factors for the Implementation of E-Procurement: E-procurement adoption, like other E-governance strategies, hinges on technology (tools, funding, security, legal framework) (Moh, 2025), human behaviour (acceptance, skills) (Egwim, Dike, & Nmecha, 2024), and organizational factors (structure, size) (Gunasekaran, McGaughey, Ngai, & Rai, 2009). Larger, centralized organizations are more likely to implement e-procurement due to availability of the required resources (Issah, David, & Eric, 2024). However, human resistance, especially from management, and inadequate staff skills are major obstacles (Shakya, 2024), (MavenVista, 2024), (Lakhani, 2020), (Abache, 2022).

3. RESEARCH METHODOLOGY

This research investigates e-procurement data security, cyberattack dynamics, mitigation, and critical success factors to develop a secure system for a Nigerian public sector service industry. Data was collected via questionnaires from public sector professionals in Nigeria and the UK, and from professionals in financial institutions, private sector, and non-profit organizations. Analysis will inform security measures for an agile software development approach (Hoda, Salleh, & Grundy, 2018), (Chapple, Stewart, & Gibson, 2021). A systematic approach is essential for valid research (Saunders, Lewis, & Thornhill, 2012).

Research Philosophy: This research uses a mixed-methods approach, combining positivism (objective, empirical observation via questionnaires) and interpretivism (subjective interpretation via interviews) (Saunders M. , 2009), (Ryan, 2018), (Serva & Chapel, 2015), (BRM, 2021), (Žukauskas, Vveinhardt, & Andriukaitienė, 2018). This approach aims for accurate data on e-procurement security and answers the research questions while minimizing subjectivity.

Research Design: This mixed-methods research design used a literature review, expert interviews, and questionnaires to gather data on e-procurement data security in a public sector service industry. Data was analysed using JISC. This design captures both objective and subjective perspectives for a comprehensive understanding (Mitchell, 2018), (Maarouf, 2019), (Khatri, 2020).

Research Strategy: This research focuses on designing a secure e-procurement application for SAKOVIC Corporation, a public sector service industry, hardened against SQL injection (a top OWASP threat) (Alenezi, Nadeem, & Asif, 2021), (Tsing, 2019), (Chapple, Stewart, & Gibson, 2021). Data was gathered from procurement and IT professionals. The application was developed using ASP.NET Core in C# (Microsoft, 2021) with SSL/TLS, input validation (Roth, Anderson, & Luttin, 2020), (Microsoft, 2021), JavaScript (Toledo, 2018), (Achary, 2018), and Bootstrap (Berezhnoi, 2019), (Keller, 2019). Two-factor authentication and RBAC were implemented.

Data Collection and JISC Software: Data was collected via a JISC-based questionnaire, focusing on e-procurement systems, cybersecurity, and mitigation methods. Data handling complied with the Data Protection Act 2018/GDPR (Proton Technologies AG, 2021), (Hoofnagle, Sloot, & Borgesius, 2019), (GOV.UK, 2018). JISC facilitated quantitative data collection and analysis. Qualitative data was collected through focus group interviews. Respondents were primarily Nigerian (81.1%), with most having at least a bachelor's degree (94.6%), aged 31+, and male (70.3%). The majority worked in the public sector (67.1%).

4. FINDINGS AND DISCUSSION

This research revealed key e-procurement implementation challenges, particularly in cybersecurity. While 65.7% of respondents have adopted e-procurement, process-related constraints include inadequate IT infrastructure (42.6%), internet issues (17%), and

Cybersecurity Threats and Mitigation Strategies in E-Procurement Systems: A Case Study of A Local Government (Public Sector)

lack of qualified personnel (17.7%). Administrative constraints include lack of management support (24.1%), inadequate policies (27.7%), lack of policy implementation (14.6%), funding issues (10.2%), and security concerns (23.4%). Governments and top management's commitment is crucial for secure e-procurement implementation (Omweri, 2024), (Moh, 2025).

While 91.7% acknowledge e-procurement's potential to curb unethical behaviour, only 69% have experienced it, raising questions about ongoing practices and measurement challenges that might require further study (Schøll & Ubaydi, 2017). Furthermore, despite cybersecurity measures, human capacity building is essential, as human error contributes to over 90% of breaches (Thakur, Barker, & Ali, 2024), (Tikanmäki & Ruoslahti, 2024). Pre-employment security checks are important, but the 11% who don't conduct them pose a risk. While 76.8% have some form of disaster recovery plan (DRP) or backup, 23.2% lack a DRP, highlighting a vulnerability. Cyberattack prevention requires a comprehensive approach from management to all personnel. Strong policies and enforcement are essential.

