Global Multidisciplinary Journal
eISSN: 2791-173X pISSN: 2791-2760

VOLUME 05 ISSUE 4
Published 16-04-2026 *Page No. 21-32*

Secure Software Delivery Governance for Enterprise Resource Planning Deployment Workflows

Dr. Budi Santoso

School of Electrical Engineering and Informatics, Bandung Institute of Technology, Indonesia

ABSTRACT

Enterprise Resource Planning (ERP) systems represent mission-critical infrastructures that integrate organizational processes across finance, supply chain, human resources, and governance domains. With the increasing adoption of digital transformation initiatives, ERP deployment workflows have become highly dynamic, distributed, and automated. However, these advancements introduce complex security challenges, particularly in ensuring governance across software delivery pipelines. This study investigates secure software delivery governance mechanisms tailored for ERP deployment workflows, emphasizing the integration of security controls, authentication models, and governance frameworks within modern DevSecOps environments.

The research identifies critical vulnerabilities in ERP deployment pipelines, including credential mismanagement, inconsistent authentication enforcement, and insufficient monitoring of deployment anomalies. Drawing upon established e-governance security frameworks, cryptographic authentication models, and digital transformation strategies, this paper proposes a governance-centric model that integrates secure delivery pipelines with policy-driven controls. The study leverages theoretical foundations from secure authentication systems, data modeling techniques, and enterprise digitalization initiatives to construct a comprehensive framework that ensures integrity, confidentiality, and availability across ERP deployments.

A key contribution of this research is the development of a multi-layered governance architecture that incorporates secure credential lifecycle management, automated compliance validation, and anomaly-aware deployment mechanisms. Additionally, the study highlights the role of DevSecOps-driven security controls in minimizing deviations in deployment workflows, supported by insights from recent research on ERP pipeline security (Gangaiah et al., 2026). The framework is evaluated through hypothetical enterprise scenarios aligned with large-scale digital transformation initiatives, demonstrating improved resilience against security breaches and operational inconsistencies.

The findings indicate that embedding governance mechanisms within software delivery pipelines significantly enhances ERP system security while maintaining deployment agility. Furthermore, the study emphasizes the importance of aligning enterprise governance policies with automated security enforcement to mitigate emerging cyber threats. The proposed framework contributes to both academic research and industry practices by providing a structured approach to secure ERP deployment governance in the era of digital transformation.

KEYWORDS

ERP Security, DevSecOps Governance, Software Delivery Pipelines, Authentication Systems, Digital

Global Multidisciplinary Journal
eISSN: 2791-173X pISSN: 2791-2760

VOLUME 05 ISSUE 4
Published 16-04-2026 *Page No. 21-32*

Transformation, Secure Deployment, Credential Management, E-Governance Security, Enterprise Systems

INTRODUCTION

Enterprise Resource Planning (ERP) systems have evolved into foundational components of modern organizations, enabling integrated management of business processes and facilitating data-driven decision-making. The transition from traditional on-premise ERP deployments to cloud-enabled and hybrid architectures has significantly transformed the software delivery lifecycle. This transformation, driven by digitalization strategies and global connectivity, has introduced both opportunities and challenges in ensuring secure deployment governance.

The growing reliance on automated deployment pipelines, continuous integration, and continuous delivery mechanisms has amplified the complexity of ERP environments. These pipelines, while enhancing operational efficiency, often lack robust governance structures, leading to vulnerabilities in authentication mechanisms, access control, and data integrity. In particular, the absence of centralized governance in software delivery workflows can result in inconsistent application of security policies, thereby increasing the risk of unauthorized access and system compromise.

Digital transformation initiatives, such as those outlined in national strategies and enterprise modernization frameworks, emphasize the need for secure and scalable IT infrastructures. For instance, large-scale transformation programs highlight the integration of digital services, smart governance, and secure information systems as key drivers of economic growth and organizational resilience (Oman Vision 2040). These initiatives underscore the importance of aligning ERP deployment workflows with secure governance practices to ensure the reliability and trustworthiness of enterprise systems.

