Literature Review of Approaches in Cloud-based Management systems for Legal Firms

Ayushi Soumya, Bhumika Nayak, Deepthi Dayanand, Vaishnavi V B, and Professor Venkatesh Prasad

Department of Computer Science, PES University Bangalore, India

Abstract

This paper presents the development of a legal technology strategy that aims to address the challenges faced by law firms in responding to technology-driven changes in the corporate environment. The proposed strategy focuses on the creation of a Software-as-a-Service (SaaS) cloud model tailored to the needs of small-scale legal enterprise systems. This approach offers several key benefits, including scalability, modularity, lower cost, availability, reduced hardware costs, and enhanced security. To achieve these goals, we plan to leverage various cloud computing resources to support real-time collaboration, communication, and data management within legal firms.

The developed solution will incorporate automation capabilities for drafting, negotiation, and execution of contracts, legal documents, and templates. Furthermore, the system will provide efficient storage and retrieval functionalities for contract documents. By implementing this technology strategy, law firms can adapt to the changing landscape of the corporate environment and leverage technological advancements to streamline their operations. The proposed SaaS cloud model offers cost-effective solutions for small-scale legal enterprises, promoting accessibility and enhancing productivity. The research outcomes aim to contribute to the overall efficiency and effectiveness of legal practices in the era of technology-driven changes. We intend to leverage various cloud computing resources to support instantaneous collaboration, communication, and data management within legal firms. We plan on using Advanced encryption Standard (AES) algorithm and Amazon Quantum Ledger Database (QLDB) to provide confidentiality and security to Personal Identifiable Information (PII).

1. Main Project Modules

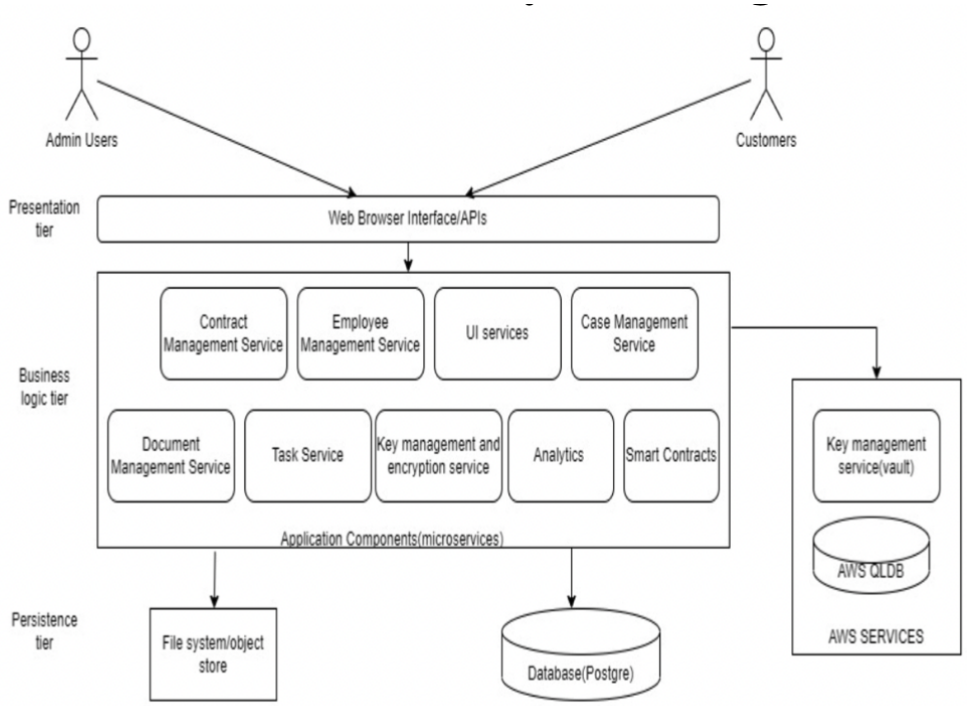

Fig. 1: Project Modules

1.1 Main features of the product

The main features of this project include microservices that any legal tech corporate company should encompass, security features for gaining user trust, and deploying all of it on the cloud platform as a Saas product for ease of maintenance and cost effective management are the features implemented within the scope of this project.

1.2. Implementation

The implementation is split into three tiers of production. The first tier is the persistence tier, which deals with storage. The data will be stored using file storage and the image of PostgreSQL pulled from Docker will also be used for storage. The second layer is the business logic layer which will contain administrative microservices for the platform under production. This will manage the data and also perform executive tasks that keep the application running consistently. This tier also deals with data security using encryption algorithms and key management services. The final layer is the presentation layer, where we will expose our application to users through APIs to a web browser interface.

1.3. AES encryption

AES (Advanced Encryption Standard) is an algorithm that uses a symmetric block cipher to protect classified information. We plan on using the AES algorithm to encrypt sensitive data on files and folders on disk storage. It is widely used for database encryption, and file and disk encryption. The AES algorithm is known for its security, cost efficiency and overall simplicity of execution given the benefits of implementation.

1.4. Amazon Quantum Ledger Database

Amazon QLDB is a centralized ledger database, with benefits that include transparency, immutability and a cryptographically verifiable log owned by a central trusted authority. We plan on connecting our application to a ledger and run CRUD (create, read, update, delete) transactions on the database.

A traditional database writes data to tables as part of a transaction, after which a transaction log records all the modifications made to the database. However, database transaction logs are not immutable. Amazon QLDB uses the concept of a journal to overcome this. The journal is structurally similar to a transaction log, with the exception being that it is an *'immutable, append-only'* data structure. The journal handles concurrency, sequencing, cryptographic verification, and availability of the ledger data. Journal blocks are sequenced and chained together with cryptographic hashing techniques, similar to blockchains. This provides us with additional security for confidential data storage. The database transactions are compliant with ACID (atomicity, consistency, isolation, and durability) properties. It uses optimistic concurrency control and transactions are fully serializable.