In summary, the research identified SQLi attacks and DDoS as primary threats to e-procurement systems. Key mitigation strategies include:

- **Enforcing input validation and prepared statements:** Preventing SQLi attacks by sanitizing user inputs.
- **Deploying robust authentication mechanisms:** MFA and role-based access control minimize unauthorized access.
- **Implementing network security measures:** Firewalls, Intrusion Detection and Prevention Systems (IDPS), and load balancing reduce the risk of DDoS attacks.
- **Regular security training:** Increasing staff awareness to mitigate risks related to human error.

5. FUTURE WORK

This study has identified several areas for further research:

- a. A significant drop from 91.7% to 69% was observed when respondents compared the expected benefits of e-procurement in reducing fraud to their personal experiences. This raises questions about whether unethical practices persist, the effectiveness of e-procurement in curbing corruption, or the complexity of fraud measurement.
- b. E-procurement adoption appears higher in the public sector (67.3%) than in the private sector (53.9%). Further research is needed to verify this and explore possible reasons.
- c. Automating the verification of registration evidence through integration with registration authorities could improve efficiency. Investigating its feasibility and reliability is essential.

6. CONCLUSION AND RECOMMENDATIONS

The recommendations for secure e-procurement implementation, especially in developing nations, fall into three categories: human resources, technology, and workload influence.

Human Resources: Top management buy-in is crucial, requiring clear communication of e-procurement benefits. Thorough pre-engagement security checks are essential, especially for SoC personnel. Strict access control protocols, based on least privilege, must be enforced. Continuous personnel capacity building, including security awareness training, is vital.

Technology: Cybersecurity should be integrated into e-procurement systems from the design phase. Real-time incident response features, such as honeypots and automated alerts, are recommended. Comprehensive activity logging is needed for audit trails and accountability. Other crucial security measures include firewalls, input validation, role-based access control, data masking, encryption, tokenization and multi-factor authentication.

Workload Influence: Public sector e-procurement adoption offers numerous benefits: access to global markets, reduced turnaround time and paperwork, improved monitoring and evaluation, better inventory control, and fraud/corruption prevention. Centralized coordination of e-procurement deployment, including capacity building, ensures standardized service delivery.

In conclusion, the study reaffirms the importance of integrating security measures into e-procurement systems from the design phase. Public sector organizations must adopt a proactive approach by implementing multi-layered security controls, conducting regular vulnerability assessments, and enforcing compliance with data protection regulations. Future research should explore AI-driven security enhancements to strengthen e-procurement resilience against emerging threats.

REFERENCES

- 1) Abache, S. (2022, December 12). *Ancient kingdom, modern procurement: Edo State, Nigeria's lessons from going digital and open in public contracts*. Retrieved March 08, 2025 from Open Contracting Partnership: <https://www.open-contracting.org/2022/12/12/ancient-kingdom-modern-procurement-edo-state-nigerias-lessons-from-going-digital-and-open-in-public-contracts/>

Cybersecurity Threats and Mitigation Strategies in E-Procurement Systems: A Case Study of A Local Government (Public Sector)

