JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2025, VOL 8, NO S10

Data Security And Compliance In Modernized Cloud-Enabled Healthcare And Financial Systems

Sudharshan Kumar Ramayanam

Independent Researcher, USA.

Abstrac
Modernization of cloud-based healthcare and financial systems, compliance, and data security are complex issues as companies shift their legacy infrastructures to distributed infrastructures. This change harmonizes innovation needs with high regulatory demands in multifaceted frameworks such as HIPAA, GDPR, PCI-DSS, and SOX. The combination of old systems and new cloud systems also introduces special vulnerabilities to the migration processes, where advanced technical measures, such as encryption and secure exchange of data protocols, extensive key management, and identity systems are needed. The application of the standards of interoperability, including HL7 FHIR and ISO 20022, facilitates safe information exchange and ensures compliance with the help of special validation tools. Organizations can achieve a sustainable architecture by addressing security and compliance concerns as design elements and not as an appended element to the current architecture to generate a resilient system to guarantee that the regulations are observed, even in a changing technological environment.

Keywords: Cloud Security, Regulatory Compliance, Healthcare Interoperability, Zero-Trust Architecture, Data Sovereignty.

I. Introduction

The digital revolution in the medical and financial sectors has completely transformed the structures of operation and models of service delivery over the past years. Hospitals have progressively transformed the paper-based system into built-in digital platforms, and financial organizations rarely think about customer relationships using technology-based services. This change is not just the shift in the use of technology but the overall reconsideration of how an organization works to be responsive to the changing demands of the stakeholders living in a more interconnected world. This change has taken off at the speed of the outside forces to consolidate what would have taken years of slow change to achieve in the short-lived cycle of necessity-driven innovation that places a high value on accessibility and continuity of operation [1].

Cloud-enabled systems are the core of this transformation, which offer the scalability, computing power, and collaborative features that are essential in service delivery in an age of modernity. Healthcare facilities are moving toward the use of cloud computing in clinical information systems, data analytics, and administration, whereas financial institutions are turning to cloud computing in transaction processing, customer interactions, and risk management. These implementations provide significant payoff in terms of the optimization of resources- without having to maintain expensive excess resources during normal operations, organizations can dynamically scale up and down computing capacity when demand changes. Cloud architectures also allow sophisticated analytics, not possible in traditional computing methods, and support clinical decision support to fraud detection algorithms, and many more [2].

Sensitive information management in highly regulated settings is unique and becomes even more difficult when the data crosses past the traditional organizational borders. Healthcare organizations should exercise a high level of patient information protection and walk the fine line among highly complicated regulatory frameworks, such as HIPAA, that establish data handling practices. Likewise, financial institutions have to protect the financial records of customers under the law, like PCI-DSS and SOX, and allow authorized parties to access the data. The two industries are both faced with advanced threat environments, which will exploit risks at the system periphery and data transfer, necessitating holistic security strategies that go beyond the conventional perimeter protection [1].

Organizations constantly operate amid the tensions between the needs of innovation and security, a balancing exercise that characterizes effective modernization efforts. New capabilities should be implemented in conjunction with relevant security controls, and even in the context of regulatory frameworks, which are slow to change compared to technology. This relationship poses a lot of challenges to the organization, especially when the functions of technology and compliance work separately instead of working together [2].

A combination of security and compliance is the best strategy to address this issue by considering the issues in the early stages of the infrastructure design process until completion and operation of the infrastructure. Such an approach of security and compliance as a design changes the organizational mindset that these two factors are considered only after the implementation to ones that are considered as core design requirements integrated into the system architectures. Integrating these needs at the very beginning allows organizations to develop systems that automatically respond to regulatory needs and help to foster innovation, develop sustainable frameworks to undergo continuous change [1].

II. Regulatory Landscape and Compliance Requirements

The regulatory environment of healthcare, as well as the financial sectors, is becoming more multifaceted and has changed as a result of digitization and cloud adoption. The main area of HIPAA regulations that healthcare organizations encounter is the comprehensive regulation of patient information protection with the help of certain administrative, technical, and physical barriers. Organizations that process the European citizen data should also conform to GDPR rules that mandate clear consent procedures, data minimization guidelines, and breach notification procedures. Both financial institutions have equally strict frameworks, such as PCI-DSS on the protection of cardholder data and SOX on the accuracy of financial reporting. These frameworks have been mostly created before the popularity of cloud computing, and they create substantial interpretation difficulties as companies migrate sensitive workloads to distributed systems. The regulatory environment keeps changing at a fast rate, and organizations must keep in mind the dynamism of various compliance requirements within different jurisdictions [3].

