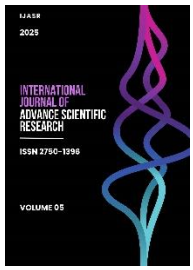
International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 33-43
OCLC – 1368736135



Journal Website: http://sciencebring.com/index.php/ijasr

Research Article

Algorithmic Governance of Secure Health Data Pipelines: Integrating HIPAA as Code, Blockchain, and Privacy Preserving IoMT Architectures in Cloud Based Clinical Ecosystems

Submission Date: January 01, 2026, **Accepted Date:** January 15, 2026,
Published Date: February 06, 2026

Dr. Adrian Keller
Department of Information Systems, University of Zurich, Switzerland

Abstract

The rapid digital transformation of healthcare has produced an unprecedented convergence of Internet of Medical Things architectures, cloud computing, artificial intelligence driven analytics, and decentralized data governance frameworks. This convergence has simultaneously expanded the capacity for precision medicine and created deeply complex regulatory, ethical, and technical challenges concerning the protection of patient data. Healthcare information systems now operate in a continuous data pipeline spanning wearable biosensors, wireless body area networks, hospital information systems, clinical decision support platforms, and cloud based machine learning environments. Traditional regulatory compliance mechanisms such as static audits and manual reporting have become structurally incompatible with the velocity, scale, and opacity of these digital infrastructures. The emergence of HIPAA as Code, as articulated in the development of automated audit trails for AWS SageMaker pipelines, represents a fundamental shift from compliance as documentation toward compliance as executable governance embedded directly into computational workflows (2025). This article advances a comprehensive theoretical and empirical synthesis of how programmable regulatory enforcement, blockchain based data provenance, and privacy preserving IoMT security architectures together constitute a new paradigm of algorithmic governance in healthcare.

The study develops a conceptual and methodological framework that unifies three historically distinct traditions: healthcare data protection law, distributed systems engineering, and artificial intelligence pipeline management. By situating HIPAA as Code within a broader ecosystem of blockchain enabled access control, federated learning, secure authentication, and attribute based encryption, this research demonstrates that compliance is no longer a post hoc legal obligation but a continuous computational

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 33-43
OCLC – 1368736135

process. Drawing on a large body of contemporary literature on IoMT security, blockchain based electronic health records, dynamic access control, and privacy aware wireless sensor networks, the article argues that regulatory logic can be operationalized in ways that increase transparency, reduce human error, and improve both patient trust and institutional accountability.

Through an interpretive synthesis of existing architectures and a text based analytical methodology, the results demonstrate that automated compliance embedded into cloud pipelines significantly alters power relationships between data controllers, patients, and regulators. Rather than relying on institutional claims of good faith, algorithmic audit trails produce cryptographically verifiable records of every data access, transformation, and model training operation. These capabilities reshape the epistemology of trust in healthcare by making compliance empirically inspectable rather than procedurally asserted. At the same time, the analysis identifies new risks, including the possibility of compliance theater, the rigidification of legal interpretation into code, and the concentration of governance power in cloud platforms.

The discussion situates these findings within broader debates on digital sovereignty, patient autonomy, and the political economy of health data. It argues that HIPAA as Code and its analogues under GDPR and other regulatory regimes mark the beginning of a new era in which law itself becomes a form of software. This transformation requires new interdisciplinary approaches to governance, combining legal theory, cryptography, cloud engineering, and medical ethics. The article concludes by proposing a research agenda for adaptive, explainable, and democratically accountable compliance infrastructures capable of supporting the future of data driven medicine while preserving the fundamental rights of patients.