- 2) Abdullahi, A., Oyewobi, L. O., Ganiyu, B. O., & Shittu, A. A. (2021, May 5). E-Procurement Implementation in the Public Construction Sector in Nigeria: A Review. *SETIC International Conference*. Retrieved June 24, 2021 from <http://repository.futminna.edu.ng:8080/jspui/handle/123456789/3517>
- 3) Achary, N. (2018, June 25). *Importance of JavaScript in Web Application Development*. Retrieved August 20, 2021 from LinkedIn: <https://www.linkedin.com/pulse/importance-javascript-web-application-development-achary>
- 4) Alenezi, M., Nadeem, M., & Asif, R. (2021, February). SQL injection attacks countermeasures assessments. *Indonesian Journal of Electrical Engineering and Computer Science*, 21(2), 1121-1131. doi:10.11591/ijeecs.v21.i2.pp1121-1131
- 5) Alex, S. (2021, May 26). *More data stolen in January 2021 than in all of 2017*. Retrieved May 28, 2021 from computerweekly: <https://www.computerweekly.com/news/252501400/More-data-stolen-in-January-2021-than-in-all-of-2017-says-report>
- 6) Banafa, A. (2019, May 6). *Blockchain and AI: A Perfect Match?* Retrieved June 7, 2021 from OpenMind BBVA: <https://www.bbvaopenmind.com/en/technology/artificial-intelligence/blockchain-and-ai-a-perfect-match/>
- 7) Berezhnoi, R. (2019, January 18). *What is Bootstrap?* Retrieved August 20, 2021 from F5 Studio: <https://f5-studio.com/articles/what-is-bootstrap-and-how-to-use-it-in-web-development/>
- 8) Bofo, N. D., Ahudey, E., & Darteh, A. O. (2020, May 25). Evaluating E-Procurement Impact In The Public Sector. *Archives of Business Review*, 8(5). doi:10.14738/abr.85.8268
- 9) BRM. (2021). *Positivism Research Philosophy*. Retrieved August 27, 2021 from Business Research Methodology (BRM): <https://research-methodology.net/research-philosophy/positivism/>
- 10) Chapple, M., Stewart, J. M., & Gibson, D. (2021). *(ISC)² CISSP certified information systems security professional official study guide* (Eighth edition ed.). John Wiley and Sons, Inc. : Sybex. Retrieved December 15, 2020 from <https://onlinelibrary-wiley-com.ntu.idm.oclc.org/doi/pdf/10.1002/9781119549567>
- 11) Charnor, I. T., & Quartey, E. K. (2024, October 29). Electronic procurement adoption and procurement performance: does institutional quality matter? *Business Process Management Journal*, 30(6). Retrieved March 8, 2025 from <https://www.emerald.com/insight/content/doi/10.1108/bpmj-02-2024-0106/full/html?skipTracking=true>
- 12) Cloudflare. (2025). *What is a DDoS attack*. Retrieved March 13, 2025 from Cloudflare: <https://www.cloudflare.com/en-gb/learning/ddos/how-to-prevent-ddos-attacks/>
- 13) Droppe. (2023, September 19). *Cyber Security In Procurement: How To Safeguard Your Supply Chain*. Retrieved March 08, 2025 from Droppe: <https://droppe.com/blog/article/cibersecurity-in-procurement/>
