JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 07 Issue 02
2024

Research Article
https://doi.org/10.56979/702/2024

A Security Framework for Data Migration over the Cloud

Muhammad Azam[1*], Fawad Nasim[1], Jawad Ahmad[1], and Sohail Masood Bhatti[1]

[1]Faculty of Computer Science and Information Technology, The Superior University, Lahore, 54600, Pakistan.
[*]Corresponding Author: Muhammad Azam. Email: buzdarsuperior@gmail.com

Received: March 12, 2024 **Accepted:** August 19, 2024 **Published:** September 01, 2024

Abstract: The adoption of cloud services has ushered in a new era of business efficiency. However, major organizations' migration of critical software and data has encountered unanticipated obstacles, chiefly driven by concerns regarding data privacy and security. This article highlights the profound ramifications of migration delays, emphasising their potential to disrupt the uninterrupted flow of information, particularly in public and hybrid cloud environments. Our study reveals a well-organized framework that highlights essential security measures, such as the use of SSL/TLS protocols, which provide a secure channel of communication over the internet, data confidentiality and integrity (transmitted between a user's web browser and a website's server), encryption, authentication, building trust, and supporting data transmission integrity. In addition, we support the thoughtful application of restricted migration tickets, which effectively control access privileges and thwart unauthorized access. An innovative addition to this framework is the incorporation of Prediction-Based Encryption (PBE), a cutting-edge methodology uniquely suited to the intricacies of the healthcare and e-commerce sectors. PBE inherently segregates sensitive data, isolating it for separate storage, thereby mitigating the risk of data breaches during migration. It also refers to a theory wherein encryption techniques combine models or prediction algorithms to improve security. This could entail anticipating possible security risks or modifying encryption settings in response to expected shifts in the security environment. In conclusion, by embracing these meticulously devised security measures, organisations can surmount the challenges posed by migration delays and fortify their data protection strategies in the digital age.

Keywords: Cloud Computing; Data Migration; Data Transfer; Cloud Storage; Framework; Security.

1. Introduction

When using cloud technology, you may access an utterly virtual environment to store and access data. The success of the migration to the cloud depends on gathering as much information as possible about the capabilities of the cloud provider. If data is not migrated systematically, the company's data assets could be at risk from cloud computing and data security issues [1]. Regardless of their size or age, organizations that move their data to the cloud risk losing it or having it accessed by unauthorized parties. The organization may suffer significantly as a result in terms of finances and reputation. Therefore, it is essential to balance the potential drawbacks with the benefits of cloud computing, as it is a good example of risk management in action [2].

All created data is gathered and safely stored in the cloud using cloud analytics technology, making it available from any internet-connected device. The data can then be processed, cleaned, arranged, and analyzed by the cloud analytics system using its unique algorithms, considering both qualitative and quantitative aspects simultaneously. Even when safeguards are in place, and there may be advantages, it is crucial to pay close attention to the dangers involved. The responsibility for an organization's safety remains with the organization itself [3]. Too much oversight can lead to system failure, so it is crucial to strike a balance between the amount of control a program has and the associated risks. When working within a virtual private cloud (VPC), it is essential to consider the security settings, as the service provider can modify them remotely without knowing what the end user is doing.

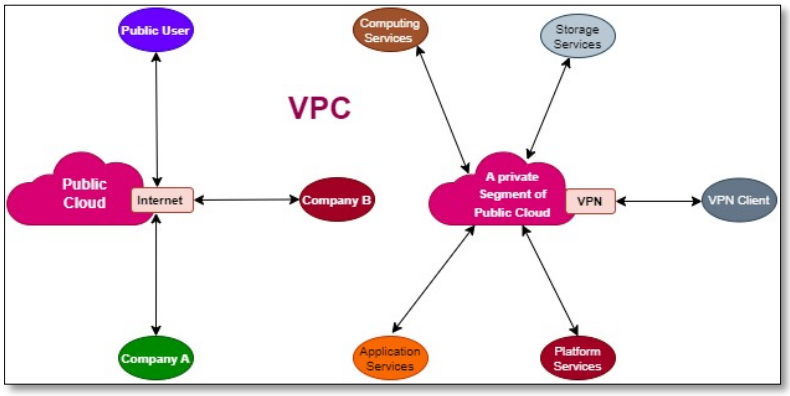

Figure 1. Virtual Private Cloud (VPC)

When transferring data, it is essential to consider the underlying infrastructure's secrecy and traceability requisites [4]. Using cryptography protects data's secrecy during transmission and access, while audibility ensures that security configurations have not been tampered with. Remote attestation methodologies have made this possible, with a trusted platform module (TPM) providing a summary of the system to attest to its safety level before attestation can occur, and a computer or virtual machine that has an inbuilt secure crypto processor chip is called a TPM. It generates and stores cryptographic keys, measures the system's state safely, and performs cryptographic operations while functioning as a safe hardware vault. Consider it your device's haven for private information [5].