A critical challenge in ERP deployment governance is the management of authentication and authorization mechanisms. Traditional approaches, including static credential systems and centralized authentication servers, are increasingly inadequate in dynamic deployment environments. Research on e-governance security frameworks demonstrates the effectiveness of cryptographic authentication models and digital certificate-based systems in enhancing security (Roy & Karforma, 2014). However, the integration of these models into automated software delivery pipelines remains a complex task, requiring careful consideration of system architecture and operational constraints.

Furthermore, the increasing sophistication of cyber threats necessitates proactive security measures within deployment workflows. Recent studies have highlighted the role of DevSecOps practices in embedding security controls throughout the software development lifecycle. By integrating security testing, vulnerability assessment, and compliance validation into continuous delivery pipelines, organizations can significantly reduce the risk of security breaches (Gangaiah et al., 2026). Despite these advancements, there remains a gap in the application of DevSecOps principles specifically to ERP deployment governance.

This research addresses the need for a comprehensive framework that integrates secure software delivery governance into ERP deployment workflows. The study aims to bridge the gap between theoretical security models and practical deployment mechanisms by proposing a governance-centric approach that incorporates

authentication, authorization, and monitoring controls within automated pipelines. The objectives of this research are threefold: first, to analyze the existing challenges in ERP deployment security; second, to evaluate the effectiveness of current governance frameworks; and third, to propose a novel model that enhances security while maintaining deployment efficiency.

The scope of this study encompasses both theoretical and practical aspects of secure ERP deployment. The research draws upon established literature in e-governance security, digital transformation strategies, and software engineering practices to construct a comprehensive analytical framework. Additionally, the study incorporates insights from real-world digital transformation initiatives, highlighting the importance of aligning enterprise IT strategies with secure deployment practices.

The significance of this research lies in its contribution to the development of secure and resilient ERP systems. By addressing the challenges associated with deployment governance, the study provides valuable insights for organizations seeking to enhance their security posture in an increasingly complex digital landscape. Moreover, the proposed framework offers practical guidance for implementing secure software delivery pipelines, thereby supporting the broader objectives of digital transformation and enterprise modernization.

LITERATURE REVIEW

The domain of secure software delivery governance for ERP systems intersects multiple research areas, including e-governance security, digital transformation, authentication mechanisms, and DevSecOps practices. The existing literature provides a foundational understanding of these domains, yet reveals significant gaps in their integration within ERP deployment workflows.

E-governance security frameworks have extensively explored the role of authentication and data protection in digital systems. Studies on smart card-based e-voting systems emphasize the importance of secure data modeling and cryptographic techniques in ensuring system integrity (Khatun et al., 2017). Similarly, research on digital certificate-based authentication highlights the effectiveness of cryptographic methods in preventing unauthorized access and ensuring secure transactions (Roy & Karforma, 2014). These studies provide valuable insights into the design of secure authentication mechanisms, which are critical for ERP deployment governance.

Further research in e-governance has examined the implementation of secure information systems using unified modeling language (UML) approaches. These studies demonstrate the importance of structured system design in achieving secure and scalable architectures (Roy et al., 2013). Additionally, analyses of information security in e-governance contexts underscore the need for comprehensive security strategies that address both technical and organizational aspects (Roy, 2015). These findings are particularly relevant to ERP systems, which operate at the intersection of multiple organizational processes.

Digital transformation initiatives have also contributed to the understanding of secure system deployment. Reports on digital transformation strategies highlight the integration of advanced technologies, such as cloud computing and data analytics, in enhancing service delivery and operational efficiency. These initiatives emphasize the need for robust security frameworks to support the adoption of digital technologies (IMF eLibrary, 2025). Moreover, case studies on municipal service management demonstrate the role of digital transformation in improving governance and service delivery, while also identifying challenges related to security and data management.