- 14) Ebong, K. U. (2020, July). E-Procurement Systems in Public Sector: Implications for Corruption and Development in Nigeria. *International Journal of Strategic Research in Public Administration and Organizational Process*, 2(1), 1-13. Retrieved June 27, 2021 from <http://internationalpolicybrief.org/images/2020/JULY/IJSRPAOP/ARTICLE1.pdf>
- 15) Egwim, P. U., Dike, B., & Nmecha, M. (2024, October 31). ADAPTING THE E-PROCUREMENT PROCESS FROM THE PRIVATE AND PUBLIC SECTOR: A COMPREHENSIVE OVERVIEW. *Alvan Journal of Social Sciences*, 1(2), 1 – 15. Retrieved March 08, 2025 from [https://www.researchgate.net/profile/Michael-Nmecha/publication/384909351_ADAPTING_THE_E-PROCUREMENT_PROCESS_FROM_THE_PRIVATE_AND_PUBLIC_SECTOR_A_COMPREHENSIVE_OVERVIEW/links/670e064723e2381cf6f1ff72/ADAPTING-THE-E-PROCUREMENT-PROCESS-FROM-THE-PRIVATE-AND-PUBLIC-SECTOR-A-COMPREHENSIVE-OVERVIEW/links/670e064723e2381cf6f1ff72/ADAPTING-THE-E-PROCUREMENT-PROCESS-FROM-THE-PRIVATE-AND-PUBLIC-SECTOR-A-COMPREHENSIVE-OVERVIEW.pdf](https://www.researchgate.net/profile/Michael-Nmecha/publication/384909351_ADAPTING_THE_E-PROCUREMENT_PROCESS_FROM_THE_PRIVATE_AND_PUBLIC_SECTOR_A_COMPREHENSIVE_OVERVIEW/links/670e064723e2381cf6f1ff72/ADAPTING-THE-E-PROCUREMENT-PROCESS-FROM-THE-PRIVATE-AND-PUBLIC-SECTOR-A-COMPREHENSIVE-OVERVIEW.pdf)
- 16) Ferrillo, P. (2016, February 23). *Defending Your Network Against DDoS Attacks*. Retrieved June 13, 2021 from Tripwire, Inc: <https://www.tripwire.com/state-of-security/security-awareness/defending-your-network-against-ddos-attacks/>
- 17) Fourie, D., & Malan, C. (2021, June 24). Technological Approach to Ensure Ethical Procurement Management. doi:10.5772/intechopen.98650
- 18) Gadour, M. M. (2024, April 07). Corruption in public procurement: Can e-procurement and artificial intelligence make a difference in Africa? <https://www.qscience.com/>. doi:https://doi.org/10.5339/connect.2024.spt.2
- 19) Gartner. (2025). *DDoS Mitigation Solutions Reviews and Ratings*. Retrieved March 13, 2025 from Gartner Peer Review: <https://www.gartner.com/reviews/market/ddos-mitigation-solutions>
- 20) Girgvliani, S. (2023, November 28). *Public Procurement Transparency and its Potential to Reduce Corruption in Low-Income Countries*. Retrieved March 8, 2025 from CSIS: <https://www.csis.org/blogs/development-dispatch/public-procurement-transparency-and-its-potential-reduce-corruption-low-income-countries>
- 21) GOV.UK. (2018). Data Protection Act 2018. Retrieved May 29, 2021 from https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf
- 22) Gunasekara, H. G., Sridarran, P., & Rajaratnam, D. (2021, February 1). Effective use of blockchain technology for facilities management procurement process. *Journal of Facilities Management*. Retrieved June 7, 2021 from <https://www.emerald.com/insight/content/doi/10.1108/JFM-10-2020-0077/full/html?skipTracking=true>