Sector-specific compliance demands pose differences in sectors. Healthcare institutions have special concerns about patient consent management, especially concerning confidential groups such as genetic data, substance abuse treatment records, and mental health information. Another aspect of the healthcare industry that presents complex compliance environments is divergent state-level regulation on top of federal standards, making cross-state operations difficult. Another common challenge that financial institutions face is the increased frequency and prescriptive technical provisions, which are geared towards monitoring transactions, fraud detection, and audit capabilities. Both industries need strict access control systems and monitoring, but with varying emphasis: healthcare institutions should be concerned with clinical situations and relations between caregivers, whereas financial institutions should be focused on verifying transactions and detecting suspicious activities [4].

Cloud environments have led to a major change in compliance strategies because the old paradigm had assumed that the data would be confined within the organization's boundaries on infrastructure that would be directly managed by controlled parties. Regulatory agencies have, over time, created cloud-specific regulations that are related to shared responsibility models, vendor management practices, and data protection reviews. These requirements put more emphasis on the existence of clear contractual requirements between cloud providers and regulated organizations to help in the effective implementation of control across organizational boundaries. Such developments have been accompanied by the concept of

compliance as code that gives organizations the ability to enforce regulatory requirements as programmatic controls that are automatically deployed and reported in the cloud environments [3].
Geographic factors create significant complexity in terms of data sovereignty and transfers across borders. The principles of data sovereignty state that data stored physically is also governed by laws, and this presents a compliance challenge to distributed architectures. In healthcare organizations, there is often a rigid residency rule that does not allow to store the information about a patient beyond the national borders, especially in the European Union, Canada, and Australia. The case of geographic restrictions on personally identifiable financial information is also the same for financial institutions. The enforcement of these restrictions involves advanced technical controls such as data classification, location controls, and restrictions by geographic access [4].

Table 1: Regulatory Landscape and Compliance Requirements [3, 4]

Sector	**Key Regulations**	**Geographic Considerations**	**Compliance Evolution**
Healthcare	HIPAA, GDPR	Patient data residency requirements	Continuous monitoring replacing periodic assessments
Financial	PCI-DSS, SOX	Cross-border transaction limitations	Compliance-as-code implementation
Cross-Industry	Industry-specific frameworks	Data sovereignty principles	Automated compliance verification
Cloud-Specific	Shared responsibility models	Jurisdictional variations	Real-time configuration assessment

The compliance documentation has now advanced to the continuous monitoring strategies as opposed to the periodic assessment strategies due to the dynamic nature of the cloud environment. Companies should have a detailed record of compliance efforts, such as risk evaluations, policy records, and specifications of control implementation. Contemporary methods also take advantage of automated systems that compare cloud infrastructure to regulatory policies to identify and fix compliance failures as quickly as possible in the context of environments where infrastructure is delivered programmatically via automated deployment pipelines [3].

III. Security Challenges in Legacy-to-Cloud Migration

Migration to the new system is necessitated by the need to undertake extensive risk assessment mechanisms that consider the security issues that are unique to migration processes. Organizations need to assess multidimensional risks in terms of technological incompatibilities, operational, and the changing threat environment unique to distributed architectures. Proper assessment starts with proper analysis of the security controls that are present in the legacy environment and the compensating controls that ought to be adopted during the transition periods when the traditional security boundaries are blurred. The migration of clinical systems in healthcare organizations presents special challenges in cases where availability requirements are inadmissible, and financial institutions should pay close attention to transaction processing systems in which integrity breaches might produce downstream effects immediately. Effective companies have special risk governance boards that are cross-functional to assess security implications at every migration step, and that carry out continuous risk analyses instead of point-in-time risk evaluations that keep up with the dynamic character of migration processes [5].
The processes of cloud migrations create unique vulnerabilities as organizations exist in a state of transition between both past and present, with the legacy and cloud systems coexisting, but still allow continuity of operations. These transitional periods are usually longer than they were originally estimated, and they expose prolonged vulnerability to transition-related security issues. Vulnerabilities shared across environments include authentication differences, insufficient protection of information flowing between

