Open Access

SCHOLARENA

SAJ Pharmacy and Pharmacology

RESEARCH ARTICLE

ISSN: 2375-2262

Enhancing Data Security and Efficiency in Online Pharmacies through Cloud Technology

Friday Othniel Enyo[1, *], Sunday Bakel Samuel[1], Konstantin KOSHECHKIN[2]

[1]*Department of Epidemiology and Evidence-based Medicine, F.Erisman Institute of Public Health, I.M Sechenov First Moscow State Medical University, Moscow, Russia*

[2]*Department of Business Administration in Public Health Care, I.M Sechenov First Moscow State Medical University, Moscow, Russia*

[*]**Corresponding Author:** Friday Othniel Enyo, Department of Epidemiology and Evidence-based Medicine, F.Erisman Institute of Public Health, I.M Sechenov First Moscow State Medical University, Moscow, Russia, Tel.: +79991140702, E--mail: othnielenyo@gmail.com

Citation: Friday Othniel Enyo, Sunday Bakel Samuel, Konstantin KOSHECHKIN (2025) Enhancing Data Security and Efficiency in Online Pharmacies through Cloud Technology, J Pharm and Pharmacol 10: 101

Abstract

The continuous upscaling of online pharmacies have progressed immensely, this growth is catalysed by a series of both regional and global health crises and gross changes in consumer's mode of operation. However, this positivity is followed by a series of difficult situations such as patient data protection and maintenance as well as improving operational efficiency. This study demystifies how cloud technology can stabilize pharmaceutical services while also cautioning the urgent security and conformance issues. A systematic literature review spans through studies from 2014 to 2025 as important databases including Researchgate, PubMed and Google Scholar were queried for relevant information. Series of research portray negativities arising from the integration of cloud-based systems among which is data breaches and other security risks. Via backgrounds of several cases, this research examines the interlocking of both cloud services, digital patient care, data protection regulations as well as blockchain-enhanced privacy measures. It summarizes a fact that an all-encompassing cloud-based solutions tightened with regulatory compliance and advanced auditing mechanisms are important in building a secure, efficient, and trustworthy online pharmaceutical terrain. The paper endorses a strategic data governance architecture including stakeholder accountability in an attempt to scale digital transformation in pharmaceutical outputs while limiting all forms of systemic risks.

Keywords: Cloud Computing; Cloud-based solutions; Data Management; Data Governance; Pharmaceuticals

Introduction

The online pharmacy market has continued to grow on a rapid scale based on its chains and supply algorithm since the start of this century [1, 2]. Despite its surge in adoption, the actual market size remains difficult to analyse, with a host of internet pharmacies accessible worldwide [3]. Though the purchase of pharmaceutical products from legalized online pharmacies remains an accepted action in most developed countries, different studies have ascertained important changes in demands from consumers for long range buying of pharmaceutical products [4]. The market is ravaged by scammers and fraudulent elements thus poses a significant risk for patients who sought patronage [5-8]. Engaging cyberspace, the cloud may remotely host and offer different computer services to users as it promises both flexibility, storage, automation, and lower prices. As reported by [9] cloud computing advances patient care as it is the most basic information technology that has become a connective tool for collaboration, communication, and invention in countries and across continents. The pharmaceutical industry has long adopted advanced technologies to enhance drug development, manufacturing processes, and quality control. In recent years, the integration of computerized systems has become ubiquitous, revolutionizing various aspects of pharmaceutical operations [10]. These systems range from laboratory information management systems (LIMS) to enterprise resource planning (ERP) software, playing crucial roles in data management, process control, and regulatory compliance. As the industry continues to evolve, there has been a significant shift towards cloud-based systems. This transition is driven by the numerous advantages cloud computing offers, including scalability, cost-effectiveness, and improved accessibility [11]. Whereas existing literature has referred to cloud adoption in the healthcare industry at large, a particular exploration of internet pharmacies—encompassing the particular intersection of e-commerce activities, stringent pharmaceutical regulations (e.g., GDPR and HIPAA), and real-time data safety for very personal patient data—has been lacking. This paper attempts to bridge this gap by systematically examining the potential for cloud computing to be custom-developed to mitigate data threats and maximize organizational efficiency in the online pharmacy industry, proposing an adaptive, integrated architectural model for future development.

Methodology

Study Design

This study was designed based on the previous studies published between January 2015 and February 2025 were obtained and relevant information was deduced as basics for improvement.

Search Strategy

A systematic literature search was conducted on four online databases: PubMed, Scopus, Google Scholar, and ResearchGate to give peer-reviewed as well as grey literature. Keywords and Boolean operators were used for searching. The primary search query was: ("cloud computing" OR "cloud-based solutions" OR "cloud technology") AND ("online pharmacy" OR "e-pharmacy" OR "digital pharmacy" OR "pharmaceutical services"). Though there were no linguistic restrictions at the initial stage, the final review was limited to publications made in English. In an attempt to capture both technological and regulatory progress made in recent times, the research was restricted to embody studies published between January 2015 and February 2025. 238 records were generated.

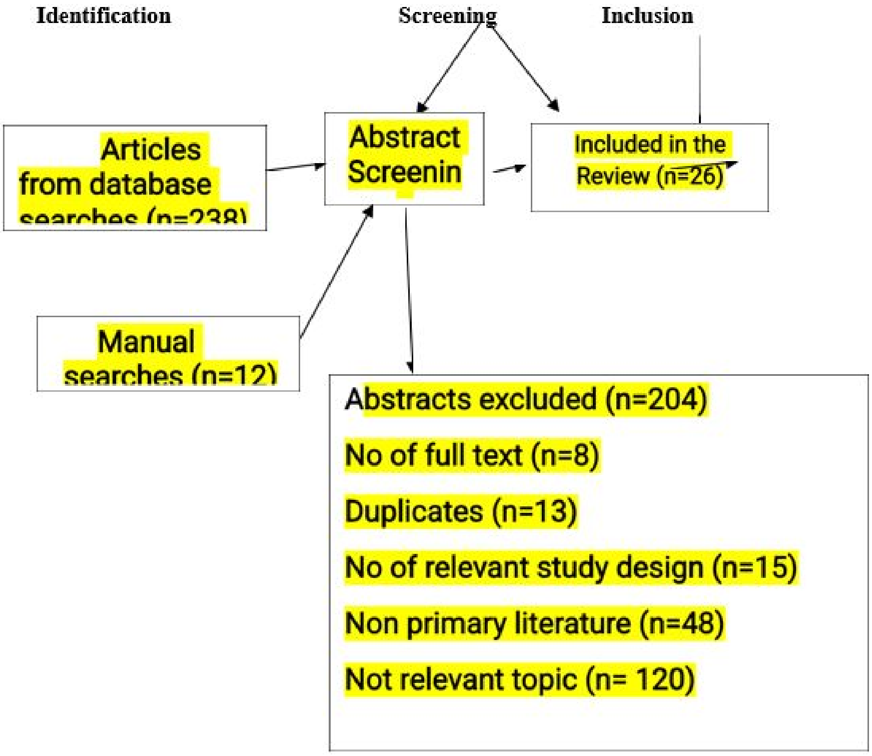
Identification
Screening
Inclusion
Articles from database searches (n=238)
Abstract Screenin
Included in the Review (n=26)
Manual searches (n=12)
Abstracts excluded (n=204)
No of full text (n=8)
Duplicates (n=13)
No of relevant study design (n=15)
Non primary literature (n=48)
Not relevant topic (n= 120)

Figure 1: Flow chart of the systematic search of literature.

A summary of the systematic search which started with 238 searched articles. This number was refined to 26 articles included in the final review (204 excluded articles) based on the pre-defined inclusion/exclusion criteria.