Cybersecurity Threats and Mitigation Strategies in E-Procurement Systems: A Case Study of A Local Government (Public Sector)

- 23) Gunasekaran, A., McGaughey, R. E., Ngai, E. W., & Rai, B. K. (2009, November). E-Procurement adoption in the Southcoast SMEs. *International Journal of Production Economics*, 122(1), 161-175. Retrieved May 3, 2021 from <https://www.sciencedirect.com/science/article/pii/S092552730900173X#!>
- 24) Hoda, R., Salleh, N., & Grundy, J. (2018, July 11). The Rise and Evolution of Agile Software Development. *IEEE Software*, 35(5), 58 - 63. doi:10.1109/MS.2018.29011318
- 25) Hoofnagle, C. J., Sloat, B. v., & Borgesius, F. Z. (2019 , February 10). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1), Pages 65-98. Retrieved August 16, 2021 from <https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501>
- 26) Hurst, A. (2021). *Cyber security spending heading for \$200 billion a year*. Retrieved April 16, 2021 from [information-age.com:https://www.information-age.com/cyber-security-spending-heading-for-200-billion-year-bloomberg-123494864/](https://www.information-age.com/https://www.information-age.com/cyber-security-spending-heading-for-200-billion-year-bloomberg-123494864/)
- 27) IBM. (2021). *What is data security?* Retrieved May 5, 2021 from <https://www.ibm.com/topics/data-security>
- 28) Inusah, Y., Kazaz, A., & Ulubeyli, S. (2025, February 27). Barriers to E-Tendering Implementation in the Construction Industry: A Comprehensive Review and Analysis of a Decade and Beyond. <https://www.mdpi.com/>, 17(5). doi:<https://doi.org/10.3390/su17052052>
- 29) Irwin, E. (2020, January 7). *Network Redundancy vs. Network Diversity: What's the Difference, and Do I Need Both?* Retrieved September 3, 2021 from INAP: <https://www.inap.com/blog/network-redundancy-vs-network-diversity/>
- 30) Isberto, M. (2021, January 19). *What Are the Benefits of Building Redundancy into a Network?* Retrieved September 3, 2021 from Colocation America: <https://www.colocationamerica.com/blog/benefits-of-a-redundant-network>
- 31) Islam, M. L. (2024). Impact of e-Procurement over Traditional Physical Procurement. *BRAC University*. Retrieved march 13, 2025 from https://dspace.bracu.ac.bd:8443/xmlui/bitstream/handle/10361/25628/22164070_BBS.pdf?sequence=1
- 32) Issabayeva, S., Yesseniyazova, B., & Grega, M. (2019). Electronic Public Procurement: Process and Cybersecurity Issues. *The NISPAcee Journal of Public Administration and Policy*, 7(2). Retrieved August 18, 2021 from https://www.researchgate.net/profile/Juraj-Nemec/publication/345356530_Welfare_Co-Production_Hungarian_and_Slovak_Reality/links/6035372fa6fdcc37a8495dba/Welfare-Co-Production-Hungarian-and-Slovak-Reality.pdf#page=63
- 33) Issah, O., David, A., & Eric, D. B. (2024, September 28). Analyzing the Influence of Organizational Culture and Top Management Orientation on the relationship between E-Procurement and Firms Performance: A Contingency Factors Perspective. *Project Management Scientific Journal*, 7(9), 93-116. doi:<https://dx.doi.org/10.4314/pmsj.v7i9.6>
- 34) Iwerebor, H. B., Nwaogwugwu, C. C., Amade, B., Anyanwu, C. I., Ubani, E. C., & Okorocho, K. A. (2024, November). Corruptible Tendencies and Public-Sector Construction Project Procurement. *PM World Journal*, XIII(X). Retrieved March 8, 2025 from <https://pmworldlibrary.net/wp-content/uploads/2024/11/pmwj146-OctNov2024-Iwerebor-et-al-Corruptible-Tendencies-Public-Sector-Construction.pdf>
- 35) Kaur, N., & Kaur, P. (2014, Decemeber 9). Mitigation of SQL Injection Attacks using Threat Modeling. *ACM SIGSOFT Software Engineering Notes*, 39(6). Retrieved August 24, 2021 from <https://dl.acm.org/doi/abs/10.1145/2674632.2674638>
- 36) Keller, S. D. (2019, September 2). *8 Reasons to Use Bootstrap for Web Development*. Retrieved August 20, 2021 from Creative Tim: <https://www.creative-tim.com/blog/web-design/8-reasons-to-use-bootstrap-for-web-development/>
- 37) Kemp, S. (2021, January 27). *DIGITAL 2021: GLOBAL OVERVIEW REPORT*. Retrieved September 3, 2021 from DataReportal: <https://datareportal.com/reports/digital-2021-global-overview-report>
- 38) Kerner, S. M. (2025, January 10). *35 cybersecurity statistics to lose sleep over in 2025*. Retrieved March 10, 2025 from TechTarget: https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020?_gl=1*9f36se*_ga*MTQ3MjY4MTM1OS4xNzQxNjJzODYx*_ga_TQKE4GS5P9*MTc0MTYyMzg2MC4xLjEuMTc0MTYyMzkyOC4wLjAuMA..
- 39) Khatri, S. (2020, July 3). *Positivism and Interpretivism in Social Research*. Retrieved July 12, 2021 from ReviseSociology: <https://revisesociology.com/2015/05/18/positivism-interpretivism-sociology/>
- 40) Kilincer, I. F., Ertam, F., & Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer networks (Amsterdam, Netherlands : 1999)*, 188. doi:10.1016/j.comnet.2021.107840
- 41) Lakhani, A. (2020). Building the Human Firewall. Retrieved May 31, 2021 from <https://www.darkreading.com/endpoint/building-the-human-firewall/a-d-id/1339045>
- 42) Lashkov, A. (2018, October 3). *Access Control Models: Review of Types and Use-Cases*. Retrieved July 9, 2021 from 1Ci Yellow Universe: <https://medium.com/yellow-universe/access-control-models-review-of-types-and-use-cases-1f4c427b0cc2#:~:text=%20Access%20Control%20Models%3A%20Review%20of%20Types%20and,but%20reads%20as%20rule-based%20access%20control.%20More%20>

Cybersecurity Threats and Mitigation Strategies in E-Procurement Systems: A Case Study of A Local Government (Public Sector)