systems, partial logging between the hybrid architectures, and insecure phases of integration between legacy systems and cloud services. Security visibility in transitional scenarios can be a major challenge in organizations because the monitoring tools used to track either the traditional data center or the cloud environments tend to offer partial views of the hybrid operations. Migration-related security surveillance is a highly sensitive control in such vulnerable times, and specialized monitoring to track authentication patterns, movement abnormalities, and modifications to access control in environments is also critical [6].
The integration of legacy systems has been extremely challenging in terms of security, especially when combining systems that are developed based on an architecture that may be decades old with the up-to-date cloud technology. The legacy systems frequently use outmoded authentication systems that are not compatible with current identity management systems and pose security risks when integrating with the new system. The encryption features of various environments are often widely varied, which requires elaborate translation layers that create a vulnerability in case of misuse. The restricted logging provision of most of the legacy platforms also complicates security attempts. Effective strategies deploy security intermediaries between the old and the cloud and have standardized controls such as modern authentication enforcement, extensive logging, encryption standardization, and behavioral analysis with the ability to detect possible compromises despite the limitations of the legacy systems [5].
Cloud environments essentially change organizational attack surfaces relative to traditional infrastructure and break down traditional network boundaries with resources that may be available via a variety of pathways based on configuration. The dynamic nature of provisioning of the cloud platforms presents configuration management issues because the environment is constantly changing due to both planned and unplanned changes. The physical segregation of infrastructure-related duties between providers and customers causes certain security vulnerabilities under the circumstances when the areas of responsibility are not clearly delineated. Resource misconfiguration is also a big security issue, especially in the process of migration, where security departments might lack experience with cloud-specific models. Effective security strategies focus on ongoing testing and not periodic tests, as the cloud environment changes faster than the traditional infrastructure [6].

Table 2: Security Challenges in Legacy-to-Cloud Migration [5, 6]

Challenge Category	**Legacy System Concerns**	**Transition Period Risks**	**Cloud Environment Considerations**
Authentication	Outdated mechanisms	Inconsistent implementation	Identity-based access models
Data Protection	Limited encryption capabilities	Transit protection gaps	Dynamic resource provisioning
Monitoring	Insufficient logging	Hybrid visibility challenges	Expanded attack surface
Integration	Architectural incompatibilities	Security control gaps	Configuration management
Governance	Static security models	Extended transition timelines	Shared responsibility boundaries

The issue of data classification is even more important when the migration of data occurs, since the data is transported across different environments with diverse levels of security. Good practices adopt formal classification systems with different levels of sensitivity that have set controls for each level. Healthcare organizations must maintain strict categorization of patient information, while financial institutions require careful classification of financial records and transaction data. Organizations demonstrating migration success implement data security frameworks addressing protection requirements across the full information lifecycle within both legacy and cloud environments [5].

IV. Technical Security Controls for Cloud-Enabled Systems

Encryption standards are also the building blocks towards protecting health and financial systems that are enabled by the cloud against unauthorized disclosure of data. The protocols of Transport Layer Security (TLS) are critical to securing data during transmission between system components, and current versions remove weak cipher suites and enhance the cryptographic algorithms. RSA encryption has continued to play an important role in asymmetric cryptography applications despite the increasing use of elliptic curve-based cryptography, but there is still an increasing requirement for the length of the key to use as computing power grows. Advanced Encryption Standard (AES) has become almost everywhere to encrypt data at rest in controlled settings, and financial and healthcare industries have generally adopted authenticated encryption schemes that are also used to check the integrity of data. Regular encryption in a hybrid environment is heavily difficult, especially in the case of integration with legacy applications that only use old cryptographic standards. The encryption gateways are usually developed by organizations to exchange between modern and legacy standards, but the elements in the middle should be carefully designed to prevent vulnerabilities being created at the point of transition [7].