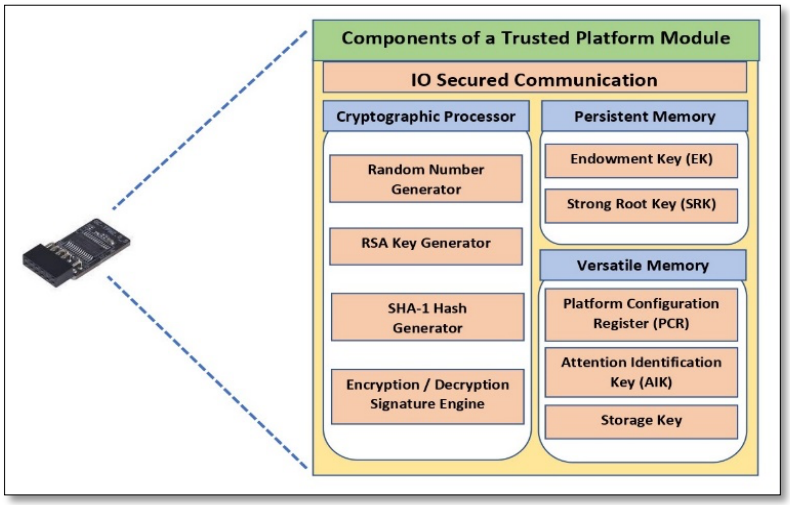

Figure 2. Trusted Platform Module (TPM)

Transferring virtual computers (VMs) is now more straightforward [6] thanks to the cloud and other virtual environments. As a result, it is essential to establish a method for trusting each tier of a cloud architecture. Keeping data secure is of the utmost importance, and infrastructure providers must share the precautions they take to protect their physical assets. So, there are a lot of issues related to the cloud environment we have to face these days.

A. Data Loss and Data Breaches: When a third party lacks permission to access confidential information, the risk of data breaches increases with cloud computing. Malware injection, service hijacking, and other forms of attack are among the factors that contribute to this risk. Data loss can result from malevolent attacks, service provider deletions, and natural disasters. For instance, Amazon lost information about its customers permanently, and Google lost user data due to repeated lightning strikes on its electrical infrastructure [7].

B. Insider Threat: Malicious acts, whether deliberate or accidental, committed by persons inside an organization. The misuse of cloud resources and the risks posed by employees and other insiders are other concerns. Employees with access to a company's cloud services can misuse customer accounts, financial data, and other sensitive information. Secure procedures, access control, and technical solutions can help

prevent these security breaches. The abundance of available space also makes it easy for hackers and ordinary users to engage in dangerous activities such as data theft and virus hosting [8].

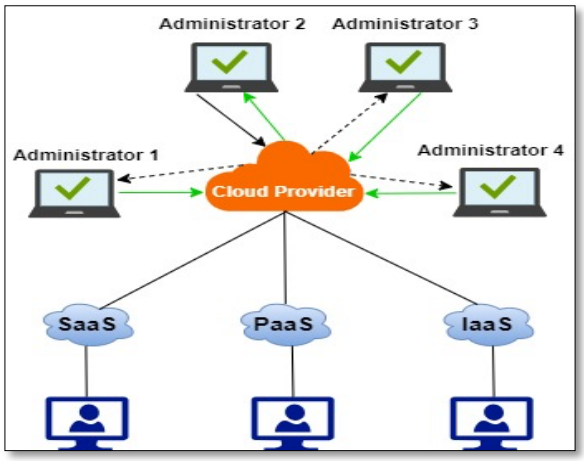

Figure 3. Insider Threat (IT)

C. Insecure APIs*:* API security vulnerabilities are another potential issue. Customers can create their unique cloud-based services by connecting to, managing, and retrieving information from the cloud using application programming interfaces (APIs). This makes it easier to customize cloud services to meet the specific needs of each company. Mobile apps can connect with servers and other online resources using APIs, and developers can integrate them with other systems [9].

D. Attacks by a Man-in-the-Middle (MitM): A Man-in-the-Middle (MitM) attack occurs when an unknown third party, such as a client and a cloud service, intercepts and perhaps alters communication between two parties without the parties' knowledge. This form of attack could compromise the confidentiality, availability, and integrity of data and services in the context of cloud computing.