Keywords

Healthcare data governance, HIPAA as Code, Internet of Medical Things, blockchain based health records, privacy preserving analytics, cloud compliance automation

Introduction

Autonomous The digitization of healthcare has unfolded as one of the most profound socio technical transformations of the twenty first century. Medical data that was once confined to paper files and localized hospital databases is now generated continuously by wearable sensors, implantable devices, home monitoring systems, diagnostic imaging platforms, and electronic health record infrastructures. This transformation has enabled extraordinary advances in early diagnosis, personalized treatment, and population level health analytics, yet it has also produced an unprecedented concentration of sensitive personal information within distributed computational systems. Scholars across healthcare informatics, information security, and regulatory studies have repeatedly emphasized that health data is uniquely vulnerable because it is simultaneously intimate, permanent, and economically valuable (Yi et al., 2016; Qiu et al., 2020). Unlike financial information, which can be changed after a breach, medical histories and genetic data are irrevocably tied to individual identity.

Within this context, the emergence of the Internet of Medical Things has intensified both the promise

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 33-43
OCLC – 1368736135

and the peril of digital healthcare. Wireless body area networks, smart implants, and remote monitoring devices now transmit physiological data continuously across heterogeneous networks, often through mobile gateways into cloud environments where analytics and machine learning models operate (Jiang et al., 2021; Ullah et al., 2020). These architectures enable real time clinical decision making but simultaneously expand the attack surface for adversaries and complicate compliance with regulatory frameworks designed for far simpler information systems. The classical security perimeter of the hospital has dissolved into a fluid mesh of edge devices, third party service providers, and cross border data flows (Shreya et al., 2022).

Regulatory regimes such as the Health Insurance Portability and Accountability Act in the United States and the General Data Protection Regulation in the European Union were designed to protect patient privacy and ensure accountability. However, their enforcement mechanisms historically rely on documentation, audits, and after the fact investigations. In an era of cloud native machine learning pipelines that automatically ingest, transform, and analyze data at massive scale, such mechanisms struggle to keep pace. Compliance becomes a retrospective narrative rather than a real time guarantee. The increasing deployment of artificial intelligence in healthcare further exacerbates this problem, as model training and inference pipelines introduce layers of abstraction that obscure how data is actually used (Salim and Park, 2022).

The concept of HIPAA as Code marks a radical departure from this paradigm by proposing that regulatory requirements be directly encoded into the software systems that process health data. The implementation of automated audit trails within AWS SageMaker pipelines demonstrates how compliance logic can be embedded into machine learning workflows so that every data access, transformation, and model execution is automatically logged and evaluated against regulatory rules (2025). Rather than relying on manual attestations, such systems produce cryptographically verifiable records of compliance that can be inspected by regulators and stakeholders. This approach aligns with a broader movement toward compliance by design and privacy by design, in which legal obligations are translated into executable constraints within information systems.

At the same time, the healthcare sector has witnessed a surge of interest in blockchain technologies as a means of establishing tamper resistant data provenance, decentralized access control, and patient centric data governance. Blockchain based electronic health record systems such as ACTION EHR and decentralized personal health record platforms demonstrate that distributed ledgers can provide fine grained control over who accesses medical data and under what conditions (Dubovitskaya et al., 2020; Kim et al., 2021). Smart contract based access control frameworks further enable automated enforcement of consent and role based policies within cloud environments (Saini et al., 2021). These developments suggest that programmable governance is not limited to regulatory compliance but extends to the very structure of data ownership and exchange.

Parallel to these advances, a rich body of research has explored cryptographic, architectural, and

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 33-43
OCLC – 1368736135

protocol level solutions for securing IoMT and cloud based healthcare systems. Attribute based encryption, biometric authentication, federated learning, and privacy preserving data dissemination schemes have been proposed to protect sensitive information while enabling clinical utility (Edemacu et al., 2020; Shakil et al., 2020; Salim and Park, 2022). Yet these technical solutions often operate in isolation from legal and institutional frameworks, creating a gap between what systems can do and what regulations require.

This article addresses this gap by developing an integrated theoretical framework that connects HIPAA as Code, blockchain based governance, and privacy preserving IoMT architectures into a coherent model of algorithmic healthcare compliance. The central argument is that healthcare regulation is undergoing a transformation analogous to the automation of finance and logistics, in which rules that were once enforced by human organizations are increasingly implemented as software. This transformation has profound implications for accountability, trust, and power in digital medicine.