Paper Review: How Cloud Computing is Making Law Firms More Efficient and Profitable: What Moving to the Cloud Means for Legal Practices

Motivation: Despite the benefits that cloud-based solutions provide, many legal firms have not yet adopted them. The paper argues that cloud computing is essential for law firms due to the secure, remote accessibility it provides, along with more reliable, efficient, and collaborative workflows. In comparison to conventional on-premise legal software, it also highlights how simple setup and use are. The authors assert that cloud adoption will become ubiquitous among law firms in the future, and early adopters will gain a competitive edge. The purpose of the paper is to provide a summary of cloud computing technology and to emphasize the advantages of legal software powered by the cloud for law offices in terms of cost savings, productivity enhancement as well as increased security. They also discuss how cloud computing enables law offices and firms to "productize" the services they offer to clients. Additionally, the authors provide guidance on evaluating and selecting the right cloud software for law firms.

The need for legal firms to shift to the cloud is emphasized by the International Legal Technology Association's (ILTA) 2018 Legal Technology Survey. This survey found that more law firms planned to increase their use of cloud technology than they had the previous year. This has happened three years in a row.
69% of all legal companies reported that they intended to increase their use of the cloud; 84% of larger law firms said the same.

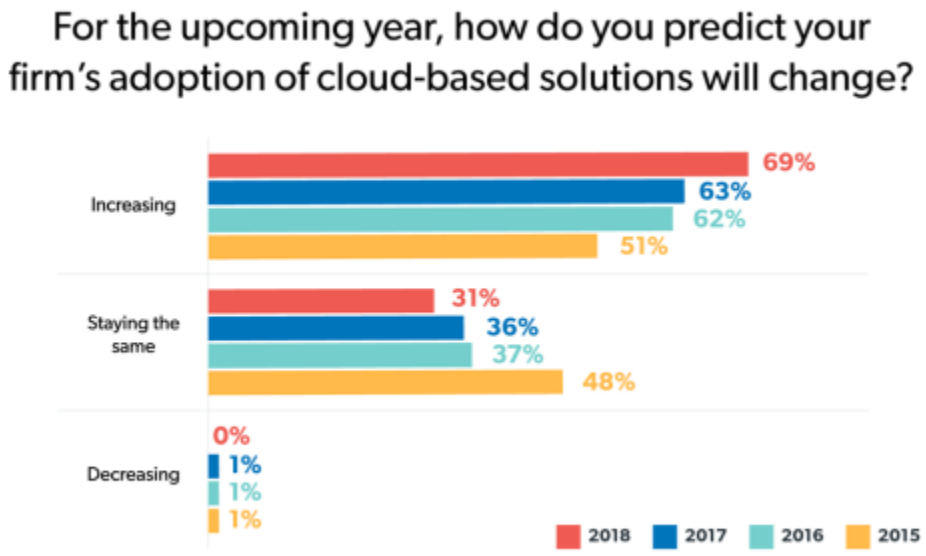

Figure 2: Graph depicting firm's cloud usage

The motivation of the paper is to highlight how crucial cloud computing is in helping law firms become more effective, lucrative, and competitive in the rapidly changing legal market. By embracing cloud technology, law firms can streamline their workflows, enhance client interactions, and maximize the use of their resources.

Method: The authors provide a comprehensive overview of cloud computing, starting with the National Institute of Standards and Technology's definition, which is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". It explains how the cloud enables secure internet-based storage and access to data, applications, and tools from any location.The three main layers of cloud computing—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—are also discussed by the writers. They illustrate how these levels work together to enhance software integration and efficiency. Through a single platform, today's cloud enables users to connect a great number of programmes, whereas people previously had to utilize many different software programmes independently of one another. This allows people to collaborate much more efficiently than they could individually.

The authors then go on to describe the three main reasons to adopt cloud computing- mobility, cost efficiency and security.

Mobility: The ease of synchronizing data across numerous devices, including computers, tablets, and phones, is made possible by cloud technology. Data transfer between devices would be labor-intensive without the cloud. A 2017 American Bar Association Legal Technology Survey also revealed that 79% of attorneys telecommute and spend a substantial amount of time working outside of their workplaces. Lawyers can access their work using a

variety of devices and from any location thanks to cloud computing. They can have complete access to their clients and matters whether they are at the office, traveling for a client meeting, or at home. Cloud mobility also makes it simple for team members to collaborate, regardless of their geographical locations or time zones.

Costs: For enterprises, cloud computing offers huge cost reductions. By doing away with internal servers and on-premise hardware, cloud solutions can, on average, reduce technological costs by at least 30%. The majority of cloud applications are turnkey solutions that can be quickly set up by downloading an app or going to a website, and they don't call for expensive hardware purchases or long-term contracts. According to research by the Information Systems Audit and Control Association (ISACA), 71% of businesses who made the switch to the cloud experienced a ROI that was on-target or greater than anticipated. These businesses ascribed the ROI to staff time savings, which allowed them to concentrate on more important duties, and lower operational costs than expected. The report focused on the FLRA Case Management System, which offered safe access to case data from any internet connection across the world and saw an 88% decrease in total cost of ownership over a five-year period. This system also eliminated upfront licensing costs, reduced annual maintenance expenses, eliminated hardware acquisition costs, and reduced annual maintenance costs.