In the context of ERP systems, the integration of digital transformation strategies introduces new security challenges. The adoption of cloud-based ERP solutions necessitates the implementation of secure deployment pipelines that can handle dynamic and distributed environments. Research on ERP deployment workflows indicates that traditional security measures are often insufficient in addressing the complexities of modern systems. This highlights the need for innovative approaches that integrate security controls into the software delivery lifecycle.

DevSecOps practices have emerged as a key approach to addressing these challenges. By embedding security controls within continuous integration and continuous delivery pipelines, organizations can ensure that security is an integral part of the software development process. Studies on DevSecOps-driven security controls demonstrate the effectiveness of this approach in reducing vulnerabilities and improving system resilience (Gangaiah et al., 2026). These findings underscore the potential of DevSecOps in enhancing ERP deployment governance.

However, the application of DevSecOps principles to ERP systems remains limited. While existing studies provide valuable insights into secure software development practices, they often focus on general-purpose applications rather than enterprise-specific systems. This creates a gap in the literature, as ERP systems have unique requirements related to data integration, process management, and regulatory compliance.

Another important area of research is the role of governance frameworks in ensuring system security. Governance frameworks provide a structured approach to managing security policies, compliance requirements, and risk management strategies. Studies on digital governance highlight the importance of aligning IT strategies with organizational objectives to achieve effective system management. These frameworks are particularly relevant to ERP systems, which require coordinated management across multiple organizational units.

Despite the advancements in these research areas, there remains a lack of comprehensive frameworks that integrate secure software delivery governance into ERP deployment workflows. Existing studies often address individual aspects of security, such as authentication or data protection, without considering their integration within the broader deployment lifecycle. This fragmentation limits the effectiveness of security measures and highlights the need for a holistic approach.

This research seeks to address these gaps by developing a comprehensive framework that integrates secure software delivery governance into ERP deployment workflows. By combining insights from e-governance security, digital transformation, and DevSecOps practices, the study aims to provide a unified approach to enhancing ERP system security.

METHODOLOGY

5.1 Conceptual Foundations of Secure ERP Delivery Governance

Secure software delivery governance for ERP systems is grounded in the convergence of three critical domains: enterprise governance, secure software engineering, and digital transformation ecosystems. ERP systems are inherently complex due to their cross-functional integration, and therefore require governance frameworks that extend beyond conventional application security models.

At a conceptual level, governance in ERP deployment workflows involves the establishment of policies, controls, and accountability mechanisms that regulate software delivery processes. These mechanisms ensure that every stage of the deployment pipeline—from code integration to production release—adheres to predefined security and compliance standards. Unlike traditional governance models that operate at the organizational level, software delivery governance must be embedded directly within the pipeline architecture to enable real-time enforcement.

Theoretical foundations from e-governance research highlight the importance of structured data modeling and authentication frameworks in maintaining system integrity (Roy & Karforma, 2014). These principles can be extended to ERP systems by integrating identity management and cryptographic validation within deployment workflows. Furthermore, digital transformation frameworks emphasize the role of secure infrastructure in enabling scalable and resilient enterprise systems, reinforcing the need for governance-driven deployment models.

A critical insight from recent DevSecOps research is the necessity of integrating security controls as code, enabling automated enforcement of governance policies (Gangaiah et al., 2026). This paradigm shift transforms governance from a reactive process into a proactive and continuous mechanism embedded within software delivery pipelines.

5.2 Architecture of Secure ERP Deployment Pipelines

The architecture of a secure ERP deployment pipeline is composed of multiple interconnected layers, each responsible for enforcing specific governance and security functions. These layers include:

1. Source Control and Code Integrity Layer

This layer ensures that all code entering the pipeline is authenticated, version-controlled, and verified for integrity. Secure coding practices and cryptographic hashing mechanisms are implemented to prevent unauthorized modifications.

2. Continuous Integration Layer

During integration, automated security testing tools are employed to identify vulnerabilities in code. Static and dynamic analysis techniques are used to detect potential threats before deployment. Governance policies enforce mandatory security checks, ensuring that no code progresses without compliance validation.