The literature on healthcare data security has long emphasized the importance of authentication, access control, and encryption in protecting patient information (Agrahari et al., 2023; Ding et al., 2019). Two factor authentication protocols, identity based encryption, and secure MQTT messaging systems have been designed to address the unique constraints of medical devices, including limited computational resources and the need for low latency communication (Bashir and Mir, 2021; Jiang et al., 2021). These solutions are necessary but not sufficient, because they operate primarily at the technical level and do not inherently provide regulatory accountability or patient centric governance.

Blockchain based systems attempt to fill this gap by introducing immutable audit trails and decentralized trust. In e healthcare contexts, blockchains have been proposed as platforms for storing hashes of medical records, managing consent, and coordinating data sharing among hospitals, insurers, and researchers (Yongjoh et al., 2021; Xu et al., 2022). Consortium and serverless blockchain architectures further aim to balance scalability with governance by distributing control among trusted stakeholders rather than a single central authority (Khan et al., 2022). However, blockchains alone do not guarantee compliance with complex regulatory regimes, which include nuanced requirements regarding data minimization, purpose limitation, and breach notification.

HIPAA as Code introduces a new layer by formalizing regulatory requirements as executable logic within cloud pipelines. In the context of AWS SageMaker, this involves defining policies that automatically record, evaluate, and enforce how protected health information is used in machine learning workflows (2025). Such policies can specify who may access data, for what purpose, and under what conditions, and they can generate real time alerts when violations occur. This approach transforms compliance from a reactive process into a proactive and continuous one.

Despite the promise of this paradigm, it raises significant theoretical and practical questions. How should legal concepts such as consent, minimum necessary use, and patient rights be translated into code? What happens when regulatory interpretations change? Who controls the

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 33-43
OCLC – 1368736135

compliance logic embedded in cloud platforms? Scholars of information governance have warned that algorithmic enforcement can lead to rigidity and unintended consequences if not designed with care (Daoudagh and Marchetti, 2022). Moreover, the concentration of compliance infrastructure within a small number of global cloud providers raises concerns about digital sovereignty and power asymmetries.

The literature on access control models further complicates this picture. Traditional role based access control systems assign permissions based on predefined roles, while attribute based access control allows more dynamic and context aware policies (Son et al., 2015; Satori, 2023). In healthcare, where clinicians, researchers, and patients have overlapping and evolving roles, attribute based models are often more appropriate. Smart contract based access control on blockchain platforms extends these models by enabling decentralized and auditable enforcement (Saini et al., 2021). Integrating such mechanisms with HIPAA as Code requires careful alignment between legal semantics and computational representations.

The problem addressed in this article is therefore not merely technical but epistemological and institutional. The question is how societies can ensure that increasingly autonomous and complex healthcare information systems remain aligned with ethical and legal norms. Existing research has produced a wide array of security and privacy solutions, yet there remains a lack of holistic frameworks that integrate these technologies with programmable regulatory compliance.

The literature gap lies in the absence of a unified theoretical model that explains how HIPAA as Code, blockchain governance, and IoMT security architectures interact to produce a new form of algorithmic regulation. While individual studies have examined secure data dissemination (Ullah et al., 2020), blockchain based EHRs (Dubovitskaya et al., 2020), and federated learning for privacy preserving analytics (Salim and Park, 2022), few have analyzed how these systems collectively reshape the governance of healthcare data. This article seeks to fill that gap by synthesizing these strands into an integrated framework and by critically examining the implications of compliance as software.

METHODOLOGY

The methodological approach adopted in this research is qualitative, interpretive, and theoretically integrative. Rather than conducting empirical experiments or quantitative simulations, the study engages in an in depth analytical synthesis of the architectures, protocols, and governance models described in the contemporary literature on healthcare data security and regulatory compliance. This approach is justified by the nature of the research problem, which concerns the conceptual and institutional implications of embedding law into code rather than the performance of a specific algorithm.