- 43) Looker. (2021). *Data security*. Retrieved May 5, 2021 from <https://looker.com/>: <https://looker.com/definitions/data-security>
- 44) Maarouf, H. (2019, August 26). Pragmatism as a Supportive Paradigm for the Mixed Research Approach: Conceptualizing the Ontological, Epistemological, and Axiological Stances of Pragmatism. *International Business Research*, 12(9). doi:10.5539/ibr.v12n9p1
- 45) Martin, J. A. (2019, August 21). *What is access control? A key component of data security*. Retrieved July 9, 2021 from CSO UK: <https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html>
- 46) Masudin, I., Aprilia, G. D., Nugraha, A., & Restuputri, D. P. (2021). Impact of E-Procurement Adoption on Company Performance: Evidence from Indonesian Manufacturing Industry. *Logistics*, 5(16). Retrieved May 3, 2021 from https://www.researchgate.net/profile/Ilyas_Masudin/publication/350176451_Impact_of_E-Procurement_Adoption_on_Company_Performance_Evidence_from_Indonesian_Manufacturing_Industry/links/605483c5458515e834562354/Impact-of-E-Procurement-Adoption-on-Company-Per
- 47) MavenVista. (2024, December 25). *Why e-Procurement Implementations Fail? Key Reasons Behind It*. Retrieved March 13, 2025 from <https://mavenvista.com/>: <https://mavenvista.com/why-e-procurement-implementations-fail/>
- 48) Microsoft. (2021). *ASP.NET documentation*. Retrieved August 16, 2021 from [docs.microsoft.com](https://docs.microsoft.com/en-us/aspnet/core/?view=aspnetcore-5.0): <https://docs.microsoft.com/en-us/aspnet/core/?view=aspnetcore-5.0>
- 49) Mitchell, A. (2018, October 1). A Review of Mixed Methods, Pragmatism and Abduction Techniques. *The Electronic Journal of Business Research Methods*, 16(3), 103-116. Retrieved July 12, 2021 from <https://academic-publishing.org/index.php/ejbrm/article/view/1378>
- 50) Moh, E. K. (2025). *E-Governance as a Panacea to Advance Local Development in Cameroon Post-COVID 19*. doi:10.5772/intechopen.114341
- 51) Mohungoo, I., Brown, I., & Kabanda, S. (2020, April 1). A Systematic Review of Implementation Challenges in Public E-Procurement. *Conference on e-Business, e-Services and e-Society*, 12067. Retrieved April 26, 2021 from https://link.springer.com/chapter/10.1007/978-3-030-45002-1_5
- 52) Mohungoo, I., Brown, I., & Kabanda, S. (2020, April 1). A Systematic Review of Implementation Challenges in Public E-Procurement. *Conference on e-Business, e-Services and e-Society*, 12067. Retrieved April 26, 2021 from https://link.springer.com/chapter/10.1007/978-3-030-45002-1_5
- 53) Naeem, M. (2021). *Uncovering and Addressing the Challenges in the Adoption of E-Procurement System: Adoption Process Stages in SMEs*. Retrieved May 5, 2021 from www.igi-global.com: <https://www.igi-global.com/article/uncovering-and-addressing-the-challenges-in-the-adoption-of-e-procurement-system/267735>
- 54) Naeem, M., Sulaimani, A., & Anwar, S. (2021). *A Resource-Based Technological View in the Adoption of an E-Procurement System: Evidence from Textile Sector SMEs*. Retrieved April 26, 2021 from <https://www.igi-global.com/article/a-resource-based-technological-view-in-the-adoption-of-an-e-procurement-system/273198>
- 55) National Cyber Security Centre. (2018, November 17). *Cloud security guidance*. Retrieved July 9, 2021 from National Cyber Security Centre: <https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles/identity-and-authentication>
- 56) NITDA. (2019). *Nigeria Data Protection Regulation 2019*. Retrieved May 29, 2021 from <https://ndpr.nitda.gov.ng/Content/Doc/NigeriaDataProtectionRegulation.pdf>
- 57) Okon, S. U., Olateju, O., Ogungbemi, O. S., Joseph, S., Olisa, A. O., & Olaniyi, O. O. (2024, October 7). Incorporating Privacy by Design Principles in the Modification of AI Systems in Preventing Breaches across Multiple Environments, Including Public Cloud, Private Cloud, and On-prem. *SSRN*. doi:<https://dx.doi.org/10.2139/ssrn.4945564>
- 58) Omweri, F. S. (2024, August). A Systematic Literature Review of E-Government Implementation in Developing Countries: Examining Urban-Rural Disparities, Institutional Capacity, and Socio-Cultural Factors in the Context of Local Governance and Progress towards SDG 16.6. *International Journal of Research and Innovation in Social Science (IJRISS)*, VIII(VIII). doi:<https://dx.doi.org/10.47772/IJRISS.2024.808088>
- 59) Oseni, K. O. (2024, April 16). Barriers facing e-service adopting and implementation at local environment level in Nigeria. *Cornell University*. doi:<https://doi.org/10.48550/arXiv.2406.15375>
- 60) Oshoma, A. O., Raji, I. O., & Yusuf, A. (2024, November 22). Impact of e-procurement adoption on the performance of SMEs in emerging economy. *inderscienceonline*, 21(4), 440-466. doi:<https://doi.org/10.1504/IJPM.2024.142788>
- 61) OWASP. (2025). *OWASP Top Ten*. Retrieved March 08, 2025 from OWASP: <https://owasp.org/www-project-top-ten/>
- 62) Proton Technologies AG. (2021). *General Data Protection Regulation (GDPR)*. Retrieved August 16, 2021 from [GDPR.EU: https://gdpr.eu/tag/gdpr/](https://gdpr.eu/tag/gdpr/)
- 63) PYMNTS. (2019). *Cyberattack Paralyzes India eProcurement Portal*. Retrieved May 5, 2021 from www.pymnts.com: <https://www.pymnts.com/news/b2b-payments/2019/cyberattack-paralyzes-india-eprocurement-portal/>