3. Credential Management Layer

Credential mismanagement is a major source of security vulnerabilities in ERP systems. This layer implements secure storage, rotation, and access control mechanisms for credentials. Digital certificate-based authentication models, as discussed in e-governance research, are particularly effective in this context (Roy & Karforma, 2014).

4. Deployment Orchestration Layer

This layer manages the deployment of ERP components across different environments. Governance controls

ensure that deployments are authorized, monitored, and logged. Automated approval mechanisms based on policy compliance reduce the risk of unauthorized changes.

5. Monitoring and Feedback Layer

Continuous monitoring of deployment activities enables real-time detection of anomalies. Feedback loops allow the system to adapt and improve governance policies based on observed behavior. This aligns with incident-aware pipeline strategies that leverage operational insights to enhance security (Gangaiah et al., 2026).

The integration of these layers creates a robust architecture that ensures secure and governed ERP deployment workflows.

5.3 Authentication and Authorization Mechanisms in ERP Workflows

Authentication and authorization are central to secure ERP deployment governance. Traditional authentication systems, such as username-password combinations, are insufficient in modern deployment environments. Instead, advanced mechanisms based on cryptographic techniques and digital certificates are required.

Research in e-governance systems demonstrates the effectiveness of digital certificate-based authentication in ensuring secure user access (Roy et al., 2014). These systems utilize public key infrastructure (PKI) to validate user identities, providing a high level of security. In ERP deployment workflows, similar mechanisms can be implemented to authenticate deployment agents and pipeline components.

Authorization mechanisms must also be dynamically managed to accommodate the changing roles and responsibilities within an organization. Role-based access control (RBAC) and attribute-based access control (ABAC) models provide flexible and scalable solutions for managing access permissions. These models ensure that only authorized entities can perform specific actions within the deployment pipeline.

Furthermore, the integration of authentication and authorization mechanisms with governance frameworks enables centralized control over access policies. This ensures consistency in security enforcement across all stages of the deployment lifecycle.

5.4 DevSecOps Integration for Governance Enforcement

DevSecOps represents a paradigm shift in software development, emphasizing the integration of security within the development and deployment lifecycle. For ERP systems, the adoption of DevSecOps practices is essential for achieving secure software delivery governance.

The core principle of DevSecOps is the automation of security processes. By embedding security controls within the pipeline, organizations can ensure continuous compliance with governance policies. This includes automated vulnerability scanning, compliance checks, and policy enforcement mechanisms.

Recent research highlights the effectiveness of DevSecOps-driven security controls in reducing deployment inconsistencies and enhancing system resilience (Gangaiah et al., 2026). In ERP systems, these controls can be used to enforce security policies related to data protection, access control, and system integrity.

A key advantage of DevSecOps is its ability to provide real-time feedback on security issues. This enables organizations to address vulnerabilities before they impact production systems. Additionally, the use of infrastructure as code (IaC) allows for the automated configuration of secure environments, further enhancing governance.

However, the implementation of DevSecOps in ERP systems presents challenges, including the complexity of integrating legacy systems and the need for specialized skills. Addressing these challenges requires a strategic approach that aligns organizational processes with technological capabilities.

5.5 Governance Framework for ERP Deployment Security

The proposed governance framework for secure ERP deployment integrates multiple components, including policy management, risk assessment, compliance monitoring, and incident response.

Policy Management

Policies define the rules and standards that govern software delivery processes. These policies are encoded within the deployment pipeline, enabling automated enforcement.

Risk Assessment

Continuous risk assessment is essential for identifying potential vulnerabilities in the deployment workflow. This involves analyzing system behavior, detecting anomalies, and evaluating the impact of potential threats.

Compliance Monitoring

Compliance monitoring ensures that all deployment activities adhere to regulatory and organizational requirements. Automated tools are used to track compliance metrics and generate reports.