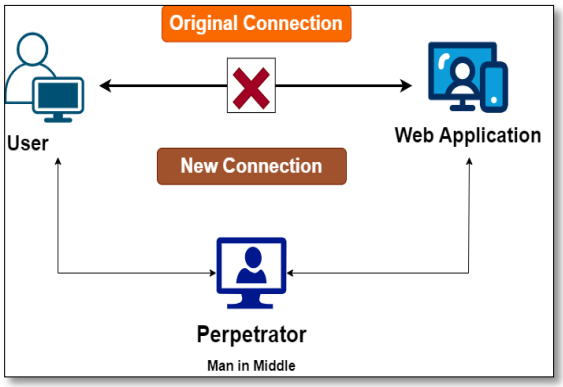

Figure 4. Man-in-the-Middle (MitM)

E. Eavesdropping: In cloud computing, eavesdropping attacks refer to the unapproved monitoring and interception of communication between two parties, usually with the intention of obtaining confidential data. Because cloud computing depends on network connections to transport data between users and cloud service providers (CSPs), improper security measures might lead to eavesdropping attacks.

F. Shared vulnerability: The responsibility for data security in the cloud falls on both the user and the cloud service provider. If either party fails to meet their responsibilities, sensitive information may be at risk of being compromised. Finally, the accessibility of cloud computing advantages a large number of users but can also contribute to a sense of inferiority [10].

G. DoS Attacks: DoS attacks overload the network with traffic, preventing authorized users from accessing the targeted server or website. Malicious code intended to evade security precautions can also be hidden by this kind of attack, rendering the server inoperable. Network intrusion detection systems (IDS) can be used to detect and lessen the effects of DoS assaults, and traffic can be distributed across different pathways to assist reduce their effects. [11].

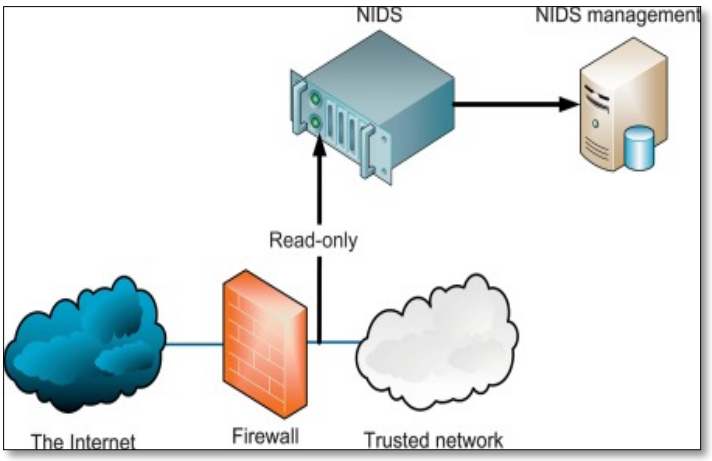

Figure 5. DoS Attacks

H. Identity and Credential Theft: In the context of cloud computing, identity and credential theft attacks are defined as malicious activities in which an attacker obtains unauthorized access to private user data, including usernames, passwords, and other authentication credentials, with the intention of impersonating a legitimate user or gaining access to cloud resources without authorization. The confidentiality, obtainability, and integrity of data and services kept in the cloud may be jeopardized by these attacks. The following explains the main elements of attacks involving identity and credential theft in cloud computing:

2. Literature Review

The practice of utilizing cloud-based resources to deliver additional capability in mobile devices is referred to as "elastic mobile cloud computing" (EMCC), which is an abbreviation of the full phrase. Cloud computing allows mobile devices to get some of the processing power they need without having to upgrade their hardware. It has been proposed that a comprehensive framework for the management of risks in elastic mobile cloud computing be put into place (EMCC). Its framework makes certain that EMCC is utilized even though some people are hesitant to use it due to concerns about its safety. The development of a generic EMCC framework begins with an analysis of the many EMCC schemes that are already in use. If adequate precautions are not taken during the transfer of crucial modules in the EMCC project, EMCC may face several security risks, including, but not limited to, the invasion of personal privacy and the management of the flow of information, to name only two of these risks. Another tough component of risk management is determining which modules are vulnerable and estimating the degree of risk that is connected with those modules. In this environment, we work to establish methods for quantitatively analyzing risks, build a tool for automatically identifying sensitive portions of Android applications, and conduct tests to check the correctness of the labeling [12].

The use of cloud computing is demonstrated as an approach that can successfully process data. The amount of secrecy is determined by the data weights, which are scaled according to the preprocessing attribute scale and depend on the size of the file. Eleven elements were chosen to make up the sensitivity category, and the quantity and quality of the information that was provided served as the deciding factor in whether or not those factors should be included. In the end, we use a method called K-means clustering to separate the parts into no more than five unique groups. Two frequent uses are the encrypting of data and setting the level of sensitivity of the information. Under the context of cloud computing, the methodology demonstrates how effectively data processing and sorting may be accomplished [13].