Security: Comparing cloud computing to on-premises systems, data security is improved. Because of economies of scale, cloud software vendors may offer low pricing and cutting-edge security features. They make investments in infrastructure, dedicated security teams, network assault defense, compliance analysis, disaster recovery, data storage options, and other things. In the 2017 ABA Legal Technology Survey Report, large law firms claimed that 76% of their clients wanted them to apply stricter security measures. The survey also discovered that the majority of suppliers' cloud solutions met or exceeded return on investment (ROI) expectations. The Federal Labour Relations Authority's (FLRA) Case Management System's total cost of ownership (TCO) dropped by 88% over a five-year period after shifting to the cloud.

Cloud computing not only ensures data security but also contributes to cost savings and compliance with client demands for increased security measures. However, despite client expectations, many law firms are currently unprepared in terms of modern cybersecurity.

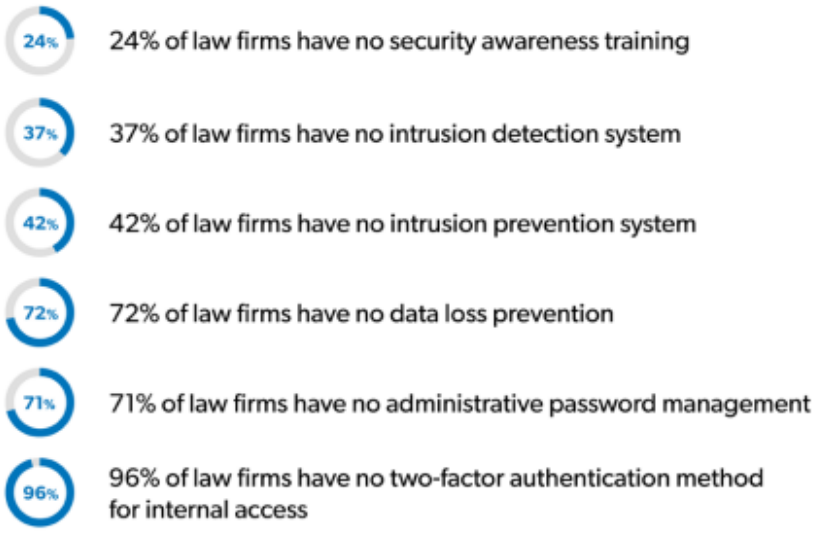

Figure 3: Percentages of cybersecurity usage in law firms

The ILTA 2018 Tech Survey exposed avoidable security vulnerabilities by highlighting alarming security patterns in the legal sector. The transfer to the cloud allows businesses to meet strict privacy legislation and professional security requirements while also saving money. The chosen cloud service must, however, include vital security precautions. For instance, Amazon Web Services supports a number of standards and laws, including IRS 1075, HIPAA, and GDPR. Failure to follow these guidelines could result in security breaches, which could have financial repercussions. Cost savings come from compliance, which a capable cloud service guarantees. Businesses may accomplish compliance, save money, and reduce security concerns by choosing the proper cloud provider.

Results: Firms can produce additional revenue streams without only depending on growing their client base and hiring more people by implementing cloud technologies and productizing some of their legal services. By delivering pre-packaged products alongside bespoke services, productization enables businesses to standardize and systematize legal services, resulting in cost savings and better resource utilization. In this paradigm, the cloud is essential for delivering digital services and automating tasks like document generation and administration. Applications (like Clio Manage) that streamline workflows and improve communication between lawyers and clients must be built . It is crucial to assess legal cloud technology, and while there may be issues with cost, security, and dependability, cloud computing excels in these areas when applied and maintained correctly. By using comprehensive cloud-based solutions (like the Clio Suite), businesses can effectively manage key operations like time and invoicing, case management, scheduling, document management, and contact management from a single platform made just for legal firms.

Paper Review: Reasons behind growing adoption of Cloud after Covid-19 Pandemic and Challenges ahead

Motivation: Cloud computing has been a prevalent term in the IT industry for many years, but its adoption among organizations has seen an unprecedented surge. In the wake of the Covid-19 pandemic, the global health crisis has compelled certain organizations to rethink their IT strategies and consider cloud computing as a viable solution.

The cloud has emerged as an essential and irresistible technology, offering organizations unparalleled access to IT systems, applications and software. It now serves as a catalyst for enterprise organizations seeking digital transformation, enabling remote working across the IT industry and ensuring continuous service availability.

The Covid-19 pandemic has transformed cloud adoption from a gradually approached future transformation to an immediate priority for organizations. Release from the limitations of closed hardware-based IT infrastructure is one of the main advantages of cloud computing. Employees can now access resources and services whenever they need them, eliminating the requirement to work from networked office spaces. As a result, there is a sizable need for qualified cloud professionals who are capable of managing and supporting cloud systems across various geographies.

The author aims to shed light on the transformative potential of cloud computing in the IT industry.

Method: The author highlights the benefits of the adoption of Cloud Computing, especially as seen during the Pandemic. The benefits include:

Remote Working Solution:

Cloud computing has provided a remote working solution that became crucial during the Covid-19 pandemic. With the implementation of lockdown measures worldwide, organizations with cloud-based infrastructure were able to adapt quickly to remote work. Cloud adoption allowed employees to work from anywhere, ensuring business continuity and minimizing disruptions. This realization led to a significant increase in cloud adoption among enterprises.

Business Continuity:
Organizations with robust cloud-based IT infrastructure experienced minimal disruptions during the pandemic. Cloud storage ensured secure access to critical data from any location. Even with lockdowns in place, businesses could continue their operations, thanks to the availability and accessibility of data stored in the cloud.

Efficient Collaboration:
Cloud computing simplified collaboration among team members, especially when working remotely from different geographic locations. Cloud-based platforms facilitated video conferences, content sharing, and secure group discussions, enabling efficient teamwork. Collaboration became essential for businesses, and cloud solutions provided an easy and effective way to connect employees and enhance productivity.