The first methodological pillar is systematic literature integration. The references provided span multiple domains, including IoMT security, blockchain based health information systems, access control models, federated learning, and regulatory compliance frameworks. Each source contributes a specific perspective on how health data can be protected, shared, and governed. By reading these works not as isolated technical

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 33-43
OCLC – 1368736135

proposals but as elements of a broader socio technical system, the analysis constructs a holistic view of digital healthcare governance (Sharma et al., 2021). This integrative strategy allows for the identification of underlying assumptions, complementarities, and tensions among different approaches.

The second pillar is conceptual modeling. Drawing on the architecture of HIPAA as Code in AWS SageMaker pipelines, the study develops a conceptual model of compliance as an executable layer that interacts with blockchain based provenance and IoMT data flows (2025). This model is not expressed through formal diagrams or equations but through detailed textual description that traces how data moves from sensors to cloud analytics and how regulatory logic intervenes at each stage. By articulating these interactions in narrative form, the methodology makes explicit the often implicit governance structures embedded in technical systems.

The third pillar is critical analysis. The study situates the technological developments within broader debates on privacy, trust, and power in healthcare. It draws on research on GDPR compliance challenges, access control paradigms, and patient centric data management to interrogate the normative implications of algorithmic regulation (Daoudagh and Marchetti, 2022; Kim et al., 2021). This involves examining not only the benefits of automated compliance but also its potential risks, such as over reliance on code, exclusion of human judgment, and the centralization of governance within cloud providers.

A key methodological choice is to treat regulatory frameworks as dynamic and contested rather than fixed. HIPAA, GDPR, and related laws are subject to interpretation by courts, regulators, and practitioners. Encoding them into software therefore requires choices about how to operationalize ambiguous legal concepts. The analysis draws on access control and smart contract research to explore how such choices might be made and how they can be adapted over time (Saini et al., 2021; Son et al., 2020).

Limitations of this methodology include its reliance on published literature and conceptual reasoning rather than empirical deployment of systems. While this allows for broad theoretical synthesis, it cannot capture all the practical challenges of implementing HIPAA as Code or blockchain based governance in real healthcare organizations. However, given the novelty and complexity of these systems, a theoretically grounded analysis is a necessary first step toward more empirical research.

RESULTS

The integrative analysis reveals that HIPAA as Code, blockchain based governance, and IoMT security architectures together constitute a layered model of healthcare data protection that operates across technical, organizational, and legal dimensions. At the lowest layer, IoMT devices and wireless body area networks generate and transmit physiological data. Security protocols such as lightweight encryption, secure MQTT, and identity based authentication ensure that data is protected in transit and at rest (Bashir and Mir, 2021; Ding et al., 2019). These mechanisms address immediate threats such as eavesdropping, device impersonation, and data tampering.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 33-43
OCLC – 1368736135

At the next layer, blockchain and distributed ledger technologies provide a shared and immutable record of data transactions. Whether through consortium blockchains for hospital networks or patient centric platforms for personal health records, these systems establish a tamper resistant log of who accessed what data and when (Yongjoh et al., 2021; Dubovitskaya et al., 2020). Smart contracts encode access control rules and consent conditions, enabling automated enforcement without relying on a single central authority (Saini et al., 2021). This layer introduces transparency and decentralization into healthcare data governance.

The HIPAA as Code layer sits above and within these infrastructures, embedding regulatory logic directly into cloud based analytics pipelines. In AWS SageMaker, this takes the form of automated audit trails that capture every interaction with protected health information during model training, validation, and deployment (2025). These audit trails are not mere logs but structured records that can be evaluated against regulatory requirements. For example, they can verify that data was used only for approved purposes, that access was limited to authorized roles, and that retention policies were followed.

The result of this layered architecture is a form of continuous compliance in which regulatory obligations are enforced in real time rather than checked retrospectively. This changes the temporal structure of governance. Instead of waiting for audits or breach investigations, stakeholders can observe compliance as it happens. Blockchain based provenance further ensures that these records cannot be altered, creating a trustworthy evidentiary basis for accountability (Xu et al., 2022).