Safe information processing systems require trustworthy system development. Cloud computing firms have adopted zero-trust security, which treats all inputs as malicious unless proven otherwise. This contradicts perimeter security, which states that trustworthy users are always inside a trusted network and malicious actors are always outside. Trust is hard to define, measure, and verify since until recently, people focused more on its subjective aspects. In cloud-based federated learning systems, where people learn from one another, a lack of objective, verifiable trust must be addressed immediately. Utilizing our expertise in machine learning, we provide a zero-trust security framework for SaaS trust verification based on Rich

models. Additionally, we perform multimodal data analytics on service processing patterns to gain insight into service operations and vulnerabilities. SaaS service integrity is confirmed by this. Our approach uses federated learning to leverage AI-processed data from several cloud service users. Student votes identified data features, rich models for feature extraction from large-scale multimedia data, and ensemble classifiers. The techniques kept an eye on cloud services. The model was assessed with openly available data. This demonstrated the model's ability to monitor cloud service behavior and evaluate the security and reliability of SaaS. [14].

Data centralization may help IoT adoption (IoT). Internet of Things devices are increasingly stored and managed a central server with greater memory and a user-friendly interface. Data transmission will raise network infrastructure risks. Cloud IoT streamlines IoT system development and maintenance by reducing response times, latency, and network load distribution. Advanced strategies are employed by network attackers to exploit security flaws and steal user data. It has been attempted to connect network IDS to the cloud IoT interface by utilizing deep learning and machine learning on datasets unique to IDS. The transfer learning IDS with CNN architecture proposed in this paper works well for image classification. Using the CIC-IDS2017 and CSE-CICIC2018 datasets, we train five pre-trained CNN models. VGG16, VGG19, Inception, Mobile Net, and Efficiencies are some of the models. Prior to teaching CNN to comprehend images, Quantile Transformer preprocesses, balances, decreases dimensionality, and converts feature vectors. InceptionV3, MobileNetV3Small, and EfficientNetV2B0 were selected for the purpose of constructing an ensemble model for effective lightweight ensemble transfer learning through model averaging (ELETL-IDS) based on their performance. In the evaluation, the ELETL-IDS performed better than all state-of-the-art proposals. F-score, recall, accuracy, and precision are all 100%. This finding was confirmed by the MCC and AUC-ROC remaining at 0.9996. We provide a simple, fast, and reliable model for cloud-based Internet of Things in-torsion detection systems [15].

Clinical and anatomical pathology practices are quickly adopting cloud-based IT infrastructure to meet growing data storage, processing, and IT service needs. Cloud-based IT solutions are becoming more popular because they are scalable, trustworthy, and filled with features that are out of reach for SMEs. Even Organizations using cloud-based IT infrastructure face increased security and privacy threats because of public networks, unfamiliarity, and new capabilities. IT specialists and managers of healthcare facilities can assess cloud-based IT infrastructure in research labs with the aid of this best practices guide. Best practices in technology, operations, and organizations can help ease concerns about security, privacy, and other aspects of a strong infrastructure. We also demonstrate how best practices are incorporated into healthcare industry regulations. We recommend standardized hiring, communication routes with parent IT departments, security process evaluation and auditing, and trustworthy onboarding and offboarding. Operational, financial, and auditing/logging best practices will follow. In conclusion, cloud solutions vary in security depending on resource sensitivity. Laboratory directors, managers, and IT professionals must address core organizational and process-based issues before implementing technical security solutions and using cloud infrastructure [16] [28].

The IoT can improve accuracy and intelligence for low-intervention jobs. Creating "smart cities" with the Internet of Things is crucial. These cities provide smart transportation, trash management, housing, etc. Smart cities provide a variety of options for collaboration. Smart municipalities in smart cities use digitization and automation to provide complete local government cooperation services to improve people's quality of life. As people use several platforms, data security and privacy are at risk. Data privacy and authenticity are crucial for the local government and inhabitants. Our research presented a service security architecture for collaborative operations in municipal smart cities using SDN and smart contracts. Multi-chain Blockchain networks are testing collaborative service security design. We suggest using multi-chain blockchain and smart contracts to secure data in smart city governance architecture. Smart contracts are advised to secure heterogeneous IoT network interactions and transactions. To test the service security architecture, collaborative services use a case in an SDN-enabled IoT architecture was created [17].

To avoid chaotic node deployment and ensure methodical node expansion in big data clusters, utilize an association rule algorithm-based security scheduling strategy like the one in a cloud network. Nodes will expand systematically. The Hadoop/Map-Reduce framework's connection shape is determined by the association rule algorithm's numerous iterations. This ends the cloud network security study. After that, security mapping criteria are decided upon. Big data features are connected to the SDN scheduling system.