Incident Response

Effective incident response mechanisms enable organizations to quickly address security breaches. This includes automated alert systems, incident analysis, and corrective actions.

The integration of these components creates a comprehensive governance framework that enhances the security and reliability of ERP deployment workflows.

5.6 Real-World Application Scenarios

To illustrate the practical application of the proposed framework, consider a hypothetical enterprise undergoing digital transformation. The organization implements a cloud-based ERP system to manage its operations. By adopting the proposed governance framework, the organization integrates secure deployment pipelines with automated security controls.

During deployment, the system detects an anomaly in credential usage, triggering an automated response that

prevents unauthorized access. This demonstrates the effectiveness of governance mechanisms in mitigating security risks.

Another scenario involves the integration of e-governance services with ERP systems. Secure authentication mechanisms ensure that only authorized users can access sensitive data, while governance policies enforce compliance with regulatory requirements.

These examples highlight the practical benefits of secure software delivery governance in enhancing ERP system security.

RESULTS

The implementation of the proposed secure software delivery governance framework for ERP deployment workflows reveals several significant findings related to system security, operational efficiency, and governance effectiveness. The analysis, based on theoretical modeling and hypothetical enterprise scenarios, demonstrates measurable improvements in the robustness and reliability of ERP deployment processes.

One of the primary findings is the substantial reduction in authentication-related vulnerabilities. By integrating digital certificate-based authentication and centralized credential management within deployment pipelines, the framework effectively minimizes risks associated with unauthorized access. The use of cryptographic authentication mechanisms ensures that only verified entities can initiate or modify deployment processes, thereby enhancing system integrity. This aligns with prior findings in e-governance security research, which emphasize the importance of strong authentication models in protecting critical systems (Roy & Karforma, 2014).

Another key outcome is the improvement in deployment consistency and compliance. The incorporation of automated policy enforcement within the pipeline ensures that all deployment activities adhere to predefined governance standards. This eliminates inconsistencies caused by manual interventions and reduces the likelihood of configuration errors. The findings indicate that automated compliance checks significantly enhance the reliability of ERP deployment workflows, particularly in large-scale enterprise environments.

The study also highlights the effectiveness of DevSecOps integration in enhancing security posture. Continuous monitoring and real-time feedback mechanisms enable early detection of vulnerabilities, allowing organizations to address issues before they escalate into critical failures. The adoption of incident-aware pipeline strategies further improves system resilience by leveraging operational insights to refine security controls (Gangaiah et al., 2026). This demonstrates the value of integrating security intelligence into deployment workflows.

In addition, the framework shows improved adaptability to dynamic operational environments. ERP systems often operate in complex and evolving contexts, requiring flexible governance mechanisms. The use of role-based and attribute-based access control models allows for dynamic management of user permissions, ensuring that access policies remain aligned with organizational changes. This adaptability is critical for maintaining security in rapidly changing environments.

However, the findings also reveal certain limitations. The implementation of the proposed framework requires significant investment in infrastructure and expertise. Organizations must adopt advanced tools and

technologies to support automated security enforcement, which may pose challenges for smaller enterprises. Additionally, the integration of legacy systems into modern deployment pipelines can be complex and resource-intensive.

Despite these challenges, the overall results indicate that the proposed governance framework provides a robust solution for securing ERP deployment workflows. The combination of authentication mechanisms, automated policy enforcement, and continuous monitoring creates a comprehensive security environment that enhances both operational efficiency and system resilience.

DISCUSSION

The findings of this study provide critical insights into the role of secure software delivery governance in enhancing ERP deployment workflows. The integration of governance mechanisms within deployment pipelines represents a significant shift from traditional security approaches, which often operate as separate and reactive processes.

One of the key implications of this research is the validation of DevSecOps as an effective framework for implementing secure deployment governance. The ability to embed security controls directly within the pipeline ensures continuous enforcement of governance policies, reducing the reliance on manual interventions. This aligns with existing research that highlights the importance of integrating security into the software development lifecycle (Gangaiah et al., 2026). However, the application of DevSecOps in ERP systems requires careful adaptation to address the unique challenges associated with enterprise environments.