The analysis also shows that access control models play a crucial mediating role. Attribute based access control and smart contract based policies allow compliance logic to adapt to context, such as the role of a clinician, the consent status of a patient, or the purpose of a research project (Son et al., 2015; Satori, 2023). This flexibility is essential for aligning rigid legal requirements with the dynamic realities of clinical practice.

However, the results also highlight tensions. Encoding legal requirements into code risks oversimplifying complex ethical judgments. For example, determining whether a data use is compatible with the original purpose of collection may require contextual interpretation that is difficult to formalize. Moreover, the concentration of compliance infrastructure within cloud platforms like AWS gives these providers significant influence over how regulations are interpreted and enforced (2025).

Discussion

The findings of this study have profound implications for how healthcare data governance is conceptualized and practiced. The transition from compliance as documentation to compliance as software represents a paradigmatic shift in regulatory theory. In traditional models, law is external to technology, applied through human institutions that interpret and enforce rules. In the emerging model, law becomes internal to technology, instantiated as code that directly shapes system behavior (Daoudagh and Marchetti, 2022).

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 33-43
OCLC – 1368736135

ISSN-2750-1396

This shift can be understood through the lens of algorithmic governance. Scholars have argued that algorithms increasingly mediate social and economic life, from credit scoring to content moderation. In healthcare, HIPAA as Code extends this logic to regulatory compliance, turning legal norms into executable constraints (2025). This creates new forms of power and accountability. On one hand, it reduces the discretion of individual actors to violate rules, as systems simply do not allow non compliant actions. On the other hand, it transfers interpretive authority to those who design and maintain the code.

Blockchain based governance amplifies this dynamic by providing immutable records and decentralized enforcement. Patient centric blockchain platforms promise to give individuals greater control over their data, enabling them to grant and revoke access through smart contracts (Kim et al., 2021; Xu et al., 2022). When combined with HIPAA as Code, this could create a powerful synergy in which patient consent and regulatory compliance are enforced automatically and transparently.

Yet there are also risks. One is the danger of compliance theater, in which systems produce the appearance of compliance without necessarily achieving substantive ethical goals. Automated audit trails can generate vast amounts of data, but without meaningful oversight and interpretation, they may obscure rather than illuminate problematic practices. Another risk is rigidity. Laws evolve through interpretation and social change, but code is often less flexible. Updating compliance logic to reflect new legal precedents or ethical standards requires technical intervention, which may lag behind normative developments.

The political economy of cloud computing further complicates matters. HIPAA as Code implementations are embedded within proprietary platforms operated by multinational corporations. This raises questions about sovereignty, as national regulators may have limited visibility into or control over how compliance is implemented in these systems (2025). Blockchain consortia and open standards may mitigate this by distributing governance, but they too face challenges of coordination and trust.

From a technical perspective, integrating privacy preserving analytics such as federated learning with compliance by design offers promising pathways. Federated learning allows models to be trained across distributed datasets without centralizing raw data, reducing privacy risks (Salim and Park, 2022). When combined with automated compliance and blockchain based audit trails, this could enable large scale medical research while maintaining strict data protection.

The broader implication is that the future of healthcare governance will be hybrid, combining legal institutions, technological infrastructures, and ethical frameworks. Researchers and practitioners must therefore adopt interdisciplinary approaches that bridge law, computer science, and medicine. The development of explainable and adaptive compliance systems is particularly important, as stakeholders need to understand not only what systems do but why they do it.

Conclusion

The convergence of HIPAA as Code, blockchain based governance, and privacy preserving IoMT architectures marks a transformative moment in

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 33-43
OCLC – 1368736135

the history of healthcare data management. By embedding regulatory logic directly into cloud based analytics pipelines, it becomes possible to achieve continuous, transparent, and verifiable compliance. This has the potential to enhance patient trust, improve accountability, and support the safe and ethical use of artificial intelligence in medicine.