Data Extraction

Any information that was not found in the literature was forwarded by email to the article's related author. Issues that arose during the data extraction procedure were solved with the assistance of a third party. The first author's name, the research type, the year of publication, the research design method, type of cloud models discussed (e.g IaaS, SaaS), key findings related to security or efficiency and the main conclusions are all included in the content of the extracted data. Only the most recent research report was considered for this study.

Inclusion and Exclusion Criteria

The following were the inclusion criteria for this study;

- Peer-reviewed journal articles, conference papers, reputable white papers, systematic reviews, and government or industry reports;
- Studies published from 2015 to 2025, to reflect current cloud technologies and cyber-security practices.
- Global scope, including both developed and developing countries to allow for broader insights;
- Studies focusing on online pharmacies**,** e-health platforms**, or** telemedicine systems**.**
- Research exploring cloud computing**,** data security, and system efficiency in healthcare or pharmacy IT systems;

- Studies addressing data privacy laws (e.g., HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation)) in relation to cloud storage in healthcare;
- Papers discussing cloud-based cybersecurity threats and solutions in pharmacy or e-health systems.

The exclusion criteria were as follows:

- Studies not related to healthcare, pharmacy, or cloud technology (e.g., general e-commerce or unrelated IT infrastructure);
- Studies focusing solely on obsolete or legacy systems (pre-2015 cloud models);
- Blogs, newsletters, opinion pieces, or non-scholarly sources unless from reputable government or institutional websites;
- Papers focused entirely on brick-and-mortar pharmacies without an online or cloud-based components;
- Studies on online pharmacies that do not address security or efficiency, even if cloud-based.

Meta-analyses

Meta-analyses were conducted to combine similar studies that had comparable data in the results. Meta-analyses were not conducted in cases where data are not comparable. Comparing different outcome parameters, if only one study meets the criteria. Meta-analyses were conducted on Review Manager 5.4.1 using inverse variance (IV) as the statistical model and a fixed effect analysis model. Results from the meta-analyses were displayed in forest plot form alongside data used in the corresponding meta-analysis.

Quality Assessment

The credibility of the findings was carefully evaluated to ascertain the scientific accuracy of the included publications. The Cochrane Risk of Bias tool (RoB 2) was used to evaluate potential randomization bias, deviations from the intended interventions, missing outcome data, outcome measurement, and selection of the reported results for the quantitative and comparative studies that were used in the meta-analysis. For qualitative reviews and systematic reviews, the tool AMSTAR 2 (A MeaSurement Tool to Assess systematic Reviews 2) was applied for evaluating methodological quality. The quality appraisal was independently conducted by two authors, and conflicts were solved by referring to a third reviewer. This helped ensure that conclusions arrived at this review are based on methodologically sound evidence.

Review of Literatures

An Online Pharmacy

The trend for the use of online pharmacies has increased in recent time in respect to the insurgence of the Covid-19 pandemic, although most consumers still really prefer and rely on the tradition of buying pharmaceutical products and supply but the trend of online pharmacies have increased in most regions. Despite this, all of these online pharmacies have not been able to replace the traditional offline pharmacies [12]. Customers can simply visit the website to see local stores who have their product of interest, then place an order or reserve them. The platform prefers displaying medicine that is available nearby, and if not found locally, it searches wider areas. Additionally, retailers can create a personalized application through the website, while users can quickly find and secure their medicines without the hassle of searching from place to place. To illustrate the significance of General Data Protection Regulation (GDPR) compliance verification in a multi-cloud system, a cloud-based pharmacy scenario is utilized, which was inspired by the DermaTran software from dinCloud [13, 14]. Think about a customer who goes to an online pharmacy that is hosted in the cloud to place an order, pay, and have a prescription sent to their home address. Following order placement, the pharmacy extends the user's Electronic Health Record (EHR) and retrieves a variety of personal user data, including name, address, GP diagnosis, prescription, and bank account information. Cloud4U, an IaaS provider, receives the data; the pharmacy employs Cloud4U to host and run its mobile app and website. "Social plugins" (a "Like" and "Share" button) from a popular social network (Friendface) are integrated into the pharmacy's website and mobile app. When a user accesses the online pharmacy's website or launches the app, the Friendface API is made to automatically send the user's personal information, including IP address and location data, to Friendface [15-17]. Friendface utilizes this information to enhance the patient profile it has developed over time (a process known as profiling), which is beneficial for its advertising business. In order to generate additional money, the online pharmacy also sells advertising inventory space on its website and mobile app through the real-time bidding (RTB) system of a well-known online advertiser and intermediary (Froogle). This approach entails a great deal of profiling and sharing of personal information with other businesses (actors) in the ad techchain, including location, device characteristics, unique tracking ID, and browsing behaviors. Froogle's "Supply Side Platform" broadcasts personal information on behalf of the pharmacy in order to request bids from businesses who could be interested in showing the pharmacy's user an advertisement [18-20]. From the research of [20], it is clear that 46 % of the sample respondents were happy with offline purchase of medicine while 32.63 % of the sample respondents who also purchase medicines online feel that attractive discounts on prices and offers are major factor for their decision (personal reflection is required) therefore it becomes pertinent to generate incentives and clauses in respect to online purchase in an attempt to upscale patronage and widespread adoption.

Cloud-Based Pharmacy

Cloud computing is a kind of computer model in which a very large and vast networks are link to a private and public network, which provides a scalable and flexible medium for application, data and file management. This technology is super financially friendly when it comes to the computing, application hosting content storage and delivery of data [21]. Think about a cloud data center-hosted online pharmaceutical service, like dincloud [22-26]. After receiving prescription requests from patients, the service verifies that the medications are available and creates an invoice for the patient. In order to keep track of pertinent data regarding patients' health, the service also keeps an electronic health record (EHR) system [27-30]. To manage the payment and delivery of medications, the pharmacy service provider has two subcontractors: a payment service provider and a shipping service provider [32-33]. Infrastructure solutions can be delivered through cloud-based services. Most of the services are operated externally through a service provider and are accessed over the internet. They are categorized into two different types as illustrated in figure 2.

The cloud technology is made up of the Software-As-A-Service (SAAS) which gives millions of users a chance to connect to a single source of data, though in recent times, customers now have an individual-based software where each individual is given an opportunity to manage his or her catalogue but the ability of SAAS to orient a “Multi-tenancy” model outshines a software such as the individual-based. This software is incorporated with a code scanner capable of reading barcodes on medicines for both entries, tracking and dispensary upon request as an option of printing receipts are made available to the chemist [34].

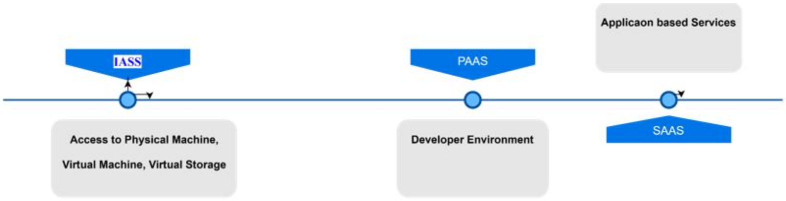
Applicaon based Services
IASS
PAAS
SAAS
Access to Physical Machine, Virtual Machine, Virtual Storage
Developer Environment

Figure 2: Components of cloud technology [35]

Figure 2 above reveals the various components of cloud technology that enhance computing efficiency and flexibility. Users gain access to physical machines through abstraction, enabling resource sharing. A virtual machine emulates a real computer, allowing multiple systems to run on one host. Virtual storage offers scalable, on-demand data storage independent of physical hardware. A developer environment provides tools and platforms for coding, testing, and deploying applications within the cloud. Additionally, application-based services deliver ready-to-use software solutions over the internet, eliminating the need for local installation. Together, these components create a robust infrastructure for scalable, secure, and efficient computing in modern digital ecosystems.