Cybersecurity Threats and Mitigation Strategies in E-Procurement Systems: A Case Study of A Local Government (Public Sector)

- 64) Qiu, G., Gui, X., & Zhao, Y. (2020, June 8). Privacy-Preserving Linear Regression on Distributed Data by Homomorphic Encryption and Data Masking. *IEEE Access*, 8, 107601-107613. doi:10.1109/ACCESS.2020.3000764
- 65) Roth, D., Anderson, R., & Luttin, S. (2020, 4 17). *Introduction to ASP.NET Core*. Retrieved June 25, 2021 from Microsoft: <https://docs.microsoft.com/en-us/aspnet/core/introduction-to-aspnet-core?view=aspnetcore-5.0>
- 66) Rowsell, J. (2021, August 3). *Supply chain cyber attacks to 'quadruple'*. Retrieved September 2, 2021 from SUPPLY MANAGEMENT: <https://www.cips.org/supply-management/news/2021/august/supply-chain-cyber-attacks-to-quadruple/>
- 67) Ryan, G. (2018). Introduction to positivism, interpretivism and critical theory. *Nurse Researcher*, 25(4), 41–49. doi:<http://dx.doi.org/doi:10.7748/nr.2018.e1466>
- 68) Sánchez-Rodríguez, C., Martínez-Lorente, A. R., & Hemsworth, D. (2020, March 21). E-procurement in small and medium sized enterprises; facilitators, obstacles and effect on performance. *Benchmarking: An International Journal*, 27(2), 839-866. Retrieved May 5, 2021 from <https://www.emerald.com/insight/content/doi/10.1108/BIJ-12-2018-0413/full/html>
- 69) Santhosh, A. U. (2024, April 14). *Strengthening Web Security: Unveiling the Power of Honeypots Against DDoS Attacks*. Retrieved March 13, 2025 from Medium: <https://santhosh-adiga-u.medium.com/strengthening-web-security-unveiling-the-power-of-honeypots-against-ddos-attacks-1aac2338d344#:~:text=What%20is%20a%20Honey%20pot%2C%20including:>
- 70) Saunders, M. (2009). *Understanding research philosophies and approaches*. Retrieved August 7, 2021 from https://www.researchgate.net/publication/309102603_Understanding_research_philosophies_and_approaches
- 71) Saunders, M. N., Lewis, P., & Thornhill, A. (2012). *Saunders: Research Methods for Bu_p6*. Financial Times Press. Retrieved August 19, 2021 from <https://www.pearson.com/uk/educators/higher-education-educators/product/Saunders-Saunders-Research-Methods-for-Bu-p-6-6th-Edition/9780273750758.html>
- 72) Schøll, A., & Ubaydi, D. (2017). *Impact of Technology on Corruption*. Norwegian School of Economics. Retrieved July 31, 2021 from <https://openaccess.nhh.no/nhh-xmlui/bitstream/handle/11250/2487632/masterthesis.PDF?sequence=1>
- 73) Serva, C., & Chapel, L. (2015, September 1). *Positivism in Sociology: Definition, Theory & Examples*, 30 July 2020. Retrieved July 12, 2021 from Study.com: <https://study.com/academy/lesson/positivism-in-sociology-definition-theory-examples.html>
- 74) Shah, S. Q., Khan, F. Z., & Ahmad, M. (2021, March 14). The impact and mitigation of ICMP based economic denial of sustainability attack in cloud computing environment using software defined network. *Computer networks (Amsterdam, Netherlands : 1999)*, 187, 1-12. doi:10.1016/j.comnet.2021.107825
- 75) Shakya, R. K. (2024, June 27). *10 success factors for implementing e-procurement system*. Retrieved March 13, 2025 from <https://blogs.worldbank.org/>: <https://blogs.worldbank.org/en/governance/10-success-factors-for-implementing-e-procurement-system>
- 76) Silva, A. (2021, January 26). Distributed denial-of-service attacks. *e-prints in library and information science*, 1-14. Retrieved June 13, 2021 from <http://eprints.rclis.org/40936/>
- 77) Statista. (2025, February 13). *Number of internet and social media users worldwide as of February 2025*. Retrieved March 08, 2025 from statista: <https://www.statista.com/statistics/617136/digital-population-worldwide/>
- 78) Stephens, J., & Valverde, R. (2018, October 8). Security of E-Procurement Transactions in Supply Chain Reengineering. *Computer and Information Science*. doi:10.5539/cis.v6n3p1
- 79) Thakur, K., Barker, H., & Ali, M. L. (2024, October 24). Human Error in Cybersecurity Management. *IEEE Xplore*. doi:<https://doi.org/10.1109/TEMSCONLATAM61834.2024.10717786>
- 80) Tikanmäki, I., & Ruoslahti, H. (2024, November 04). Human Factors Make or Break Cybersecurity! *Information & Security*, 55(3). doi:<https://doi.org/10.11610/isij.5522>
- 81) Toledo, J. (2018, June 7). *Why Millions of Developers use JavaScript for Web Application Development*. Retrieved August 20, 2021 from TORQUE: <https://torquemag.io/2018/06/why-millions-of-developers-use-javascript-for-web-application-development/>
- 82) Tsing, W. (2019, October 3). *OWASP top ten – Boring security that pays off*. Retrieved July 22, 2021 from Malwarebytes: <https://blog.malwarebytes.com/security-world/2017/05/owasp-top-ten-boring-security-that-pays-off/>
- 83) Turyatamba, C., & Turyasingura, B. (2024, April). Adoption of Digital Revolution in Government Ministries, Departments, and Agencies (MDAs) In Uganda; Reflection on Uganda Revenue Authority Digital Strategy Integration Approach towards Enhanced Tax Revenue in Post Covid-19 Pandemic. *International Journal of Academic Multidisciplinary Research (IJAMR)*, 8(4), 235-247. doi:<https://orcid.org/0000-0003-1325-4483>
- 84) UC Berkeley. (2025). *How to Protect Against SQL Injection Attacks*. Retrieved March 13, 2025 from <https://security.berkeley.edu/>: <https://security.berkeley.edu/education-awareness/how-protect-against-sql-injection-attacks>
- 85) UNDP. (2024). *BUILDING CYBERSECURITY IN WEST AND CENTRAL AFRICA*. UNDP. Retrieved March 08, 2025 from <https://www.undp.org/sites/g/files/zskgke326/files/2024-10/give-1-project-undp-en.pdf>