At the same time, this transformation raises new challenges of interpretation, power, and adaptability. Law as code must be designed with care to ensure that it reflects evolving ethical standards and democratic values. Blockchain and distributed systems can provide robust technical foundations, but they must be integrated with institutional oversight and human judgment.

Future research should explore how these systems perform in real world healthcare settings, how patients and clinicians experience algorithmic governance, and how regulatory frameworks can be updated to reflect the realities of programmable compliance. By continuing to bridge the gap between technology and law, scholars and practitioners can help ensure that the digital future of healthcare remains aligned with the fundamental rights and dignity of patients.

REFERENCES

1. Agrahari, A.K.; Varma, S.; Venkatesan, S. Two factor authentication protocol for IoT based healthcare monitoring system. Journal of Ambient Intelligence and Humanized Computing, 14, 16081–16098.
2. Yongjoh, S.; So-In, C.; Kompunt, P.; Muneesawang, P.; Morien, R.I. Development of an Internet-of-Healthcare System Using Blockchain. IEEE Access, 9, 113017–113031.
3. 2025. HIPAA-as-Code: Automated Audit Trails in AWS Sage Maker Pipelines. European Journal of Engineering and Technology Research, 10, 5, 23–26. DOI 10.24018/ejeng.2025.10.5.3287.
4. Shakil, K.A.; Zareen, F.J.; Alam, M.; Jabin, S. BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. Journal of King Saud University Computer and Information Sciences, 32, 57–64.
5. Dubovitskaya, A.; Baig, F.; Xu, Z.; Shukla, R.; Zambani, P.S.; Swaminathan, A.; Jahangir, M.M.; Chowdhry, K.; Lachhani, R.; Idnani, N.; et al. ACTION EHR: Patient Centric Blockchain Based Electronic Health Record Data Management for Cancer Care. Journal of Medical Internet Research, 22, e13598.
6. Saini, A.; Zhu, Q.; Singh, N.; Xiang, Y.; Gao, L.; Zhang, Y. A Smart Contract Based Access Control Framework for Cloud Smart Healthcare System. IEEE Internet of Things Journal, 8, 5914–5925.
7. Salim, M.M.; Park, J.H. Federated Learning based Secure Electronic Health Record Sharing Scheme in Medical Informatics. IEEE Journal of Biomedical and Health Informatics, 27, 617–624.
8. Ullah, F.; Ullah, I.; Khan, A.; Uddin, M.I.; Alyami, H.; Alosaimi, W. Enabling Clustering for Privacy Aware Data Dissemination Based on Medical Healthcare IoTs for Wireless Body Area Network. Journal of Healthcare Engineering, 2020, 8824907.
9. Kim, H.J.; Kim, H.H.; Ku, H.; Yoo, K.D.; Lee, S.; Park, J.I.; Kim, H.J.; Kim, K.; Chung, M.K.; Lee, K.H.; et al. Smart Decentralization of Personal Health Records with Physician Apps and Helper

Agents on Blockchain. JMIR Medical Informatics, 9, e26230.