IAAS (Infrastructure as a service)

In the case of the IAAS the consumer is provided with an interface that restricts the user to only process, store and make its order with other fundamental computing resources. The user is not granted access to cloud infrastructure but has control over its operating system [36], mostly limiting control over selected network systems, mainly the firewalls.

SAAS (Software as a service)

The platform offers the user access to the provider application, which runs on the internet mostly on cloud medium. The application can reach different client devices through a specific interface. Users do not manage or control most part of the interface including the network, servers, operating systems, storage, or even most parts of the applications themselves aside from a few limited configuration channeled to their need e.g., tracelink Software as a service SAAS as a cloud-based model where, designers structure application and is responsible to deliver timely updates [37]. The interface itself (SAAS) handles a wide range of features including user interface delivery, security, identity management, single sign -on (SSO), role-based access control (R-BAC), authorization and authentication, regulatory compliance, cost efficiency, and flexibility. Behind the scenes shared and virtualized servers, networks and storage systems create a resource pool designed to be accessed easily over the public internet [38].

PAAS (Platform as a service)

As in the case of PAAS, the customer does not manage or control the underlying cloud infrastructure or the application features. The customer can; however, configure user-specific application parameters and settings [39]. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. (e.g., SAP platforms) Online Pharmacy Architecture [40].

Organogram of a Traditional E-pharmacy

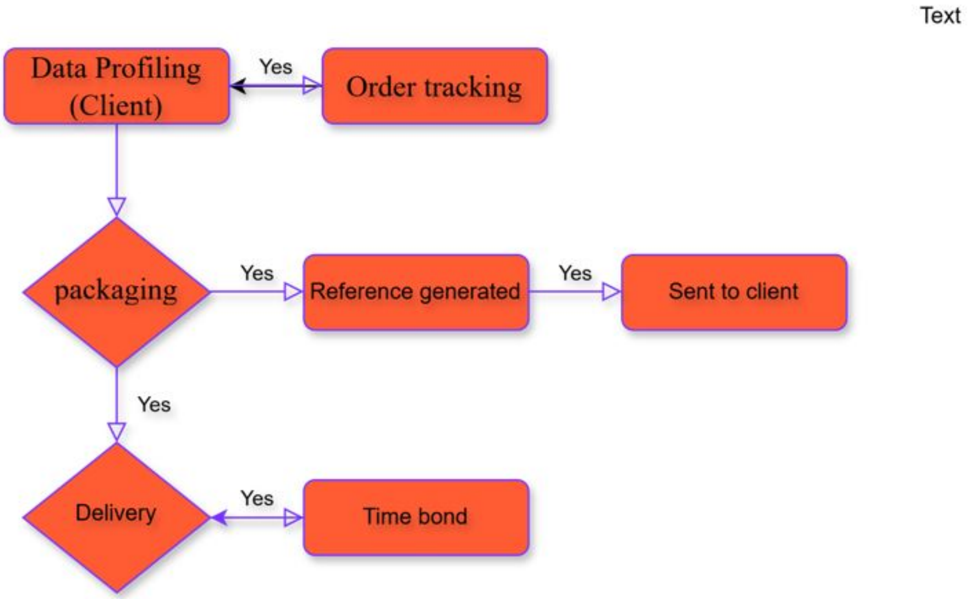

Figure 3: Existing workflow of pharmaceutical services [41]

The above figure illustrates an existing process of online pharmaceutical services that encompasses profiling of the client's necessary information to ease delivery, a generated order number to ease tracking from a host of orders placed within the said period: the order is handed over to a separate delivery service which further executes the handover. Though these processes are of good quality, it left tangible loopholes to data theft among other data related infringements. Data is shared between the cloud host, pharmaceutical setup and delivery service thus arises a great need for geo fencing of such data with highly encrypted characters that promises a strengthened security.

Drug Dispensation and Home Delivery Service

The drift in actions of patients towards adopting remote pharmaceutical services as well as home-abled prescription filling have become more a common practice thanks to the experience of the last pandemic which aided the upscaling and wild utilization of such services with a sole aim of foiling both disease burden and transmission while satisfying patients' demand [42]. However, a host of patients are not familiar to these services, and it's adaptability has been analyzed to be lower in low- and middle-income countries therefore consequently limiting the implementation of these remote patient care services.[43] The work of [44], a Chinese express service showcases how an alarm system connected to the SYSUCC drug distribution system is activated as soon as an online prescription is created using the Cloud SYSUCC app. Then, using an automatically created delivery service tracking number, the frontline pharmacists can print the drug dispensing orders. Before being sent to SF Express, which offers a prompt, economical, and careful Mainland China Express Service to guarantee safe and effective delivery, all medication orders are thoroughly examined. Using the tracking details of their medication orders placed through the Cloud SYSUCC app, patients can see real-time updates. Before distributing the parcels, SF Express delivery professionals confirm the patients' identities to guarantee that the medications are given to them accurately. Patients can easily ask for a refund of the expedited order fees if package delivery takes longer than three days [45. Orders made within a city are delivered within a very short period of time as the client is eligible for a refund when not delivered within a stipulated time, for each delivery, a feedback is generated to confirm a "delivery status" on all ends.

General Data Protection Regulation (GDPR)

In order to guarantee that non-expert users can make knowledgeable decisions regarding their privacy and provide informed consent for the use, sharing, and repurposing of their personal data, the General Data Protection Regulation (GDPR) was introduced thus curbing unauthorized cyber draining of legitimate information for different purposes ranging from competitive favoritism to exploitative criminal acts [36]. Through a distributed, consensus-based method, blockchain technology has also been used in cloud environments to improve user privacy and offer an audit trail of providers. The most relevant act of blockchain technology has been its ability to safeguard information and to foster better cooperation between the service provider and the users [37]. Blockchain-based solutions can be used by cloud applications to provide users control over their data and to let them know what kinds of data processing providers have done, also in a more easy way it provides a better environment for the user and provides a more friendly interface for processing for the user [38]. Accountability and provenance monitoring of activities performed on user data are made possible by the combination of GDPR and blockchain technology to actually get the origin of the data provided, most parts of the system will rely on the integration of General data protection regulation and blockchain technology as explained above [39]. This method improves the transparency of the use and processing of personal data by utilizing auditable smart contracts that are implemented in a blockchain. A conceptual design that leverages both GDPR and Blockchain was put up for a privacy-conscious cloud economy, thus in the quest to still provide a good environment for innovation and economic growth and still put user privacy and data security with high regards GDPR and blockchain tend to provide a more user-friendly environment. [40].

Security and Privacy Threats of Cloud-Based Management Information System

The cloud computing space is encircled by different security ranging from data leakage, unauthorized access, and ransomware threats that have ravaged a seamless process for decades. As ascertained from the Verizon Data Breach Investigations Report 2021, it was established that approximately 81% of hacking attacks that led to breaches took advantage of loopholes that granted access to stolen or poor passwords [24]. Also, there are privacy concerns since associated data may not be optimally encrypted or meet different privacy laws across continents therefore complicating the use of cloud services [25] Personal data including the likes of a users' names, contact information, and social security numbers engineers a loose structure that sinks in compromise thus aiding cases of identity theft and fraud [26]. Other sensitive details like names, addresses, and identification documents including the likes of credit card data and transaction records are also loosened due to structural loopholes thus inviting the attention of cyber criminals [24]. The most common risk is data seepage eschewed by third parties granted access on the ground of providing cloud host services. Various economic measures are targeted towards containing data breaches as evident in the 2023 report of the IBM security wing, such costs are even higher in medical data as leaked data can spore stigmatization amongst others [55]. Among a series of privacy issues is ownership of data as the user gives up control of their information after each entry. A survey conducted noted that 64 percent of the firms ‘have little idea about the legal requirements for the subject of ownership of the data to be housed in the cloud and it carries risks [56]. Consequently, paradigmatically the users may end up giving CSPs permission to process user data in a way other than what the user intended, as such permissions pop up before each entry [56].