Cybersecurity Threats and Mitigation Strategies in E-Procurement Systems: A Case Study of A Local Government (Public Sector)

- 86) University of Hawai'i. (2021). *Access Control Models*. Retrieved June 28, 2021 from Cyber Security: <https://westoahu.hawaii.edu/cyber/best-practices/best-practices-weekly-summaries/access-control/>
- 87) WEF. (2025, January). Global Cybersecurity Outlook 2025. *World Economic Forum (WEF)*. Retrieved March 08, 2025 from https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
- 88) Weisman, S. (2021). *What is a distributed denial of service attack (DDoS) and what can you do about them?* . Retrieved June 13, 2021 from Emerging Threats: <https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html#:~:text=A%20distributed%20denial-of-service%20attack%20is%20one%20of%20the,or%20network%20that%20floods%20it%20with%20Internet%20traffic>
- 89) Weisman, S. (2021A). *What are Denial of Service (DoS) attacks? DoS attacks explained*. Retrieved June 13, 2021 from Emerging Threats: <https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html>
- 90) WorldBank. (2024, January 18). *Digital Transformation Drives Development in Africa* . Retrieved March 8, 2025 from World Bank Group: <https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-africa>
- 91) WorldBank. (2025, January 29). *Enhancing Cyber Resilience in Developing Countries*. Retrieved March 08, 2025 from World Bank Group: <https://www.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries>
- 92) Žukauskas, P., Vveinhardt, J., & Andriukaitienė, R. (2018, April 18). Philosophy and Paradigm of Scientific Research. *IntechOpen*. doi:10.5772/intechopen.70628