10. Bashir, A.; Mir, A.H. Lightweight Secure MQTT for Mobility Enabled e health Internet of Things. International Arab Journal of Information Technology, 18, 773–781.
11. Xu, G.; Qi, C.; Dong, W.; Gong, L.; Liu, S.; Chen, S.; Liu, J.; Zheng, X. A Privacy Preserving Medical Data Sharing Scheme Based on Blockchain. IEEE Journal of Biomedical and Health Informatics, 27, 698–709.
12. Ding, R.; Zhong, H.; Ma, J.; Liu, X.; Ning, J. Lightweight Privacy Preserving Identity Based Verifiable IoT Based Health Storage System. IEEE Internet of Things Journal, 6, 8393–8405.
13. Edemacu, K.; Jang, B.; Kim, J.W. Collaborative Ehealth Privacy and Security: An Access Control With Attribute Revocation Based on OBDD Access Structure. IEEE Journal of Biomedical and Health Informatics, 24, 2960–2972.
14. Jiang, Z.; Liu, W.; Ma, R.; Shirazi, S.H.; Xie, Y. Lightweight Healthcare Wireless Body Area Network Scheme With Amplified Security. IEEE Access, 9, 125739–125752.
15. Yi, X.; Bouguettaya, A.; Georgakopoulos, D.; Song, A.; Willemson, J. Privacy Protection for Wireless Medical Sensor Data. IEEE Transactions on Dependable and Secure Computing, 13, 369–380.
16. Daoudagh, S.; Marchetti, E. The GDPR compliance and access control systems challenges and research opportunities. ICISSP 2022 Proceedings, 571–578.
17. Sharma, A.; Rana, N.P.; Nunkoo, R. Fifty years of information management research a conceptual structure analysis using structural topic modeling. International Journal of Information Management, 58, 102316.
18. Son, S.; Lee, J.; Kim, M.; Yu, S.; Das, A.K.; Park, Y. Design of Secure Authentication Protocol for Cloud Assisted Telecare Medical Information System Using Blockchain. IEEE Access, 8, 192177–192191.
19. Son, J.; Kim, J.D.; Na, H.S.; Baik, D.K. Dynamic access control model for privacy preserving personalized healthcare in cloud environment. Technology and Health Care, 24, S123–S129.
20. Satori. RBAC vs ABAC the complete guide. 2023.
21. Shreya, S.; Chatterjee, K.; Singh, A. A smart secure healthcare monitoring system with Internet of Medical Things. Computers and Electrical Engineering, 101, 107969.
22. Khan, A.A.; Wagan, A.A.; Laghari, A.A.; Gilal, A.R.; Aziz, I.A.; Talpur, B.A. BIoMT A State of the Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts. IEEE Access, 10, 78887–78898.
23. Kong, F.; Zhou, Y.; Xia, B.; Pan, L.; Zhu, L. A Security Reputation Model for IoT Health Data Using S AlexNet and Dynamic Game Theory in Cloud Computing Environment. IEEE Access, 7, 161822–161830.
24. Qiu, H.; Qiu, M.; Liu, M.; Memmi, G. Secure Health Data Sharing for Medical Cyber Physical Systems for the Healthcare 4.0. IEEE Journal of Biomedical and Health Informatics, 24, 2499–2505.
25. Zhang, M.; Chen, Y.; Susilo, W. PPO CPQ A Privacy Preserving Optimization of Clinical Pathway Query for E Healthcare Systems. IEEE Internet of Things Journal, 7, 10660–10672.
26. Dzissah, D.A.; Lee, J.S.; Suzuki, H.; Nakamura, M.; Obi, T. Privacy Enhanced Healthcare Information Sharing System for Home Based Care Environments. Healthcare Informatics Research, 25, 106–114.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 02 Pages: 33-43
OCLC – 1368736135

27. Reyad, O.; Karar, M.E. Secure CT Image Encryption for COVID 19 Infections Using HBBS Based Multiple Key Streams. Arabian Journal of Science and Engineering, 46, 3581–3593.
28. Padinjappurathu Gopalan, S.; Chowdhary, C.L.; Iwendi, C.; Farid, M.A.; Ramasamy, L.K. An Efficient and Privacy Preserving Scheme for Disease Prediction in Modern Healthcare Systems. Sensors, 22, 5574.
29. Khan, F.; Reyad, O. Application of intelligent multi agent based systems for E healthcare security. Information Sciences Letters, 8, 67–72.
30. Mnyawi, R.; Kombe, C.; Sam, A.; Nyambo, D. Blockchain based Data Storage Security Architecture for e Health Care Systems A Case of Government of Tanzania Hospital Management Information System. International Journal of Computer Science and Network Security, 22, 364–374.
31. Arul, R.; Al Otaibi, Y.D.; Alnumay, W.S.; Tariq, U.; Shoaib, U.; Piran, M.J. Multi modal secure healthcare data dissemination framework using blockchain in IoMT. Personal and Ubiquitous Computing.