Despite the numerous advantages offered by cloud computing—including scalability, flexibility, and cost-efficiency—organizations face several limitations and challenges when adopting cloud technologies [29]. One of the foremost concerns is regulatory compliance variances. Different regions and industries have distinct compliance requirements, such as HIPAA in the U.S. for healthcare and GDPR in the European Union for data protection. Navigating these overlapping and sometimes conflicting regulations becomes a significant hurdle, especially for multinational organizations seeking to maintain compliance across jurisdictions [30]. Closely tied to compliance is the issue of data sovereignty, which refers to the legal and policy frameworks that govern where data is stored and processed. Countries often require that sensitive data remains within their borders, limiting the ability to use global cloud infrastructure freely. This can lead to operational inefficiencies and force organizations to maintain multiple data centers or work with local cloud providers, increasing complexity and cost [31].

Interoperability issues also present a major barrier to seamless cloud adoption. Many organizations rely on hybrid or multi--cloud environments, using services from various providers. However, proprietary systems, incompatible APIs, and differing data formats can hinder integration and portability between platforms [32]. This lack of standardization may result in vendor lock-in and reduced flexibility in future technological decisions.

Lastly, cost remains a significant concern. While cloud computing can reduce capital expenditure, unpredictable pricing models—especially concerning data egress fees, storage, and long-term usage—can result in higher-than-expected operational costs. Smaller organizations in particular may struggle to optimize spending without sophisticated cost-management tools [34]. In summary, while cloud technology holds transformative potential, organizations must navigate a complex landscape of compliance, sovereignty, interoperability, and cost challenges to realize its full benefits effectively [35].

Table 1: Summary of different cloud deployment models, their key characteristics, security measures, and associated technological architectures

Deployment Model	Description	Security Measures	Technological Architectures
Public Cloud	Services offered over the internet by third party	Data encryption, multi-tenancy isolation	Virtualisation, multi-tenant architecture
Private Cloud	Dedicated infrastructure for a single organisation	Firewalls, access controls, Internal compliance	Virtualisation, hyper-converged infra
Hybrid Cloud	Combination of public and private clouds	Secure APIs, secure segmentation	Cloud orchestration, API gateways, SD-WAN
Community Cloud	Shared infrastructure between multiple organisations	Policy-driven access, compliance monitoring	Federated identity, shared infra platform
Multi-cloud	Use of multiple public cloud services from	Unified security policy	Containerisation, microservices, CI/CD pipeline

Adapted and modified from [33].

Compliance with Internal and External Auditing

All change logs in the business system must contain electronic signatures in accordance with US rule 21 CFR Part 11. Internal and external audits must have access to all transactions and events that have an impact on drug serialization. A basic audit consists of examining a company's financial records, physical inventory, and books. Because tax revenue, government compliance, and the organization's reputation are all on the line, it is imperative that everything be double checked [41]. An internal audit can be carried out by any employee of the company who is knowledgeable about fundamental financial principles, such as preparing financial statements, bookkeeping, and evaluating internal business operations. To ensure that the company's financial figures add up, that records are kept accurately, that processes are in order, and that financial controls are functioning as intended are just a few of the reasons why internal audits are carried out. The Institute of Internal Auditors' corporate governance model lists an efficient internal audit as one of the four elements of corporate governance. Since auditing is rapidly impacted by information technology improvements in all their forms, the ERP system should be viewed as a significant element influencing internal audit performance [42]. In order to ensure that the numbers in the company's financial statements, which are prepared by accountants, are not materially misled, auditors do internal audits in cases where this audit is not done the assessment obtained from the financial statement are most likely to be in discrepancy. [43] clarified that the deployment of ERP systems has been the most important IT project impacting the accounting department during the previous 15 years.

Challenges in Cloud-based Medical Development

The following are some of the primary issues and concerns with cloud-based medical development that the pharmaceutical business certainly faces. The theoretical analysis of customer desires needs to be improved. The development of business applications, including cloud-based medical construction, requires careful preparation. Both financial and technological resources must be increased. It is concerning because there is a serious lack of funding, skill, technology, and other resources. Documents may be kept safer and longer because cloud computing provides better data protection. Digital transformation is changing company practices in many situations, creating entirely new industry categories in the modern world. As a result of the digital revolution, pharmaceutical companies are stepping back and examining every aspect of their operations, including internal procedures and online and in-person client contacts. Drugs that have been purposely manufactured fraudulently or with false labels on their identity or source to pass for genuine ones are considered counterfeit [44, 45]. The technique of tracking and tracing pharmaceutical drugs in the supply chain to stop counterfeiting is not new. Other nations, like South Korea and China, already have drug traceability compliance in their laws, while Turkey approved serialization regulations in 2010 in addition to markets like China and South Korea. The importance of drug tracking is now being emphasized and even mandated in many countries worldwide. The Drug Supply Chain Security Act (DSCSA), a US regulatory body, has established procedures to accomplish interoperable, electronic tracing of medications at the package level in order to identify and monitor certain prescription medications as they are distributed in the US [46].

Existing Approaches Introduced to Ensure Data Security in Cloud Computing

After a thorough review by [11], the following are published existing approaches tailored towards a guaranteed data security in cloud: (a) Encryption, where the plain text is converted into cipher text by using some encryption algorithms; (b) Homomorphic token: A technique ensures that we do not need to decrypt the key for data checking instead we can directly compare with encrypted token; (c) Guidelines: Some of the studies have outlined some guidelines to ensure the data security in the cloud (d) Harmonizing scheme: Building a data repository (e) data concealment component; (f) token; (g) Framework; (h) stripping algorithm.

Table 2: Advantages and disadvantages of existing approaches for cloud data security

Approach	Advantages	Disadvantages	Practical Applications
Encryption	Strong confidentiality, compliance support	Key management, performance overhead	Cloud storage, TLS, DB encryption
Homomorphic token	Computation on encrypted data	High processing cost	Privacy-preserving cloud analytics
Guidelines	Policy-based control, easy to roll out	Not technical, dependent on human compliance	SLAs, ISO protocols
Harmonizing scheme	Cross-cloud interoperability	Vendor resistance, complexity	Multi-cloud security models
Data concealment	Prevents exposure during sharing	Loss of data precision	Data masking in health/finance
Token	Format-preserving protection	Requires secure vault	Credit card tokenization
Framework	Holistic, modular security	Complexity, maintenance	NIST/CSA frameworks

Stripping algorithm	Reduces risk through dispersion	Latency, fragmentation overhead	Distributed storage/security layers

Innovative Approach Utilization in Cloud Computing

The Internet of Things is a device capable of transmitting, receiving and further storing data on cloud once connected to an internet. The Internet of Things is incorporated with several devices such as sensors, physical devices, and software to control the devices. IoT devices include anything that contains a Unique Identification Number (UID) that can be used to identify uniquely over the internet (*20)* Organizations may focus on integrating standard procedures and lessons gained into practice by using IoT sensors to replace the time-consuming trial-and-error approach. In order to better understand the context of their activities, pharmaceutical IoT producers need access to sensors [47]. The pharmaceutical industry's IoT-enabled sensors send all facility data back to a centralized dashboard, allowing employees to keep an eye on super performance and make any necessary maintenance adjustments. A single digital dashboard can be used in the pharmaceutical industry to capture data related to vacuum pumps, heat exchangers, and air compressors [48]. The pharmaceutical industry has been transformed by the Internet of Things. The Internet of Things has opened up new possibilities for increased productivity and efficiency in pharmaceutical production processes by facilitating smooth equipment connections across assembly lines. In an attempt to optimize data security, [21] developed an Auditable Privacy-Preserving Federated Learning (AP2FL) model tailored for electronics in healthcare. AP2FL model provides secure training and aggregation processes on the server side as well as the client side thus building trust at both ends while protecting and minimizing the risk of data leakage. Researchers primarily focus on Machine learning-based threat detection models to address the challenges within Consumer IoT. [22] suggests use of deep learning algorithms to identify and further counter attack false data injection (FDI) assaults through automatic extraction of data and real time monitoring, this is important as artificial intelligence is coded to be at alert all seconds.