Remote Education:
Cloud technologies played a significant role in enabling remote education during the pandemic. Virtual solutions, such as Microsoft Teams, provided video-enabled remote classes and platforms for sharing documents and homework. Students and teachers could connect from anywhere, ensuring continued learning and maintaining a closer connection between educators and students.

Cybersecurity:
Cloud computing offers enhanced cybersecurity measures compared to on-premise infrastructure. The infrastructure is managed and administered by cloud service providers, who use the most recent security measures. Organizations using a shared responsibility model must keep an eye on their provisioned cloud services for potential threats and configuration errors, and take appropriate action. Cloud adoption has shown improved security for businesses and eased compliance with government regulations.

Scaling:
Businesses can increase their IT resources effectively and fast in response to demand thanks to cloud-based architecture. Organizations with fluctuating bandwidth demands can easily increase or decrease their cloud capacity without investing in physical infrastructure. This scalability offers cost management benefits and a competitive edge for enterprises.

Everlasting Advantages of Cloud Adoption:
Cloud adoption provides lasting advantages beyond immediate needs. Features such as high availability, scalability, business continuity, fault tolerance, disaster recovery, automatic software updates, and flexibility were the original benefits of cloud computing. As the adoption of cloud services grew, new features and services emerged from various cloud providers, including Amazon Web Services (AWS), Microsoft Azure, Google Cloud, IBM Cloud, and Oracle, each offering unique strengths in areas like network, storage, security, compute, and availability.
By harnessing the power of cloud computing, organizations can leverage these essential benefits, ensuring seamless remote work, business continuity, efficient collaboration, remote education, robust cybersecurity, scalability, and access to a variety of cloud services and features.

The author then goes on to specify the different types of Clouds, the differences between them and the advantages of each of them. A common choice is the public cloud, which uses a shared infrastructure paradigm to deliver cloud services via a network for public usage. Customers have little say in where the infrastructure is located,

and prices are frequently determined by pay-per-use or licensing rules. On the other hand, Private Cloud provides dedicated cloud infrastructure exclusively used by a single organization, providing greater control over security and data management. It can be hosted either on premises or off premises, depending on the organization's requirements.

The advantages of both private and public clouds are brought together in hybrid clouds. Businesses can benefit from each deployment's advantages while keeping them apart or segregated from one another. This flexibility enables scalability, adaptability, and enhanced security. Organizations can manage resources internally or choose to use external providers for specific services. Another cloud deployment option is the Community Cloud, which involves a collaborative effort between organizations with shared objectives. In this model, infrastructure is shared among the community members and can be handled either internally or by a third-party. The Community Cloud can be hosted internally within the organizations or externally, depending on their preferences and requirements.We then explore the different Cloud Computing Models:SaaS, Paas and IaaS.

Software as a Service (SaaS) is a cloud computing concept in which users can access software programmes online via a web browser. Based on their needs, it offers a quick and practical solution for enterprises to use software services. SaaS services are administered by vendors, freeing up the company's technical employees from handling software administration. Users can access the services without the need to download or install any applications or software. Popular examples of SaaS services include Dropbox, Salesforce, and GoToMeeting.

A framework for building and customizing apps is provided by the cloud computing concept known as Platform as a Service (PaaS). It provides a foundational platform so that programmers may create apps more quickly. Developers are in charge of their own customizations, while a third-party service provider is in charge of maintaining the infrastructure for servers, storage, and networking. Google App Engine, AWS Elastic Beanstalk, and Openshift are a few PaaS service examples.

A cloud computing model called Infrastructure as a Service (IaaS) offers computing infrastructure, such as networks, storage, servers, and operating systems, as services. It offers the highest level of flexibility and control to users, as they have complete control over the infrastructure. IaaS services are highly scalable and dynamic, allowing users to adjust resources as needed. IaaS services include, for instance, Microsoft Azure, Cisco Metacloud, Google Cloud Compute Engine, and Amazon Web Services EC2 instances.

While cloud adoption offers numerous advantages over on-premise infrastructure, it also presents several challenges that need to be addressed. The Australian Government stresses the significance of performing a risk analysis prior to deciding how much responsibility should be shared between the cloud provider and the end user. Data protection and security pose a significant problem. Organizations must carefully select the storage method for their data and put in place the necessary security controls. Data sensitivity determines the level of security needed, and encryption should be taken into account for both data in transit and data at rest. Due to the distributed nature of the data, data security in the cloud is more complicated than it is in traditional systems.
Another challenge is data location. Organizations need to know where their data will physically reside, as privacy and security laws vary across countries. While data replication for high availability may be necessary, local laws and regulations must be taken into account to ensure compliance.

The lack of qualified individuals with experience in cloud computing is a big barrier. For a successful cloud adoption journey, hiring and maintaining personnel with strong cloud capabilities is essential. In order to prevent unexpected vulnerabilities, proper implementation is required, and having qualified cloud professionals in the company is crucial. The lack of such engineers, however, makes it difficult to move forward with cloud adoption.

Addressing these challenges requires careful planning, considering data security measures, compliance with regulations, and access to skilled professionals. By addressing these issues, organizations can mitigate risks and fully leverage the benefits of cloud adoption.

Results:
Cloud computing has become the new normal for enterprise technology infrastructure. The fact that Microsoft's Azure was awarded a $10 billion project by the U.S. Defence Department is evidence of the security and resilience of cloud services over the past 20 years. The advantages of cloud adoption have demonstrated that businesses must use the cloud gradually. The COVID-19 epidemic has increased the adoption of cloud services as companies have realized the potential and advantages of the cloud in strengthening and enhancing their company processes.
A key factor in guaranteeing the smooth delivery of services during the pandemic has been cloud computing. It has made it possible to effortlessly provide new services. For instance, in reaction to COVID-19, Google offered the first 60 minutes of its online meeting service, Google Meet, free. The number of users using video conferencing products like Microsoft Teams, Zoom, and Google Meet each day has surged. These resources are now necessary for enterprises to continue operating.