Secure data exchange protocols facilitate doctor-to-doctor information transfer and inter-cloud information transfer with regulatory compliance. File transfer systems such as FTPS, SFTP are still being used in key roles in controlled environments, especially in batch processing processes, and integration of legacy systems. These standards have developed beyond simple transport encryption to include advanced authentication, extensive audit recordkeeping, and automatic security inspection of content exchanged. The use of APIs that are safeguarded using standards like the OAuth 2.0 has redefined the distribution patterns of data, allowing a more detailed access control and complete monitoring over traditional methods. Financial institutions introduce API security gateways, which provide uniform authentication and authorization across a variety of service endpoints, and healthcare organizations have used the same for integration of clinical systems. Regulated sectors tend to adopt data exchange zones that apply uniform security controls, disregarding certain protocols used, and all information transfers are provided with protection in accordance with data classification needs [8].

The most significant management approaches have changed significantly and are now developed to handle the distributed character of the cloud environments without exploiting the encryption material. Key management systems are centralized to give uniform lifecycle management to cryptographic keys in a variety of environments, and enact automatic rotation schedules that ensure cryptographic hygiene at minimal operational cost. Cloud-provided hardware security modules have been used to generate and secure sensitive keys, provide physical security, and remove complexity in operating specialized hardware. Split knowledge and dual control processes impose separation of duties on important key operations, whereby no individual administrator can obtain sensitive cryptographic material. The so-called bring own key has become a key idea because companies are interested in having control over the encryption key despite the use of managed cloud services [7].

Authentication and authorization of the distributed systems are regulated by an identity and access management framework. Role-based access control is still at the heart of most implementations, but is being supplemented more and more with attribute-based access control that uses contextual information in the process of determining access. Recent adoption uses standards of identity federation that provide uniform authentication experiences across different cloud environments and have centralized governance. Special interest management has been given specific attention in controlled sectors since organizations reduce standing access to protected systems. Just-in-time privileged access models have revolutionized the way of administration in that the privileged access that has always been high is now time-based and is granted only where necessary. The user behavior analytics add more and more to traditional controls and create baseline patterns and detect unusual activities that might be signs of compromised credentials [8].

Table 3: Technical Security Controls for Cloud-Enabled Systems [7, 8]

Control Domain	Key Technologies	Implementation Approaches	Security Framework Components
Encryption	TLS/SSL, AES, RSA	Transport and rest protection	Encryption gateways for legacy integration
Data Exchange	SFTP, FTPS, API security	Multi-layered protection	Protocol-specific controls
Key Management	Centralized KMS, HSM	Automated rotation	Separation of duties
Identity	RBAC, ABAC, Federation	Context-aware access	Just-in-time privileged access
Network Security	Zero-trust, Micro-segmentation	Software-defined segmentation	Continuous verification

Micro-segmentation and zero-trust security architecture have changed the model of cloud security by removing relayed trust through network location. Zero-trust principles demand pre-check of any access request, irrespective of the source, enforcing continuous authentication over the user experience. Micro-segmentation builds on these ideas by forming small security devices that have strictly defined channels of communication that are secured through strict access control procedures. Clinical network segmentation is used in healthcare organizations, whereas payment processing environments are segmented by financial institutions. The segmentation of the software-defined networking can be dynamically configured, unlike conventional methods of defining topology that relied on physical topology, and thus the security boundaries can adapt when components increase or change the environment [7].

V. Implementing Interoperability Standards While Maintaining Compliance

Interoperability standards in healthcare have been developed substantially to be able to strike a balance between the requirements of information sharing and the requirements of regulatory compliance in cloud-based settings. The Fast Healthcare Interoperability Resources (FHIR) Health Level 7 (HL7) has become a disruptive standard, tackling many of the weaknesses of the earlier healthcare data exchange solutions and offering improved security features in line with current authorization standards. This RESTful API-based standard has specific benefits in the case of cloud integration, where more specific and contextually relevant access controls can be made compared to message-based legacy standards. These capabilities are further extended to SMART on FHIR authorization framework, which uses an OAuth 2.0-based security designed specifically for healthcare settings, and supports patient-centric access models and clinical workflows, including other necessary exceptions to accommodate emergencies. The security concerns that organizations that adopt FHIR consider important are the protection of API endpoints, a proper range of scope of authorization tokens, and a detailed audit trail of every data access event. The introduction of standard security models into the FHIR interfaces poses specific challenges in hybrid environments in which both cloud-based and on-premises systems have to interact without any issues, and that retain regulatory compliance. Healthcare organizations usually deploy dedicated compliance certification of FHIR exchanges to determine whether all data transfers comply with the relevant regulatory obligations, such as HIPAA transaction criteria, minimum necessary restrictions, and jurisdiction-related consent regulations. This validation is further complicated by the information flowing among organizations that have varied compliance needs or cross or sub-jurisdictional borders that have different regulatory systems [9].