Innovative Approaches to Employing Azure Cloud in Pharma Sectors

Businesses may sample, reproduce, test, and alter tests in different settings thanks to cloud features that enable real-time data capture. Businesses may more readily modify shop-floor infrastructures that support IIoT in the cloud with the aid of these cloud services. These services enabled cloud workloads to run on IoT edge devices by helping manufacturers increase operational dependability and accelerate response times to local changes. Additionally, manufacturers can use this cloud technology to decide which data is stored on-premises and which is aggregated onto the Cloud utilizing Azure. Consequently, manufacturers can continue to use their current cloud infrastructure while utilizing incremental validation. Azure services can be used by the pharmaceutical industry to address a significant problem that has been impeding progress for years: the incapacity to preserve data and provide continuous connection across production lines. By incorporating cloud-based insights that align with business requirements, the pharmaceutical sector is witnessing a revitalization of its digital infrastructure, operational efficacy, and return on investment [49]. Transit chain custody problems might be resolved by the IIoT. IoT-enabled devices are used by pharmaceutical organizations to track drug shipments. Batch monitoring in logistics may be enhanced by smart labeling and radio frequency identification technologies. Vehicles were able to improve cargo visibility thanks to these contemporary monitoring technologies and the Global Positioning System [50]. Connected devices assist pharmaceutical businesses track expenses and maintain tight quality standards by improving production speed, inventory control, and quality assurance. Monitoring the sources of supplies is crucial for maintaining manufacturing quality and speed. Another advantage of IIoT is that it keeps pharmaceutical companies organized. When customer supplies are low, the use of IoT sensors alerts businesses to restock. In order to prevent a shortage, firms consequently lessen their need for extra supplies. Data informs stocking decisions by identifying batches that have expired. By identifying containers in a supply chain, IoT location devices enable pharmaceutical companies to recall batches in a timely and comprehensive manner. Additionally, pharmaceutical companies may be able to find cost overruns and inefficient areas of their operations with the aid of data analytics from IoT-connected equipment. Pharma companies require IoT and IIoT to meet quality standards, digitize processes, and remove errors in order to provide drugs and medical equipment in a way that complies with regulations.

Challenges of Cloud Adoption in Online Pharmacies

Cloud computing offers scalability, flexibility, and innovation opportunities, but its adoption is still hindered by significant challenges. Organizations must conduct thorough risk assessments, establish robust governance, and partner with transparent and compliant providers to navigate these challenges effectively [51]. The current limitations of cloud adoption in online pharmacies is discussed under the following headings: regulatory compliance variances, data sovereignty concerns, interoperability issues, and costs:

i. Regulatory Compliance Variances: Different countries and industries impose distinct regulatory standards that cloud providers and users must comply with. These regulations cover data protection, privacy, financial reporting, and healthcare standards (e.g., GDPR in the EU, HIPAA in the US, NDPR in Nigeria) [52].

Challenges:

(a)Lack of uniformity: A cloud service provider operating globally must navigate diverse and sometimes conflicting compliance requirements. For instance, GDPR mandates strict data privacy rules that may conflict with laws in other jurisdictions.

(b)Constantly evolving laws: Regulatory frameworks evolve rapidly. Cloud adopters must continuously monitor and update their compliance practices to avoid penalties.

(c)Limited transparency: Cloud providers may not disclose enough about how they manage compliance internally, leaving clients uncertain about their own legal exposure.

(d)Audit difficulties: Enterprises face challenges in auditing cloud environments to ensure compliance, especially in multi-tenant or hybrid setups.

ii. Data Sovereignty Concerns: Data sovereignty refers to the concept that data is subject to the laws of the country where it is physically stored. In cloud computing, where data is often stored across multiple geographic regions, this becomes a critical issue [53].

Challenges:

(a)Jurisdictional conflicts: When data is stored or processed in foreign countries, it may be subject to foreign surveillance laws or legal requests, which might violate the originating country's laws.

(b)Customer mistrust: Government agencies and enterprises in highly regulated sectors (e.g., finance, defense) often hesitate to adopt cloud due to the risks of foreign access to sensitive data.

(c)Limited control over data location: Some cloud providers do not offer fine-grained control over where data resides, making it difficult for customers to ensure compliance with local sovereignty laws.

Cross-border data transfer restrictions: Laws like GDPR place strict limitations on transferring personal data outside the EU unless appropriate safeguards are in place

iii. Interoperability Issues: Interoperability refers to the ability of different systems, services, or applications to work together seamlessly. In cloud environments, lack of standardization creates significant integration challenges [54].

Challenges:

(a)Vendor lock-in: Once an organization builds its infrastructure on a particular cloud provider's proprietary tools and APIs, it becomes difficult and costly to migrate to another provider.

(b)Lack of standard APIs: Different cloud providers use different interfaces, making it hard to integrate services or switch providers without major redevelopment.

(c)Difficulty in hybrid cloud management: Managing applications and data across a hybrid cloud (on-premises + cloud) or multi-cloud setup can be technically complex due to differing platforms, protocols, and security models.

(d)Application compatibility: Legacy systems often require significant reconfiguration or even full refactoring to function in the cloud, complicating the migration process.

iv. Costs: While cloud computing is often seen as cost-efficient, organizations may face hidden and escalating costs, especially as their use of cloud services grows [55].

Challenges:

(a)Unpredictable pricing models: Pay-as-you-go models can lead to unexpected spikes in costs if usage is not carefully monitored and optimized.

(b)Data egress fees: Transferring data out of the cloud (e.g., to another cloud or on-premise) often incurs substantial fees, which are not always clear upfront.

(c)Long-term expenses: Although initial capital costs are reduced, operational costs may exceed traditional IT budgets over time, especially for high-performance computing or data-intensive applications.

(d)Over-provisioning and underutilization: Without proper management, resources are often over-provisioned, leading to waste and inflated bills.

(e)Skill gaps: The cost of hiring or training skilled personnel to manage complex cloud environments can also be substantial.

Table 3: Summary of cloud deployment models, associated security measures, and technological architectures specifically tailored for online pharmacies

Cloud Deployment Model	Security Measures	Technological Architecture	Use Case in Online Pharmacies
Public cloud	- Data encryption (at rest/in transit) - Identity & Access Management (IAM) - Multi-factor authentication (MFA)	- Shared infrastructure - Hosted by third-party providers (e.g., AWS, Azure)	- Hosting non-sensitive operations - E-commerce interfaces and general information portals
Private cloud	- Intrusion Detection/Prevention Systems (IDS/IPS) - Dedicated firewalls - Role-based access controls	- On-premises or vendor-managed - Single-tenant architecture	- Integrating legacy health systems with modern e-commerce platforms

Hybrid cloud	- Data segregation policies - API security gateways - Secure VPNs	- Combination of public + private clouds - Integrated through orchestration layers	- Integrating legacy health systems with modern e-commerce platforms
Community cloud	- Compliance-based access control (HIPAA/GDPR) - Federated identity management	- Shared infrastructure among similar organizations (e.g., healthcare providers, pharmacies)	- Collaborative drug safety reporting - Shared research platforms and health data networks
Multi cloud	- Centralized security policies - Cloud Access Security Broker (CASB) - Continuous monitoring	- Multiple public/private clouds from different vendors - Load balancing and failover mechanisms	- Ensuring system uptime - Diversifying data storage for high availability & disaster recovery