Accurate packet routing index value is achieved and the link bandwidth time list structure is produced. The results demonstrate that the massive data transfer in this investigation's cloud network is larger than 6.50 107 MB, and the continuous occupancy duration of cluster nodes is less than 0.70 milliseconds. This approach minimizes the need of cluster nodes and speeds up large-scale data transfers. It can set up cluster nodes for large data sets and control the unequal distribution of information parameters. [18] [29].

Multimedia files have grown from gigabytes to petabytes due to more precise data. "Cloud" servers store and send the most massive datasets. As cloud computing was built on the internet, cybercriminals attacked it. They hunt for new ways to steal personal data. They often fabricate data. Therefore, data security has been a focus lately. To protect sensitive multimedia material, this research examines optimization-based secret key selection methods. Improved Blowfish encrypts and decrypts cloud data. It generates the most secure key. Confidentiality and trustworthiness require finding the right keys. Data restoration is the opposite of data cleansing (decryption). Clan-based adaptive crowd search Probability is a revolutionary hybrid strategy that selects the best key for the situations and periods when one is needed (CCS-AAP). Following this, the new approach is evaluated [19].

Large data pipelines handle large amounts, diverse, or fast-moving data. To apply state-of-the-art machine learning and artificial intelligence approaches, this is required (volume, velocity, and variety). Huge data pipeline execution (i.e., cloud, fog, and edge) is made possible by cloud computing. However, designing continuous data pipelines necessitates considering a variety of factors, including message queue integration, triggers, data transfer techniques, computer resources, and data transmission routes. Tasks are significantly complicated by pipelines and data storage. Despite various problems (such as data availability, security, and backup), maintaining locally stored data is costly and time-consuming. Compared to on-premises solutions, cloud storage, also referred to as StaaS, and may offer better scalability, fault tolerance, and availability. We propose to combine StaaS with data pipelines by utilizing StaaS and compute on-premises or in a dedicated cloud. In addition, we rank storage choices according to user weights and preferences, server-side encryption, network performance, location, and cost. The analysis demonstrates that in four crucial user scenarios, the recommended technique is effective for data transmission, feature utilization, and dynamic storage option selection. [20].

5G infrastructure is being installed worldwide. 5G technology's ability to expand communication services across society while creating security concerns is debated. Others worry about the 5G network's design and performance-boosting technology. Although some 5G security architectures have been established, a complete security architectural framework would assist in tackling security issues. This article looks at the design of 5G technology and offers ways to make it safer. Relevant results were obtained by searching for 5G security and architectural keywords. These seven stages form the basis of most 5G security approaches and could be exploited to cause the 5G network to become unstable. Man-in-the-middle vulnerabilities, eavesdropping, and denial-of-service attacks can result from 5G authentication and authorization. Risk has been minimized using artificial intelligence, machine learning, blockchain, statistical process control, unmanned aerial vehicles, field programmable logic arrays, and hybrids. Light fidelity, smart grid networks, and multiple radio access are examples of 5G security technology. Security attacks on 5G networks will decline due to new threats. Thus, regular monitoring of the application of these solutions would be required. [21].

5G and other high-speed wireless networks have improved high-speed mobility vehicle network services. If you choose the Internet of Vehicles' open communication option, anybody can access your vehicle's Wi-Fi network's sensitive data (IoV). This study prevents unauthorized cars, observers, and drivers from connecting to the network and altering critical data to enable IoV's safe real-time information flow. This study provides layered security for data transfer in IoV and cloud contexts using a M-tree-based elliptic curve digital signature (ECDSA). This study offers a range of adaptable and scalable methods that minimize the time required to reconstruct the system key and resynchronize it, and dynamically change the framework in response to the rapidly evolving IoV topology. These modifications address security concerns with transmission. Unlike other key management research, we combine M-tree key management with secure data transfer to build a secure Internet of vehicles. Because this IoV has key management for all security levels, it is perfect for scaling or adapting. [22].

In the 21st century, cloud computing has become a well-known approach to satisfy data service stresses inexpensively, with little labor, and in a form that can be scaled up quickly. Due to Public Cloud's various security weaknesses, hackers may simply access data without authorization, initiate forging attacks, and carry out several other internal and external assaults. In this study, the Needham-Schroeder symmetric key protocol with onion encryption is employed as the basis for a multilayer security system. This system produces session keys to secure data from being stolen, spied on, tampered with, or made up. Using onion encryption, it was difficult to modify or manage access routes, and a blockchain-based architecture guaranteed that data was always valid [23].