The standards of the financial data have also advanced to facilitate safe transactions and also facilitate interoperability across different systems and organizational boundaries. The ISO 20022 standard has achieved considerable usage in financial messaging, offering structured formats with clear security features such as support of digital signatures, non-repudiation, and financial-specific authentication extensions. The rich metadata of the messages of the ISO 20022 allows more advanced security measures than the legacy formats, facilitating better detection of fraud in case of anomalies and better regulation reporting in case of

standardized data formats. These foundations have been expanded by financial API standardization efforts, such as different Open Banking models that have created standardized account information interfaces and payment initiation interfaces with strong security considerations. Such requirements often involve robust customer authentication based on multi-factor authentication, explicit consent tracking including clear authorization of every data access, and extensive audit trails recording all the transaction information during the processing lifecycle. The adoption of these standards between clouds brings additional significant security concerns of protecting messages in transit and processing, and financial institutions apply specialized security controls to cloud-based message queuing services and API gateways. The multi-layered security strategies have been especially effective when it comes to financial data exchange, which incorporates transport, message, and application-level security to ensure that the sensitive financial data remains safe during the entire transaction lifecycle [10].

The issue of API security has been central to successful system integration because companies adopt cross-system communication within cloud infrastructure. Complete API protection frameworks provide coverage of several protection layers, such as authentication, authorization, input validation, output encoding, and rate limiting, to thwart numerous attacker vectors. The use of API gateways offers the central enforcement points of these security measures, which allow uniform application of the policy to a wide range of interfaces despite the technologies used at the implementation level. The OAuth 2.0 and the OpenID Connect have become standards of the API authentication and authorization with standard flows in the various access scenarios and with the relevant security controls in each case. Security testing of API interfaces has become a regular part of organizations developing new services, with specialized testing of API interfaces such as authorization bypass, injection attacks, exposing too much data, and resource exhaustion attacks, potentially impacting service availability. API security documentation has developed to encompass threat modeling, both explicit and implicit, with a description of the possible attack vectors and mitigation mechanisms against each interface. Security protection of the integration points of the legacy systems poses specific difficulties when the implementation of current security requirements is impossible directly on the old systems, and the organization applies the security proxies that apply the present-day security policies to the legacy interfaces. These proxies map between the existing and old authentication systems, enforce uniform authorization policies, and provide other supplemental security features such as input sanitization and extensive logging, which might not be present in the underlying systems [9].

Table 4: Implementing Interoperability Standards While Maintaining Compliance [9, 10]

Domain	Interoperability Standards	Security Mechanisms	Compliance Validation
Healthcare	HL7 FHIR	SMART on FHIR, OAuth 2.0	HIPAA transaction validation
Financial	ISO 20022	Digital signatures, Strong authentication	Regulatory reporting standardization
API Security	RESTful interfaces	OAuth/OpenID, Rate limiting	Security proxy implementation
Access Controls	Risk-based frameworks	Context signals, Behavioral patterns	Exception handling processes
Audit Mechanisms	Event streaming	Centralized monitoring	Cross-system correlation

The issue of finding the right balance between access and security controls is also complex in interoperable cloud environments when different user groups of various sizes need access to sensitive information using different devices and connection types. Security approaches that are risk-based carefully modify control requirements in real-time in response to various factors such as the sensitivity of the data, access context, user characteristics, and behavioral patterns. These adaptive models allow the more suitable security

measures than the static approach, and apply stronger protection in situations with higher risk and less friction in the interaction with lower risk. Context-based access controls use signals other than mere authentication credentials and consider the security posture of the device, the geographic location, the nature of connections, and usage patterns to make authorization decisions. Accessibility through mobile devices has brought specific innovation in the security solutions, whereas healthcare and financial applications have introduced specific controls such as attestation of the device to validate the endpoint integrity, user verification by biometric authentication, and application shielding technologies to resist attacker access at the device level. Organizations have a serious problem in aligning these security controls to regulatory requirements, which tend to dictate particular protection measures without considering risk factors depending on specific contexts and technological advancements. The healthcare providers use the specialized exception process in cases of emergency access to allow clinicians to have access to the information needed to treat the patient urgently and ensure that the audit trails of all the activities undertaken when the exceptional access is used are appropriate. Security and accessibility are dynamic, and this needs constant review and modification as technology, threat landscapes, and regulatory expectations change with time [10].