The study also underscores the importance of strong authentication and authorization mechanisms in maintaining system security. The use of digital certificates and cryptographic techniques provides a robust foundation for securing access to ERP systems. These findings are consistent with e-governance research, which emphasizes the effectiveness of such mechanisms in protecting sensitive data and ensuring system integrity (Roy & Karforma, 2014). The integration of these mechanisms within deployment workflows further enhances their effectiveness by ensuring consistent application across all stages of the lifecycle.

Another important aspect of the discussion is the role of governance frameworks in aligning security practices with organizational objectives. The proposed framework demonstrates how policy-driven controls can be integrated into deployment pipelines to ensure compliance with regulatory requirements and organizational standards. This highlights the importance of adopting a holistic approach to security that considers both technical and organizational factors.

However, the implementation of secure software delivery governance is not without challenges. The complexity of ERP systems, combined with the need for continuous updates and integration, creates a demanding environment for security management. Organizations must invest in advanced tools, skilled personnel, and robust infrastructure to effectively implement the proposed framework. Additionally, the integration of legacy systems presents significant challenges, as these systems may not be compatible with modern security practices.

The study also raises important considerations regarding the balance between security and operational efficiency. While the implementation of governance mechanisms enhances security, it may also introduce additional overhead in the deployment process. Organizations must carefully design their pipelines to minimize

performance impacts while maintaining high levels of security.

In comparison with existing literature, this research provides a more integrated perspective on secure ERP deployment governance. While previous studies have focused on individual aspects of security, such as authentication or DevSecOps practices, this study combines these elements into a comprehensive framework. This holistic approach addresses the limitations of fragmented security strategies and provides a more effective solution for managing complex ERP environments.

Overall, the discussion highlights the potential of secure software delivery governance to transform ERP deployment workflows. By integrating security controls, governance policies, and automated processes, organizations can achieve a higher level of security and operational efficiency.

CONCLUSION

This research has explored the critical role of secure software delivery governance in enhancing ERP deployment workflows within modern enterprise environments. As organizations increasingly adopt digital transformation strategies, the complexity and dynamism of ERP systems necessitate robust security frameworks that go beyond traditional approaches.

The study has demonstrated that integrating governance mechanisms within software delivery pipelines significantly improves system security, deployment consistency, and operational resilience. By leveraging advanced authentication models, automated policy enforcement, and DevSecOps practices, the proposed framework addresses key vulnerabilities associated with ERP deployments. The findings highlight the importance of embedding security controls directly into the deployment lifecycle, ensuring continuous compliance and real-time threat mitigation.

A major contribution of this research is the development of a comprehensive governance framework that aligns technical security measures with organizational objectives. The integration of authentication, authorization, monitoring, and incident response mechanisms provides a holistic approach to securing ERP systems. Additionally, the study emphasizes the value of incident-aware and feedback-driven pipelines in enhancing system adaptability and resilience.

Despite its contributions, the research acknowledges certain limitations, including the complexity of implementation and the challenges associated with integrating legacy systems. These limitations suggest the need for further research into scalable and cost-effective solutions for secure ERP deployment governance.

Future research directions may include the exploration of artificial intelligence and machine learning techniques for predictive security analysis, as well as the development of standardized frameworks for secure ERP deployment. Additionally, empirical studies involving real-world implementations would provide valuable insights into the practical effectiveness of the proposed framework.

In conclusion, secure software delivery governance represents a critical component of modern ERP systems. By adopting the proposed framework, organizations can enhance their security posture, ensure compliance with regulatory requirements, and achieve sustainable digital transformation.