The emergence of orchestration languages has facilitated the creation of cloud composite services, the elements of which can be located in multiple geographically separated data centers. At some point, these composite services might need to be adjusted to take use of cloud features like quick elasticity and scalability. Specifically, they can be redistributing their main resources because of performance limitations. However, there is a possibility that the resources or the cloud service might be jeopardized because of security holes created by the relocation. We suggest an automated security architecture based on SMT to streamline the resource transfer process inside cloud composite services and stop the creation of new configuration vulnerabilities. We formalize the underlying security automation based on the SMT solution, considering both internal and external security systems, in order to assess the transferred resources and choose the best countermeasures. Finally, we construct a proof-of-concept prototype to assess the merits and shortcomings of the popular open-source solver CVC4. According to our research, it is relatively cheap to move major operating systems to the cloud. [24].

Businesses and end users alike may find value in a free and open-source framework management solution. The prevention of data loss is simplified by cloud-based data leak control for both businesses and their customers. It's completely regulated, supervised in one place, and open to everyone who needs it. The Open-Source Cloud Framework enabled a method to be developed to prevent data loss. It's possible to distribute this framework under either a permissive Open License or a free and open-source Free License, allowing its usage by anybody in the world. It's compatible with Windows as well as UNIX and Linux. Despite the popularity of MySQL Server for database connectivity, open database connectivity and valid MSSQL credentials are still requirements. Case-sensitive information can be located in a single file or a batch of hundreds or thousands using the Open User Data Loss Management Console [25].

3. Proposed Framework

A. Pre-migration Security: Before initiating the data transfer process, a meticulous evaluation of all user accounts and login credentials is imperative. This proactive step guarantees the exclusion of outdated or potentially risky access methods. A single breached account can jeopardize the entire system's security. Thus, this initial step holds paramount importance in ensuring the confidentiality of data during transfer [26].

B. SSL Establishment: The foundation of migration security hinges upon establishing a secure connection between source and destination nodes using the Secure Sockets Layer (SSL) protocol.

This secure channel serves as the bedrock for fulfilling identified migration security requisites. Within this secure channel, temporary data encryption keys, random keys, and message authentication codes are employed. Notably, this stage also encompasses safeguarding the temporary migration tickets utilized by source and destination nodes to validate data node integrity. Whether migrating data from a local server to the cloud or between cloud service providers, robust secure connections are indispensable. A number of crucial aspects of SSL security are activated during the first exchange of information between two nodes. These include the usage of minimum privilege migration tickets, symmetric encryption with a random key, and message authentication coding via the initiation of a temporary session key.

C. Minimum Privilege Migration Ticket: Analogous to presenting identification and access rights at physical entry points, individuals must present valid tickets before accessing data nodes within the source cluster. This validation occurs at the data node level, where tickets are securely stored. Following an SSL handshake confirmation of ticket legitimacy, the receiving node establishes a connection. Any unauthorized access attempt is thwarted at this stage. To facilitate ease of frequent transfers while bolstering security, a strategy involves limiting the access rights granted by a single ticket. In essence, should an unauthorized entity obtain one such ticket, their freedom of movement would be severely

constrained. An essential aspect of this approach is the token's one-time use feature, impacting both data nodes and the entire system. The ticket includes an expiration date, enabling the detection of unauthorized access attempts, and thereby notifying the migration manager. Its primary purpose is to validate data transmission at the source node and restrict access to unauthorized tickets. Given that each ticket outlines data node location, concurrent migrations are discernible, ensuring a one-time usage policy.