Robust and Improved Online Pharmacy Architecture

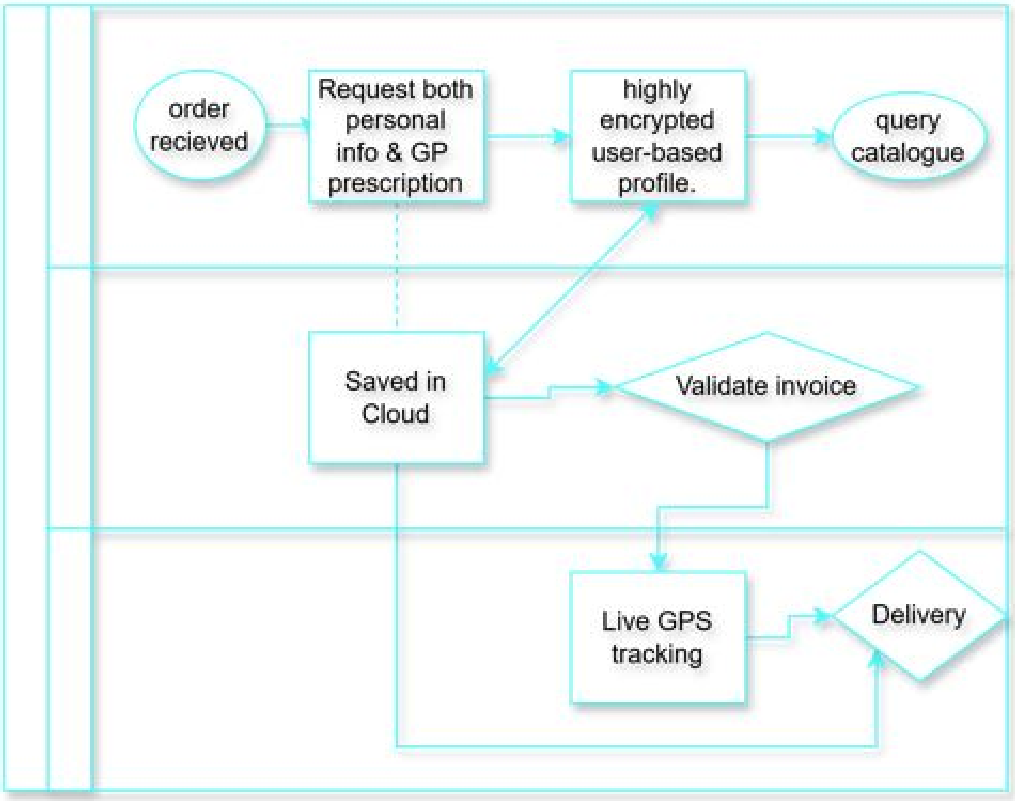

Figure 4: Improved workflow for an E-pharmacy [50]

Figure 4 shows an improved workflow diagram for an e-pharmacy which illustrates a streamlined process that enhances efficiency, data security, and customer satisfaction. It begins with user registration and authentication, followed by prescription upload and verification by licensed pharmacists. Once validated, medicines are checked for availability through an integrated inventory system. Payment is processed via secure gateways, triggering automated order fulfillment and real-time tracking. Pharmacists offer virtual consultations as needed, and delivery is handled through logistic partners with status updates. Post-delivery, patients can access medication reminders and provide feedback. The system ensures compliance with regulations and maintains patient confidentiality through encrypted cloud storage solutions.

The unique strengths of each existing solution enhanced into a more adaptive, intelligent and trust-minimized frame. A generic trust model is avoided as each entry is authenticated, validated and encrypted as the IP address and other digital information including face verification, biometrics and OTP are confirmed alongside. As the world drifts towards artificial intelligence, we must integrate a monitoring software that detects anomalous activities while keeping such software in check for leaks of private information. Data should be tagged and classified as very important data, for instance data such as related to finance should be "Geo-fenced" with a stronger encryption algorithm. The supply chain of pharmaceutical products requires a robust modus of operation as depicted above, all orders are to be screened by a central database which subsequently sends a signal to the selected stores for both packaging and delivery, the incorporation of both fingerprints and face detection section enhances confidence and also secure data through an individual based cloud blinded to an oversight through geo fencing as these information are stored and matched with subsequent query inputs. Invoices are generated and shared with a client while records of such actions are well documented in the individual's cloud. Pharmaceutical products are tracked in real time via a global positioning system as seals are used to blind delivery personnel from a client's data.

Case Study on Robust and Improved Online Pharmacy Architecture for MedSureRx

MedSureRx, a mid-sized pharmaceutical retail company based in Lagos, Nigeria, faced numerous challenges with its legacy online pharmacy system. These included frequent downtimes, security breaches, poor scalability, and inefficient data management [42]. With an increasing customer base and growing demand for telehealth services, the company needed a more secure, scalable, and efficient digital infrastructure to handle orders, prescriptions, inventory, and sensitive patient data. The previous architecture used a monolithic on-premises system that lacked interoperability and elasticity. There were no real-time inventory updates, and customer data was stored in unencrypted formats [38]. Regulatory compliance with data protection laws such as NDPR (Nigeria Data Protection Regulation) and international standards like HIPAA and GDPR was also lacking, posing legal and reputational risks.

MedSureRx adopted a robust, cloud-native microservices-based architecture built on Amazon Web Services (AWS). Each function—such as user authentication, inventory management, prescription validation, order tracking, and customer support—was separated into independent microservices [39]. A combination of secure APIs and token-based authentication ensured seamless communication between services. Data was encrypted at rest and in transit using AES-256 encryption and TLS protocols, respectively. The system integrated AI-powered prescription analysis tools to validate uploaded doctor prescriptions and detect potential drug interactions. Real-time inventory sync and automated restocking alerts were enabled via IoT sensors in warehouse facilities [40]. The platform also featured a patient health portal allowing access to e-prescriptions, order history, and teleconsultation services.

The new architecture led to a 99.98% uptime, a 60% reduction in page load time, and a 75% increase in customer retention within six months [43-45]. Cybersecurity audits confirmed compliance with local and international data privacy regulations. Scalability was drastically improved, allowing the system to handle 5x more users during peak periods. MedSureRx's transition to a modern, secure, and modular online pharmacy architecture not only enhanced operational efficiency but also built trust with patients and healthcare providers. This case underscores the critical importance of integrating cloud technology, security best practices, and intelligent automation in designing resilient online healthcare platforms [43].

The Global Impact of Online Pharmacy Platforms

Technology breakthroughs and the global COVID-19 pandemic have caused a dramatic shift in pharmacy practice and education in recent years. A shift in customer behavior toward online pharmacies is revealed by a study that highlights the growing consumer trust in online pharmaceutical purchases before, during, and after the pandemic [51]. A good response and increasing confidence in digital healthcare solutions are indicated by this trend, which highlights a rising reliance on these platforms where the perceived benefits greatly exceed the perceived risks. One example of this change is the use of telehealth, which includes telepharmacy. With healthcare providers increasing their telemedicine visits, patient use of telehealth services in the US increased from 11% in 2019 to 46% [53]. This change reflects the healthcare industry's increased customer acceptance and adaptability to digital platforms. Additionally, the epidemic has acted as a catalyst, speeding up the development and global use of online telepharmacy services. New platforms have had to be added in order to supplement well-known sources of health information due to the "new normal." An illustration of this is the development and assessment of an online telepharmacy service in the Philippines during the pandemic, which shows how swiftly the global pharmacy business embraced digital alternatives. These services are not just supplemental; they are crucial for supplying and clarifying pharmaceutical information in the framework of primary healthcare delivery [54]. In line with a shift towards customer-centric, digital-first services, pharmacist-led businesses like MedEssist and MedMehave simultaneously developed digital platforms to enable services like COVID-19 testing and flu vaccines [55]. Although this shift makes treatment more convenient and accessible, it also presents serious regulatory obstacles. Navigating these obstacles is essential for preserving patient safety, quality standards, and creating a reliable online healthcare environment as the rise of online medication sales upends traditional pharmacy markets [55].