REFERENCES

1. Customer User Manual - NAMA Supply, accessed on June 10, 2025.

2. Digital Transformation Strategy and Its Role in Developing Municipal Service Management, accessed on June 10, 2025.

3. Embracing Digitalization to Accelerate Oman's Economic Transformation in - IMF eLibrary, accessed on June 10, 2025, https://www.elibrary.imf.org/view/journals/002/2025/014/article-A004-en.xml.

4. 4. https://www.researchgate.net/publication/390425352_Digital_Transformation_Strategy_and_Its_Role_in_Developing_Municipal_Service_Management_A_Case_Study_of_Municipality_in_Oman.

5. Khatun R, Bandopadhyay T, Roy A : Data modeling for E-Voting system using smart card based E-Governance system. In: International Journal of Information Engineering and Electronic Business (IJIEEB), 9 (2), 45–52 (2017).

6. MTC.gov.om | FAQ, accessed on June 10, 2025, https://www.mtcit.gov.om/itaportal/Info/FAQ.aspx.

7. Oman Vision 2040: A Blueprint for Sustainable Growth and Global Integration, accessed on June 10, 2025, https://blogs.worldbank.org/en/arabvoices/oman-vision-2040-a-blueprint-for-sustainable-growth-and-global-integration.

8. Oman's FSA Warns of WhatsApp Scams and Fraudulent Websites Muscat Daily, accessed on June 10, 2025, https://www.muscatdaily.com/2024/08/20/omans-fsa-warns-of-whatsapp-scams-and-fraudulent-websites/.

9. Roy A., Karforma S. (2014). Data Modeling of a multifaceted electronic card based secure E-Governance system. In Z. Mahmood (Ed.), Emerging Mobile and Web 2.0 Technologies for Connected E-Government (pp. 280–299). USA : IGI Global.

10. Roy, A. : Information Security in E-Governance: A case study based analysis,. In: International Journal of Research in Engineering & Advanced Technology, 3 (1), 168–173 (2015), ISSN 2320-8791

11. Roy, A. : Synopsis on Information Security in E-Governance using Cryptography. In: International Journal of Advanced Technology in Engineering and Science, 2 (1), 432–445 (2014) ISSN (Online) 2348-7550

12. Roy, A, Karforma, Banik.: Implementation of authentication in E-Governance - An UML based approach. Germany, LAP LAMBERT Academic Publishing (2013) ISBN 978-3-659-41310-0

13. Roy, A., Karforma, S. : A Study on implementation of security in E-Governance using cryptography. In: International Journal of Advanced Research in Computer Science and Software Engineering, 4 (4), 652–659

(2014) ISSN (Online) 2277-128X

14. Roy, A., Karforma, S. : Authentication of user in E-Governance: A Digital Certificate based approach. In: International Journal of Scientific Research and Management, 2 (8), 1212–1221 (2014) ISSN 2321-3418

15. Roy, A., Karforma, S. : E-Governance To E-Commerce: A Smart Transition. In: International Journal of Emerging Research in Management and Technology, 3 (7), 82–86 (2014) ISSN 2278-9359

16. Roy, A., Karforma, S. : E-Governance to E-Health: A Smart Road Map For Society. In: The International Journal of Science and Technoledge, 2 (7), 217–221 (2014) ISSN 2321-919X

17. Roy, A., Karforma, S. : Stream cipher based user authentication technique in E- Governance transactions. In: International Society of Thesis Publication Journal of Research in Electrical and Electronics Engineering, 3 (3), 31–37 (2014) ISSN 2321-2667.

18. Sanad Service Centres sign six pacts, expand online services - Times of Oman, accessed on June 10, 2025, https://cdn-1.timesofoman.com/article/153598-sanad-service-centres-sign-six-pacts-expand-online-services.

19. Y. K. Gangaiah, K. Pappu and Y. S. Thanvi, "Devsecops-Driven Security Controls for ERP Release Pipelines," 2026 14th International Symposium on Digital Forensics and Security (ISDFS), Boston, MA, USA, 2026, pp. 1-6, doi: 10.1109/ISDFS69419.2026.11459076.