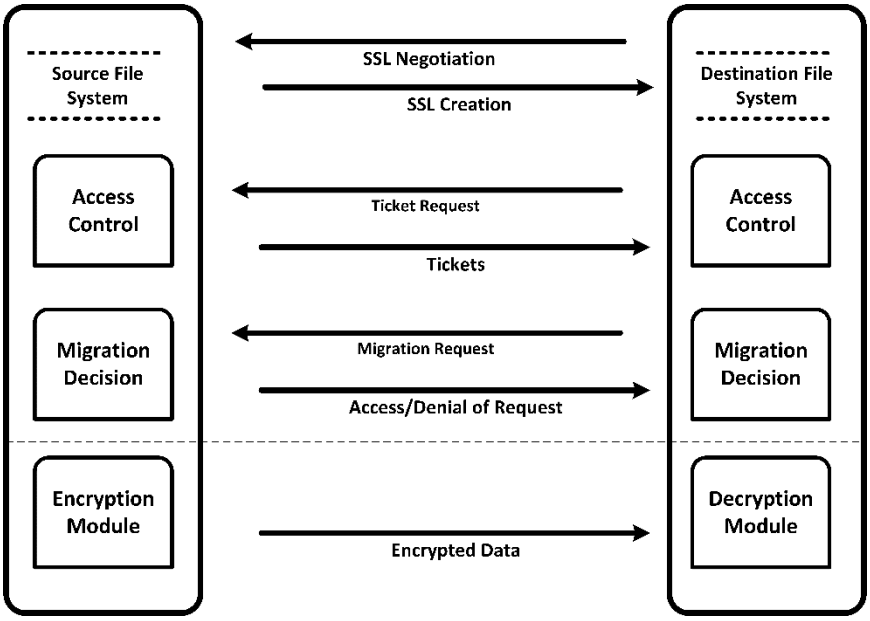

Figure 6. Proposed Framework Workflow

D. Encryption of Data via PBE: In scenarios involving file systems hosted either on-premises or in the cloud, security-conscious individuals often employ The SSL installation and establishment of secure channels require time investments, as does the generation and transmission of encryption keys, the creation of migration tickets, and the subsequent decryption of encryption keys. PBE, which employs both random and shared keys, influences the efficiency of data block encryption and decryption. In Table 1, we provide a comprehensive breakdown of the time required for key steps, such as encrypting, transmitting, and decrypting data, alongside the durations for establishing an SSL channel. These evaluations were carried out with data sizes ranging from 64 MB to 512 MB. Prediction-based encryption (PBE), identity-based encryption (IBE), and attribute-based encryption (ABE) all increase the amount of time needed to safeguard sensitive data, as would be expected. PBE is preferred because of its excellent performance. The first step in PBE is to encrypt the entire source file system with a randomly generated key. The encrypted data is then transferred. Data kept in the targeted cloud can be decoded thanks to the random key's encryption using a shared key [27].

4. Results

Security Evaluation: The effectiveness of our security measures, including Secure Sockets Layer (SSL) and restricted privilege tickets, in safeguarding data during migration is paramount. SSL, known for its robust security features, plays a pivotal role in securing point-to-point networks and various business scenarios. We successfully employed SSL for data transfer between data centers and public clouds, as well as between different public cloud providers. To deter unauthorized access, potential attackers are provided with limited-privilege "tickets" that come with both time restrictions and restricted privileges. Malicious activity often involves repeated attempts to use the same ticket, but our security measures have proven effective in preventing data breaches. The stringent restrictions placed on unauthorized users ensure that even if they gain access, the data they obtain remains unusable. Consequently, the confidentiality of the data is maintained at a high level.

B. Time/Cost Evaluation: Timeliness and cost-efficiency are vital considerations in any data migration endeavor. Our evaluation encompasses several critical aspects of the process, including SSL installation, ticket verification, data encryption using Prediction-Based Encryption (PBE), and decryption of data larger data sizes, offering valuable insights into the time and cost considerations of our migration strategy.

Table 1. Time / Cost for Data Migration

File Size	SSL Establishment	Migration Ticket Verification	PBE-Based Encryption And Decryption	Total Time
64 Mb	880ms	2ms	43600ms	44.4 s
128 Mb	895ms	2ms	93700ms	I. 576 min
256 Mb	900ms	2ms	187800ms	3.145 min
512 Mb	905ms	3ms	290000ms	4.848 min

C. Evaluation of Vulnerability to Attack: Ensuring data security involves a multi-layered approach. The SSL protocol facilitates secure communication by allowing the exchange of sensitive information, such as encryption keys and authentication codes, between senders and receivers. It stands as the most effective and secure method for data transmission. Furthermore, our approach of issuing migration tickets with minimal restrictions promotes efficient data transfer while enhancing security. Each ticket can be used only once, significantly deterring any malicious attempts to manipulate the system. Strengthening data security further, we employed Prediction-Based Encryption (PBE) with both shared and random keys. This allowed us to segment data into manageable blocks stored in distinct locations. The encryption process for data transmission can be executed independently for each data block, bolstering the overall security posture.

5. Conclusion and Future Work

Cloud migration, the process of transferring vital data and operations to the cloud, demands rigorous security measures. This paper has outlined a three-pronged strategy, aligning seamlessly with our proposed framework and supported by our research findings. Firstly, the establishment of a secure socket layer (SSL) is foundational for secure data transmission. SSL's role in enhancing cloud migration security, as per our framework, is unequivocal. Secondly, the creation of data migration tickets with minimal access privileges mirrors our framework's core principle of minimum privilege migration tickets, validated by our research as an effective means of safeguarding data integrity during migration. Data encryption, utilizing shared and random keys, is pivotal. Our research confirms the correlation between cipher strength and encryption, transmission, and decryption time, a crucial aspect emphasized in our time/cost evaluation. Looking ahead, we recognize the importance of exploring data transmission and encryption speed further. Partitioning data blocks into smaller units holds promise for optimizing both speed and security, warranting future exploration. So our approach offers a robust and practical framework for secure cloud data migration, substantiated by empirical evidence. We remain dedicated to guiding organizations through the evolving cloud technology landscape, ensuring data security and efficiency across diverse operating systems leveraging cloud storage capabilities.