Table 4: Comparative Literature Review on Cloud Technology for Online Pharmacies

Author(s) Year	Study Title	Objectives	Methodology	Key Findings	Contribution to Topic
Smith et al. [57]	*Cloud-Based E-Prescription Systems in Online Pharmacies*	To evaluate the performance and security of cloud-enabled e-prescriptions	Case study analysis of 5 online pharmacies	Improved accessibility and reduced data redundancy; issues with cloud vendor lock-in	Highlights efficiency gains and risks related to data portability
Gupta & Sharma [58]	*Security Challenges in Cloud Computing for E-Health*	To analyze specific threats and mitigation techniques in cloud healthcare	Literature synthesis and threat modeling	Encryption and role-based access control are most effective	Emphasizes need for tailored security protocols in pharmacy platforms
Li et al. [59]	*Cloud Integration in Pharmacy Logistics Management*	To assess how cloud impacts inventory and supply chain	Simulation of logistics models with and without cloud	Real-time data sync reduced medication shortages by 35%	Demonstrates efficiency improvements through cloud in supply chain management
Okoro & Adeyemi [60]	*Cloud Adoption in Nigerian Online Pharmacies: A Mixed Methods Study*	To investigate barriers to cloud adoption in low-resource settings	Surveys and interviews with 20 pharmacy operators	Cost and lack of digital infrastructure major barriers; security concerns prevalent	Provides local context and realistic challenges to cloud deployment
Zhang & Chen [61]	*Blockchain and Cloud for Securing Patient Records in Pharmacies*	To evaluate hybrid cloud-blockchain models for data security	Design and testing of a prototype system	Hybrid model reduced unauthorized access incidents by 60%	Proposes a novel approach to combine cloud and blockchain for better security

Alshamrani et al. [62]	*HIPAA and GDPR Compliance in Cloud E-Pharmacy Systems*	To examine regulatory frameworks applied in cloud-based pharmacies	Policy analysis and case law review	Many cloud systems fail full compliance; need for vendor transparency	Reinforces importance of legal and ethical compliance in security planning

Limitations

While this is an extensive review, it is subject to several limitations. Firstly, inclusion was restricted to studies that had been published in the English language, and this may have excluded other languages' evidence. Secondly, as a systematic review, its findings are dependent on the quality and quantity of accessible primary literature; the review itself does not include original empirical data. Besides, the rapidly evolving characteristics of cloud technologies and cyber-threats will render some of the specific technical solutions taken into account outdated, therefore requiring ongoing research within the area. Finally, the focus on technological and legislative aspects may not be capable of expressing all the operational and human-element problems online drugstores encounter in different socio-economic situations.

Conclusion

This research solves a very important problem within the space of the globally adopted E-pharmacies therefore guaranteeing data security including robust and enhanced efficient operational technicalities necessary for existing loopholes domiciled within the cloud-based system. This research bridges the gap between the positives of cloud computing and a tight need for pharmaceutical data management through a systematically viable approach. It elaborates on a need for an enhanced encryption, transparent blockchain and an all-encompassing data associated governance as they promise a better ground for both security and trust during and after patronage. Furthermore, the integration of emerging technologies such as IoT, artificial intelligence and real-time monitoring into the cloud domain tenders potential drivers of integrity as regards supply chain, safety as well as global standards. Importantly, this research stands in the gap for the adoption of an approach that integrates stakeholders in an attempt to holistically mop the inadequacies leading to systemic risks. In the years to come, the use of cloud technology by e-pharmacies will be the global standard, driven by advances in AI-driven predictive security, quantum-resistant cryptography, and blockchain-enabled decentralized identity frameworks. The future for e-pharmacies lies not just in cloud uptake, but in creating smart, self-healing cloud ecosystems that can predict, identify, and eliminate threats autonomously while delivering frictionless, personalized care to patients. Future research must empirically test these proposed architectures and examine the socio-technical elements of end-user trust and adoption in diverse global settings.

Authors’ Contributions

FO: Conceptualization, Writing–original draft, Writing–review and editing. BS: Writing–original draft, Writing–review and editing. KK: Writing–original draft, Writing–review and editing.

Acknowledgements

We sincerely acknowledge all authors for their contributions that make this work a success.

Funding

No special funding was received from any institute or organization for this research work.

Conflicts of Interest

The authors declare no conflict of interest regarding the publishing of this paper.

Data and Materials Availability Statement

The raw materials supporting the conclusions of this article will be made available by the authors, without undue reservation.

References

1. Chandra DG, Borah MD (2012) Cost benefit analysis of cloud computing in education. In International Conference on Computing, Communication and Applications, 1–6.

2. Orizio G, Merla A, Schulz PJ, Gelatti U (2011) Quality of online pharmacies and websites selling prescription drugs: a systematic review. J Med Internet Res 13:e74.

3. Long CS, Kumaran H, Goh KW, Bakrin FS, Ming LC, Rehman IU, et al. (2022) Online pharmacies selling prescription drugs: systematic review. Pharmacy 10:42.

4. Fittler A, Fittler M, Vida RG (2023) Stakeholders of the online pharmaceutical market. Biomed Eng (NY).

5. Lobuteva L, Lobuteva A, Zakharova O, Kartashova O, Kocheva N (2022) The modern Russian pharmaceutical market: consumer attitudes towards distance retailing of medicines. BMC Health Serv Res 22:582.

6. Mackey TK, Nayyar G (2016) Digital danger: a review of the global public health, patient safety and cybersecurity threats posed by illicit online pharmacies. Br Med Bull 118:110–126.

7. Ashraf AR, Mackey TK, Schmidt J, Kulcsár G, Vida RG, Li J (2024) Safety and risk assessment of no-prescription online semaglutide purchases. JAMA Netw Open 7:e2428280.

8. Ozawa S, Billings J, Sun Y, Yu S, Penley B (2022) COVID-19 treatments sold online without prescription requirements in the United States: cross-sectional study evaluating availability, safety and marketing of medications. J Med Internet Res 24:e27704.

9. Xing Q, Blaisten E (2018) A cloud computing system in Windows Azure platform for data analysis of crystalline materials. Concurrency Comput Pract Exper 25:2157–2169.

10. Fittler A, Fittler M, Vida RG (2023) Stakeholders of the online pharmaceutical market. Biomed Eng (NY).

11. Architha Aithal, Shabaraya AR (2018) Users perspectives on online pharmacy model. Int J Health Sci Pharm (IJHSP) 2(1):29–36.

12. Mash RJ, Schouw D, Daviaud E, Besada D, Roman D (2022) Evaluating the implementation of home delivery of medication by community health workers during the COVID-19 pandemic in Cape Town, South Africa: a convergent mixed methods

study. BMC Health Serv Res 22(1):98.

13. Brey Z, Mash R, Goliath C, Roman D (2020) Home delivery of medication during coronavirus disease, Cape Town, South Africa. Afr J Prim Health Care Fam Med 12(1):1–4.

14. Lohar N, Mhatre P, Lad A, Gaikwad A, Kulkarni S (2016) Data security in cloud computing. IOSR J Comput Eng (IOSR-JCE) 18(2):125–128.

15. Soofi A, Khan M, Amin F (2024) A review on data security in cloud computing. Int J Comput Appl 94.

16. Abu-Farha R, Alzoubi KH, Rizik M, Karout S, Itani R, Mukattash T, Alefishat E (2022) Public perceptions about home delivery of medication service and factors associated with the utilization of this service. Patient Prefer Adherence 16:2259–2269.

17. Navimipour NJ, Zareie B (2015) A model for assessing the impact of e-learning systems on employees' satisfaction. Comput Human Behav 53:475–485.

18. Kanaan R, Abumatar G, Mohammed A, Abu Hussein A (2019) Cloud-based management information system: a systematic review and future research scope. Mediterr J Soc Sci 8:509–525.