According to a US Department of Labour study, IT vocations have been demonstrated to have the lowest incidence of COVID-19 infection. This is a result of these specialists being able to operate remotely thanks to IT infrastructure, which has made this possible. The danger factor provided by COVID-19 infections can be further decreased, and future pandemic circumstances can be better prepared for, by increasing digital transformation and cloud use.

In conclusion, the Covid-19 outbreak has brought into sharp focus the crucial function of the cloud in enabling remote access to data, guaranteeing business continuity, and reducing risks. Businesses that have strong cloud capabilities performed better than those that were dependent on on-premise infrastructure. This experience has sped up the adoption of the cloud and highlighted how valuable it is for ensuring service continuity and enabling remote work. Adoption of the cloud is currently a crucial factor for designing future work plans. However, it also comes with new obligations, such as adhering to privacy and security regulations and putting in place suitable security measures. Given the hazy and unstable nature of the business environment, cloud adoption has become unavoidable for new projects and migration of existing systems.

Paper Review: Light-weight and Scalable Hierarchical-MVC Architecture for Cloud Web Applications

Motivation: The usage of lightweight and scalable Hierarchical MVC architecture is the best option given the rising demand for modular and scalable Web development technologies.
Particularly for Web applications with their pervasive user interactions and dynamic information that is becoming ever more complex.

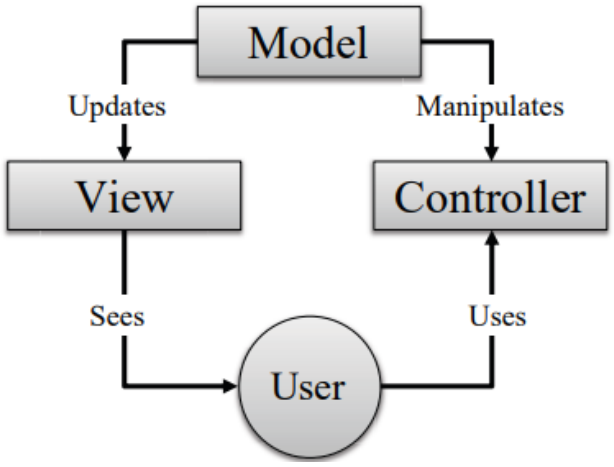

Fig. 4: Model-View-Controller Design Pattern

As shown in Figure 1 , the application is divided into three categories namely model, view and the controller where as the names suggest model defines the architecture , the view is the UI which the user can use to make changes and these changes affect the model via the controller.

Hence, the controller is a mediator. This segregation of the tasks makes the handling of the system easier and enhances the performance of the application.

Over the years different forms of MVC have been used by introducing small changes in the existing pattern. Example: MTV (Model-Template-View), MVVM (Model-View-ViewModel) etc. but the best one to utilize for the cloud based user interaction intensive web applications is the HMVC.

Method: In this study the takeaway is the further clarity of the concept of modularity of the application in the form of HMVC (Hierarchical MVC) for using our legal technology based cloud platform. In order to use it all the different functionalities of the web application will be in the form of a separate MVC and these will be linked to each other in a tree-like hierarchical architecture.

For instance , case management, document management, employee management etc. are all different microservices to be implemented. These microservices each would have their model , user interface(view) and the controller and would be linked to each other creating a hierarchy.

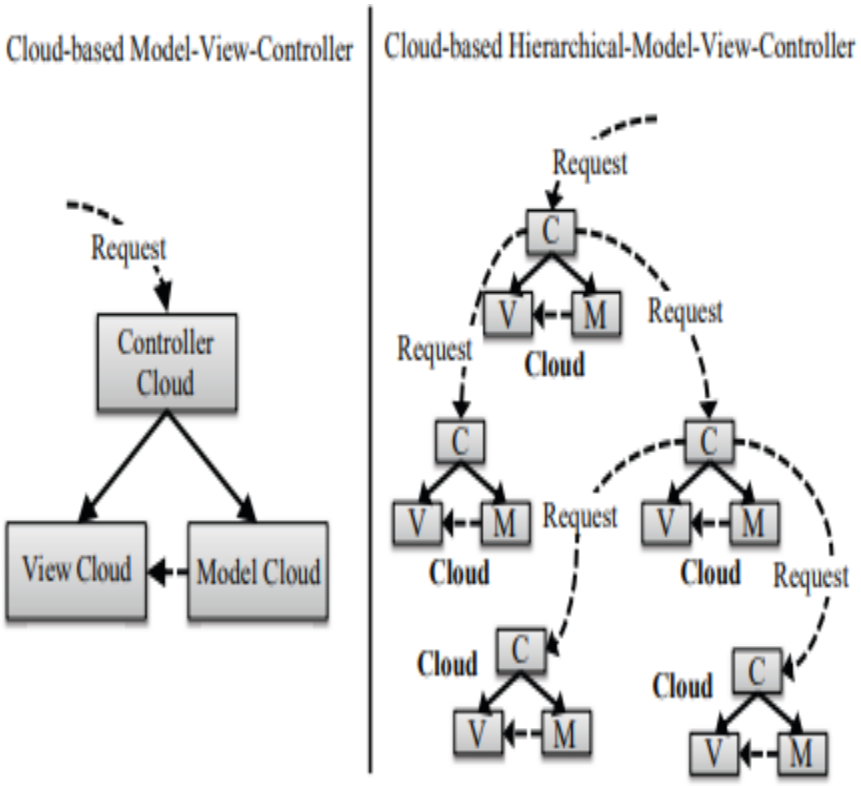

Fig 5: Differences between cloud-based MVC and cloud-based HMVC design pattern.