Conclusion

The secure cloud modernization strategic framework defines security and compliance as the core facilitators of innovation and not as a barrier to it. Developing organizations that are effective at negotiating this landscape use security by design concepts in the lifecycle of development in both the code and the deployment pipelines. Periodic assessment approaches have been substituted with constant monitoring of compliance, and automated validation offers real-time insight into the security posture of distributed environments. The sophisticated cloud solutions enhance security instead of crippling it now because they involve AI-based threat detection, behavioral analytics, and anomaly identification that are superior to conventional security protection systems. The regulatory technology environment is still dynamic towards standardized frameworks in reference to cloud architecture, and organizations are adopting compliance automation to ensure compliance in a fast-changing environment. To organizations planning a cloud modernization program, failure is likely to happen unless they come up with detailed security and compliance plans before the start of the migration process, come up with effective governance frameworks that have cross-functional checks, have strong identity foundations that can support zero-trust concepts, and have a constant evaluation mechanism during the transformation process. This combined solution allows companies to provide innovative features without compromising on the trust that is so necessary to regulated industries.

References

[1] Ahmad Al-Marsy et al., "A Model for Examining Challenges and Opportunities in Use of Cloud Computing for Health Information Systems," MDPI, 2021. [Online]. Available: https://www.mdpi.com/2571-5577/4/1/15

[2] Shekha Chenthara et al., "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing," IEEE Access, 2019. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8726303

[3] Ankur Mahida, "A Comprehensive Review on Ethical Considerations in Cloud Computing-Privacy, Data Sovereignty and Compliance," ResearchGate, 2022. [Online]. Available: https://www.researchgate.net/publication/379792762_A_Comprehensive_Review_on_Ethical_Considerations_in_Cloud_Computing-Privacy_Data_Sovereignty_and_Compliance

[4] Dereje Yimam and Eduardo B. Fernandez, "A survey of compliance issues in cloud computing," Journal of Internet Services and Applications, 2016. [Online]. Available: https://link.springer.com/content/pdf/10.1186/s13174-016-0046-8.pdf

[5] Vishnu Vardhan Reddy Boda and Hitesh Allam, "Automating Compliance in Healthcare: Tools and Techniques You Need," IJETCSIT, 2021. [Online]. Available: https://www.ijetcsit.org/index.php/ijetcsit/article/view/135

[6] Pavan Nutalapati, "A Review on Cloud Computing in FinanceTransforming Financial Services in the Digital Age," International Research Journal of Engineering & Applied Sciences, 2024. [Online]. Available: https://www.irjeas.org/wp-content/uploads/admin/volume12/V12I3/IRJEAS04V12I3005.pdf
[7] Sanjeevani Bhardwaj, "Cloud Infrastructure Modernization for Regulated Industries: Balancing Innovation, Compliance, and Scalability," Journal of Computer Science and Technology Studies, 2025. [Online]. Available: https://al-kindipublishers.org/index.php/jcsts/article/view/10987
[8] Kalaiprasath, R et al., "Cloud Security and Compliance - A Semantic Approach in End-to-End Security," ResearchGate, 2017. [Online]. Available: https://www.researchgate.net/publication/324770285_Cloud_security_and_compliance_-_A_semantic_approach_in_end_to_end_security
[9] Kinil Doshi et al., "Cloud Security Compliance: Best Practices and Key Considerations," ResearchGate, 2025. [Online]. Available: https://www.researchgate.net/publication/390107264_Cloud_Security_Compliance_Best_Practices_and_Key_Considerations
[10] Gideon Opeyemi Babatunde et al., "A Cloud Security Compliance Framework to Tackle Emerging Data Protection Issues in the U.S. and Canada," IRE Journals, 2024. [Online]. Available: https://www.irejournals.com/formatedpaper/1706123.pdf