19. Armbrust M, Fox A, Griffith R, et al. (2010) A view of cloud computing. Commun ACM 53(4):50–58.

20. Pathak M, Mishra K, Singh SP (2024) Securing data and preserving privacy in cloud IoT-based technologies: an analysis of assessing threats and developing effective safeguards. Artif Intell Rev 57:269.

21. Yazdinejad A, Dehghantanha A, Srivastava G, Karimipour H, Parizi RM (2024) Hybrid privacy-preserving federated learning against irregular users in next-generation Internet of Things. J Syst Architect 148:103088.

22. Sakhnini J, et al. (2023) A generalizable deep neural network method for detecting attacks in industrial cyberphysical systems. IEEE Syst J 17(4):5152–5160.

23. Namakshenas D, Yazdinejad A, Dehghantanha A, Srivastava G (2024) Federated quantum-based privacy-preserving threat detection model for consumer Internet of Things. IEEE Trans Consum Electron.

24. Widup S, Pinto A, Hylender D, Bassett G, Langlois P (2021) Verizon data breach investigations report.

25. Fadele A, Othman M, Hahsem I, Alotaibi F (2017) Internet of Things security: a survey. J Netw Comput Appl 88:10–28.

26. Johnson R, Lee T (2022) Cybersecurity and privacy in cloud-based systems: a systematic review. Comput Secur 103591.

27. Hammour KA, Abdeljalil M, Manaseer Q, Al-Manaseer B (2022) Jordanian experience: the internet pharmacy drug delivery platform during COVID-19. Health Policy Technol 11:100596.

28. Lorkowski J, Pokorski M (2022) Medical records: a historical narrative. Biomedicines 10:2594.

29. Osei-Tutu K, Song YT (2020) Enterprise architecture for healthcare information exchange (HIE) cloud migration. In Proc 14th Int Conf Ubiquitous Information Management and Communication (IMCOM), Taichung, Taiwan, 1–8.

30. Ethereum (2020) Ethereum official website.

31. Virvou M, Mougiakou E (2017) Based on GDPR privacy in UML: case of e-learning program. In Proc 8th Int Conf Information, Intelligence, Systems & Applications, Larnaca, Cyprus.

32. Barati M, Aujla GS, Llanos JT, Duodu KA, Rana O, Carr M, Ranjan R (2021) Cloud security and privacy challenges in distributed systems.

33. dinCloud (2020) Cloud for pharmacy platform.

34. Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin MV, Calcavecchia F, Anderson D, Burleson W, Vogel JM, O'Leary C, Eshaya-Chauvin B, et al. (2020) Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. BMC Med Inform Decis Mak 20:146.

35. Chen ZJ (2021) Digital health and online medical platforms: a review. J Med Internet Res 23(1):e24619.

36. Russo B, Valle L, Bonzagni G, Locatello D, Pancaldi M, Tosi D (2018) Cloud computing and the new EU general data protection regulation. IEEE Cloud Comput 5(6):58–68.

37. Ulybyshev G, Villarreal-Vasquez M, Bhargava B, Mani G, Seaberg S, Conoval P, Pike R, Kobes J (2018) Blockhub: blockchain-based software development system for untrusted environments. In Proc 11th ICCC, San Francisco, CA, 582–585.

38. Zyskind G, Nathan O, Pentland AS (2015) Decentralizing privacy: using blockchain to protect personal data. In Proc IEEE Security and Privacy Workshop, CA, USA, 180–184.

39. Neisse R, Steri G, Nai-Fovino I (2017) A blockchain-based approach for data accountability and provenance tracking. In Proc 12th ICARSRCI.

40. Barati M, Rana O, Theodorakopoulos G, Burnap P (2019) Privacy-aware cloud ecosystems and GDPR compliance. In Proc 7th ICFITC, Istanbul, Turkey, 117–124.

41. Schenker J (2018) Overview of audit—audit and due diligence foundations.

42. Wang B, Li B, Li H (2023) Panda: public auditing for shared data with efficient user revocation in the cloud. IEEE Trans Serv Comput 8(1):92–106.

43. Tsipouridou M, Spathis C (2014) Audit opinion and earnings management: evidence from Greece. Int J Account Audit 38(1):38–54.

44. Xing Q, Blaisten E (2018) A cloud computing system in Windows Azure platform for data analysis of crystalline materials. Concurrency Comput Pract Exper 25:2157–2169.

45. Prasanth A, Sabeena G, Sowndarya, Pushpalatha N (2023) Artificial intelligence approach for energy-aware intrusion detection and secure routing in Internet of Things enabled wireless sensor networks. Concurrency Comput Pract Exper 1–21.

46. Prakash Y (2019) Demonetisation, digitalisation in India: towards a cashless economy. Int J Bus Continuity Risk Manag 9:333–337.

47. Wu C, Chiu R, Yeh H (2017) Implementation of a cloud-based electronic medical record exchange system in compliance with the integrating healthcare enterprise's cross-enterprise document sharing integration profile. Int J Med Inform 107:30–39.

48. Pratiksha P, Ranjeetsingh S, Suryawansh (2015) Microsoft Windows Azure: developing applications for highly available storage of cloud service. IJSR 4:662–665.

49. Rajalakshmi D, Tharunya R (2022) An improved faster and novel methodology for diabetes ulcer classification based on customized CNN. In 2nd ICAECT, Bhilai, India, IEEE Xplore, 1–6.

50. Sumathi M, Rajkamal M (2022) Decision trees to detect malware in a cloud computing environment. In ICESIC, Chennai, India, IEEE Xplore, 299–303.

51. Fittler A, Ambrus T, Serefko A, Smejkalová L, Kijewska A, Szopa A, Káplár M (2022) Attitudes and behaviors regarding online pharmacies in the aftermath of COVID-19.

52. Zhang PC (2022) The future of pharmacy is intertwined with digital health innovation. Can Pharm J 155:7–8.

53. Pandemic: at the tipping point towards the new normal (2022) Front Pharmacol 13:1070473.

54. Hiskey O (2022) The era of telehealth pharmacy practice. J Am Pharm Assoc 62:10–1.

55. Plantado ANR, de Guzman HJd, Mariano JEC, Salvan MRAR, Benosa CAC, Robles YR (2023) Development of an online telepharmacy service in the Philippines and analysis of its usage during the COVID-19 pandemic. J Pharm Pract 36:227–237.

56. Shawaqfeh MS, Al Bekairy AM, Al-Azayzih A, Alkatheri AA, Qandil AM, Obaidat AA, Harbi SA, Muflih SM (2020) Pharmacy students perceptions of their distance online learning experience during the COVID-19 pandemic: a cross-sectional survey study. J Med Educ Curric Dev 7:2382120520963039.

57. IBM Security (2023) Cost of a data breach report 2023.

58. WEEK (2010) Businesses unsure how to protect cloud data: survey.

59. Smith J, Patel A, Wong K (2020) Cloud-based e-prescription systems in online pharmacies: a case study approach. J Health Inform Technol 12(3):145–156.

60. Gupta M, Sharma R (2021) Security challenges in cloud computing for e-health applications. Int J Cybersec Health IT 8(2):99–112.

61. Li Y, Tan W, Zhou M (2019) Cloud integration in pharmacy logistics management: a simulation-based study. Comput Ind 106:1–12.

62. Okoro SM, Adeyemi TO (2022) Cloud adoption in Nigerian online pharmacies: a mixed methods study. Afr J Health Technol 14(1):25–38.

63. Zhang L, Chen Y (2023) Blockchain and cloud for securing patient records in pharmacies: a hybrid model approach. J Med Syst 47(2):38–50.

64. Alshamrani M, Khan I, Alotaibi B (2020) HIPAA and GDPR compliance in cloud e-pharmacy systems: an evaluation framework. Health Policy Technol 9(4):410–421.