In this study, we will also use component-based Web application architecture that is based on Web Module Definition (WMD), in addition to HMVC. A Web module's dependencies and structure are described in the Web Module Definition (WMD) specification. Decoupled into a collection of Web modules is the complete application. Each module is capable of autonomous development, testing, and deployment.These microservices are to be connected via the RestAPIS.

Results: The goal of all the features to be used as mentioned above is to achieve three most required qualities of all the applications in today's world of high amount of data flow and the aim to achieve the highest possible efficiency and performance.Those qualities are :

1. Scalability
2. Maintainability
3. Simplicity

One of the other most important features of this model is that each microservice MVC architecture serves as the template for the others which introduces a reusability factor for the cloud based service .The connections between the microservices will be based on the links between the data in hand in terms of foreign keys introduced in the database to be used.

This architecture can be used with any language for our backend and frontend and hence gives us the utmost flexibility.Our model uses Java for the controller and model code and React JS for our UI which will serve as a view for our users.

The takeaway from this paper is the use of HMVC for our cloud application to be hosted on AWS which will have other important attributes from our base paper as well as other novelty based papers. This study just serves as a characteristic of our utility which makes it easier to use and is being implemented worldwide now.
Lastly, there will be the huge task of connecting all the microservices. Even though the life-saving RESTful APIs will come into play there will be the inevitable dependency issues. The future scope of this study is to resolve those dependency issues and implement the dependency management tool.

Paper Review: CloudInspector: A Transparency-as-a-Service Solution for Legal Issues in Cloud Computing

Cloud computing is currently one of the most well-known trends in the IT industry. Using cloud computing has many advantages, including greater redundancy, scalability, pay as you go, resilience, flexibility, and cost savings.There are different ways in which these can be used in the form of public , private or hybrid cloud platforms. This versatile nature of cloud has increased its demand in the tech society and every major sector is advancing towards betterment in this field.

On the other hand , there are industries which are skeptical to use the cloud platforms because of security and privacy concerns of their data.Since, the cloud providers serve as a third party for this whole process to work , legal ,health industries etc. which run on the trust of the people or their customers are not fully accepting of this trend.

In this study we focus on the need to balance the transparency of the data and its privacy Legally speaking, this is extremely important because, for example, data protection law demands that personal data be handled transparently, which implies that the data subject must be aware of what happens to his personal data and that it must be protected at all costs from system failure and saved from any unwanted alterations or destruction.

Hence, the software as a service that is to be built should have enough transparency that the trust factor is not hampered. This is a very important part of our project as this goes to the root of why the legal industry is behind and helps us eradicate the problem by giving us Transparency-as-a-Service.It offers a technique and answer for increasing openness and addressing issues with legal compliance, privacy and security of data in cloud environments.

Method:

To achieve transparency in cloud computing, CloudInspector uses a collection of approaches. These techniques include:

1. Monitoring: To make sure that the cloud service provider complies with regulatory requirements and industry standards, the solution regularly examines and monitors its operations and procedures. It monitors the supplier's compliance with pertinent laws, rules, and contractual requirements.

2. Auditing: CloudInspector conducts routine audits of the cloud service provider's policies, procedures, and infrastructure. By doing this, the provider may be sure that the necessary security controls, data protection strategies, and compliance procedures are in place.

3. Risk Assessment: The solution does thorough risk analyses to find any potential legal problems related to cloud computing. It assesses variables such data privacy, security lapses, jurisdictional issues, and adherence to national and international regulations.

4. Verification of Compliance: CloudInspector examines the compliance of cloud services.

` Some of these features will be used in our cloud based web application to ensure that the tenants of the cloud service provider are able to achieve the benefits of the cloud and the trust is established by providing them with real-time data enabling them to know the altercations in a transparent way. This transparency though should be just for the individuals who own the data others in the network will have the data in the encrypted format using AES and blockchain techniques so the data is as safe as it can be.

This is where privacy policy and access rights / privileges for the data is to be used. Besides , there are legal issues in the cloud computing industry and contracts regarding these laws are present when there is tie up between tenants and the cloud service providers.For instance, a tenant can incur some financial loss as a result of a malfunctioning cloud service they use. There are Civil Laws as well as Data protection laws for the same.

Results:

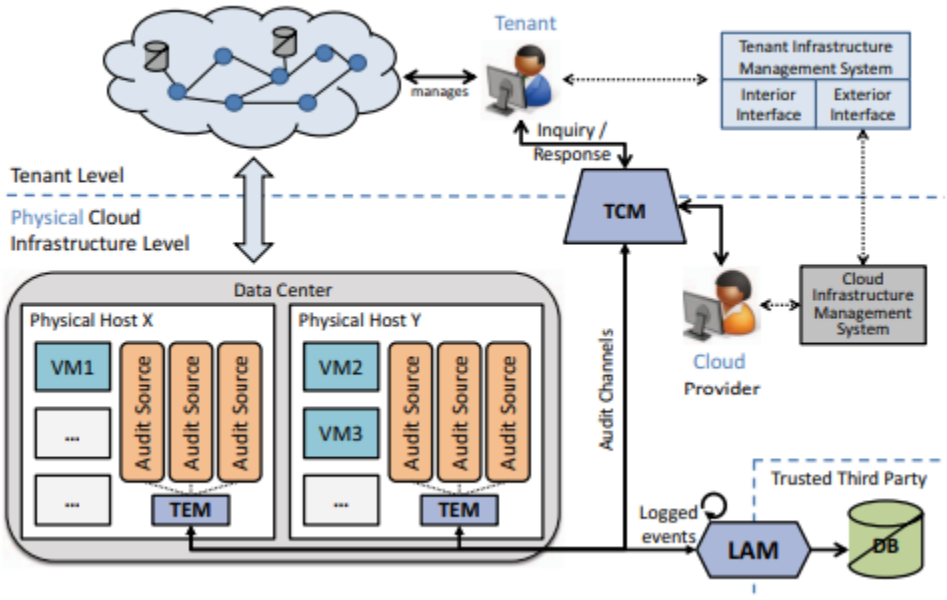

Fig 6: CloudInspector – Transparency-as-a-Service Framework

To address legal concerns in cloud computing, CloudInspector provides the following solutions:

Transparency is improved by CloudInspector's monitoring, auditing, and evaluation of the cloud service provider. Customers can learn more about the practices, data handling procedures, and compliance initiatives of the supplier, ensuring more visibility and control over their data.

Legal Compliance: CloudInspector assists clients in making sure that their cloud service providers abide by applicable laws and regulations. It aids in assessing how well the provider's operations adhere to all applicable legal requirements, market norms, and contractual commitments.

Risk Reduction: CloudInspector identifies potential legal issues through thorough risk evaluations and offers suggestions to reduce them. This aids clients in selecting trustworthy cloud service providers and putting suitable risk management techniques into practice.

CloudInspector is primarily concerned with data protection and privacy.

This study also brings light to the cases of negligent behavior or contract violation which is to be prohibited at all costs while developing the cloud application for enhancing legal tech.

Our objective is to improve consumers' visibility and control over cloud service providers so they can make wise decisions and safeguard their data. Organizations can confidently navigate the legal environment of cloud computing and make sure their activities comply with pertinent laws and regulations by utilizing this service.

Paper Review: Secure Cloud-based E-Health System using Advanced Encryption Standard

Motivation: The greatest option for managing vast amounts of data at a lesser cost than replacing hardware and reorganizing infrastructure is cloud storage. There is an increasing need for more storage space as the use of digital image applications grows. Image-based data requires more storage space than text-based data because it is essential for applications like face and object identification. Cloud computing is used for image processing applications, enabling large photo databases to be outsourced to cloud servers and reducing the storage burden on local hardware. To protect sensitive information, it is crucial to encrypt photographs before transferring them to the cloud. The difficult problem of safe data interchange in cloud computing has long been regarded as being best addressed by ciphertext-policy attribute-based encryption.

Method:
The AES algorithm outperforms the DES algorithm in terms of strength and speed. As a symmetric key block cipher, AES uses the same keys for both encryption and decryption. A 128-bit key needs 10 rounds; a 192-bit key needs 12 rounds; and a 256-bit key needs 14 rounds. The number of rounds needed for AES encryption varies based on the key length. Each round of encryption uses a variety of methods, including adding the round key to the plaintext, shifting and combining rows and columns, altering sub bytes, and more.

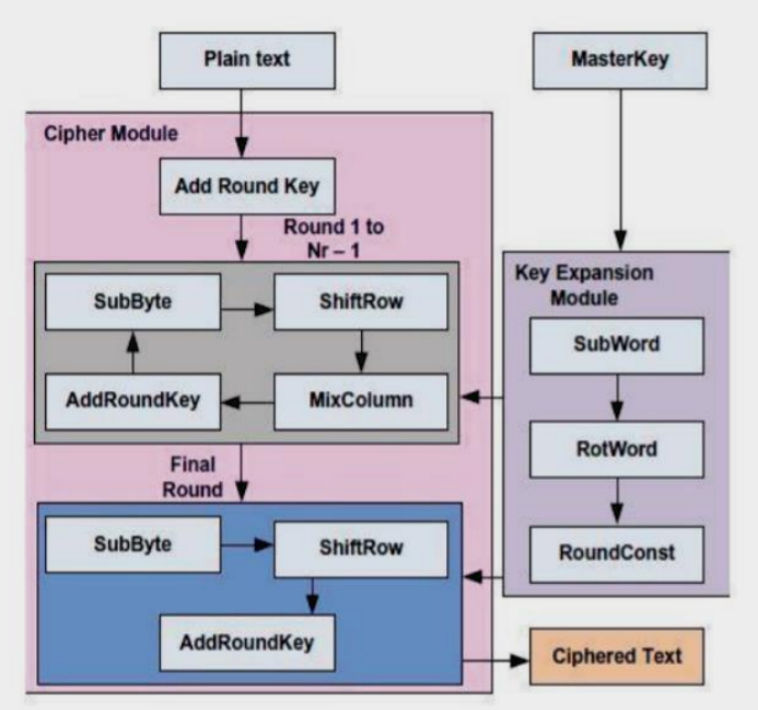

Figure 7 : Complete AES encryption process.

Results:

An image's gray histogram, which shows the frequency of different pixel values, is a useful tool for figuring out the image's general features. Therefore, in digital image encryption, the contrast of the histogram can be used to evaluate the level of picture encryption. A significant difference between the original and encrypted photos can be seen by contrasting their histograms. This finding confirms the AES method's suitability for image encryption and points to the high level of security this algorithm offers.

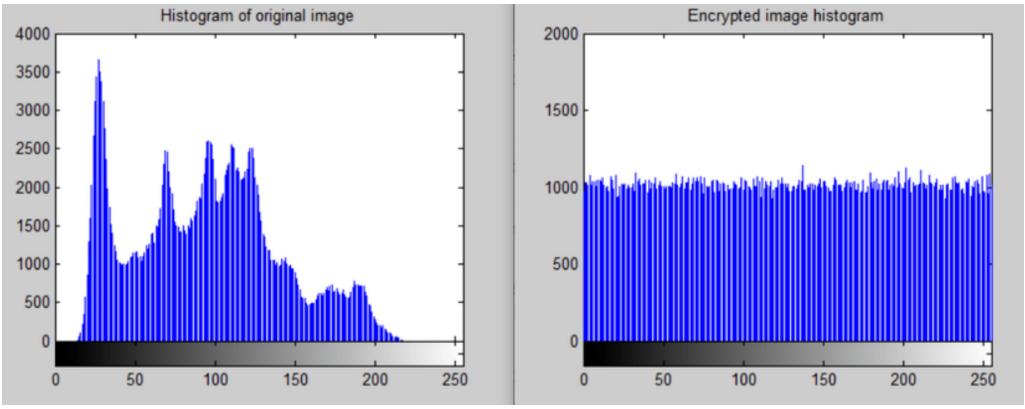

Figure 8 : Histogram of original image and the encrypted image

Paper Review: Securing Cloud Native Applications Using Blockchain

Motivation: Cloud computing has gained prominence over time and is now a well-known technology. The benefits of cloud computing include economies of scale, modularity, and adaptability. Decentralization, immutability, traceability, and transparency are all added benefits of combining blockchain technology with cloud computing.

Network security: Cloud-based installations depend on the supporting networking infrastructure, such as DNS servers, offered by cloud providers. These DNS servers are susceptible to online attacks, though. Common instances of DNS attacks include man-in-the-middle attacks, DNS cache poisoning, and DNS hijacking. The current DNS system has a centralized paradigm of operation. Blockchain-based DNS implementations have been offered as a solution to these issues, seeking to decentralize the system and lessen the aforementioned cyberattacks.

Container security: Due to their packaging and deployment capabilities, containers have emerged as a key component of cloud-native applications. Containers provide minimal virtualization without adding a lot of processing burden. However, image flaws, orchestration risks, runtime risks, and host OS risks can all lead to container vulnerabilities. A blockchain-based image registry can be used to enforce and guarantee security measures in order to improve security for openly accessible container images. Blockchain can also be used to manage vulnerabilities in container images, in addition.

Identity management: Identity management is frequently centralized and handled by a reliable central organization in cloud-based systems. This centralized system, though, is vulnerable to both internal and external dangers. Each account in blockchain is uniquely recognised by a public key, and the account holder is required to maintain the confidentiality of the matching private key. Utilizing smart contracts created on the blockchain, blockchain-based identity management and authentication procedures offer increased security and decentralization.

Audit log: Forensic procedures including data collection, investigation, analysis, and reporting, such as attack analysis, depend heavily on audit logs. However, the centralized nature of the existing logging techniques makes it difficult to ensure data integrity. Blockchain-based audit log systems provide a solution for these issues. The immutable ledger of a blockchain can be used to enable tamper-proof logging, enhancing security and integrity.

Method: Blockchain keeps track of all transactions using a decentralized peer-to-peer ledger. The blockchain network's peers and nodes each keep a copy of the ledger on file. A technique for distributed consensus ensures that the ledger state is consistent between multiple nodes. Each node's ledger is made up of a sequence of blocks, each of which is connected to the one before it using cryptographic hashing. The transaction data is briefly represented within each block. The diagram shows a series of connected blocks to show how the blockchain is structured. It is difficult for an attacker to alter blockchain data because of the interconnectedness of the blocks and the distributed structure of the ledger on each node.

Results: Cloud-native application architecture is expected to overtake traditional approaches to development in the upcoming years. The security of these applications, however, presents a considerable barrier. A blockchain-based strategy has a lot of promise to satisfy these security needs. Various security requirements, including network security, container security, identity management and authentication, and audit log management, are addressed in the current study by a potential blockchain-based solution.

References

1. [5] Joshua Lenon and Sam Rosenthal: How Cloud Computing is Making Law Firms More Efficient and Profitable: https://cdn2.hubspot.net/hubfs/470182/Clio-how-cloud-computing-makes-law-firms-efficient-and-profitable%20asset.pdf

2. [1] Mayank Gokarna: Reasons behind growing adoption of Cloud after Covid-19 Pandemic and Challenges ahead :arXiv:2103.00176 [Cloud]

3. [1] M. Ma, J. Yang, P. Wang, W. Liu and J. Zhang, "Light-Weight and Scalable Hierarchical-MVC Architecture for Cloud Web Applications," 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Paris, France, 2019, pp. 40-45, doi: 10.1109/CSCloud/EdgeCom.2019.00017.

4. [1] M. Flittner, S. Balaban and R. Bless, "CloudInspector: A Transparency-as-a-Service Solution for Legal Issues in Cloud Computing," 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), Berlin, Germany, 2016, pp. 94-99, doi: 10.1109/IC2EW.2016.36.

5. [1] D. B, P. J, S. C. M, S. Rajagopal and B. Jegajothi, "Secure Cloud-based E-Health System using Advanced Encryption Standard," 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2022, pp. 642-646, doi: 10.1109/ICESC54411.2022.9885501

6. [1] P. Mendki, "Securing Cloud Native Applications Using Blockchain," 2021 12th International Conference on Information and Communication Systems (ICICS), Valencia, Spain, 2021, pp. 419-423, doi: 10.1109/ICICS52457.2021.9464583.

7. Author(s): Amazon Web Services
Title: "AWS QLDB- Developer Guide" Website: AWS Documentation
URL: https://docs.aws.amazon.com/qldb/latest/developerguide/what-is.html
Accessed: [9th July 2023]