References

1. K. KARUPPASAMY, 'Secure Framework to Enhance Security Using Hybrid Algorithm in Cloud Computing With Ssl'.
2. R. Mangalagowri and R. Venkataraman, 'Ensure secured data transmission during virtual machine migration over cloud computing environment', International Journal of System Assurance Engineering and Management, pp. 1–12, 2023.
3. S. Barhate and M. Dhore, 'Evaluating Data Migrations concerning Interoperability in Hybrid Cloud', presented at the Machine Learning, Image Processing, Network Security and Data Sciences: Select Proceedings of 3rd International Conference on MIND 2021, 2023, pp. 795–804.
4. L. Ghafoor, 'A Survey of Data Safekeeping in Cloud Computing under Different Scenarios', Authorea Preprints, 2023.
5. Tahir, Muhammad, Muhammad Rahim Zafar, Muhammad Talha Bashir, Saleem Zubair, Muhammad Waseem Iqbal, and Fawad Nasim. "An Automated Performance Enhancement Approach for Mobile Applications." Bulletin of Business and Economics (BBE) 13, no. 1 (2024).
6. Khan, Hira Haroon, Saleem Zubair, Fawad Nasim, Shamim Akhter, Muhammad Naushad Ghazanfar, and Sumbul Azeem. "Role of Kubernetes in DevOps Technology for the Effective Software Product Management." Journal of Computing & Biomedical Informatics 7, no. 01 (2024): 313-327.
7. A. Shehloo, M. A. Butt, and M. Zaman, 'Energy Saving Techniques for Cloud Data Centres: An Empirical Research Analysis', presented at the Machine Learning, Image Processing, Network Security and Data Sciences: Select Proceedings of 3rd International Conference on MIND 2021, 2023, pp. 763–779.
8. N. M. Reddy, G. Ramesh, S. B. Kasturi, D. Sharmila, G. Gopichand, and L. T. Robinson, 'Secure data storage and retrieval system using hybridization of orthogonal knowledge swarm optimization and oblique cryptography algorithm in the cloud', Applied Nanoscience, vol. 13, no. 3, pp. 2449–2461, 2023.
9. A. Chakraborty, M. Kumar, N. Chaurasia, and S. S. Gill, 'Journey from a cloud of things to the fog of things: Survey, new trends, and research directions', Software: Practice and Experience, vol. 53, no. 2, pp. 496–551, 2023.
10. D. Rambabu and A. Govardhan, 'Optimization assisted frequent pattern mining for data replication in the cloud: Combining sealion and grey wolf algorithm', Advances in Engineering Software, p. 103401, 2023.
11. Wang, R. Guo, H. Yu, Y. Hu, C. Liu, and C. Deng, 'Task offloading in cloud-edge collaboration-based cyber physical machine tool', Robotics and Computer-Integrated Manufacturing, vol. 79, p. 102439, 2023.
12. H. Hamad, A. Y. Dawod, M. F. Abdulqader, I. Al_Barazanchi, and H. M. Gheni, 'A secure sharing control framework supporting elastic mobile cloud computing', International Journal of Electrical and Computer Engineering, vol. 13, no. 2, p. 2270, 2023.
13. R. Singh and R. Pateriya, 'Data Clustering Approach based on Data Sensitivity for Implementation of Secure Cloud Computing Environment', presented at the Machine Learning, Image Processing, Network Security and Data Sciences: Select Proceedings of 3rd International Conference on MIND 2021, 2023, pp. 715–724.
14. M. Saleem, M. Warsi, and S. Islam, 'Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in SaaS cloud computing environment', Journal of Information Security and Applications, vol. 72, p. 103389, 2023.
15. O. D. Okey, D. C. Melgarejo, M. Saadi, R. L. Rosa, J. H. Kleinschmidt, and D. Z. Rodríguez, 'Transfer Learning Approach to IDS on Cloud IoT Devices Using Optimized CNN', IEEE Access, vol. 11, pp. 1023–1038, 2023.
16. N. Krumm, 'Organizational and Technical Security Considerations for Laboratory Cloud Computing', The Journal of Applied Laboratory Medicine, vol. 8, no. 1, pp. 180–193, 2023.
17. S. Siddiqui, S. Hameed, S. A. Shah, A. K. Khan, and A. Aneiba, 'Smart contract-based security architecture for collaborative services in municipal smart cities', Journal of Systems Architecture, vol. 135, p. 102802, 2023.
18. T. Peng and X. Wang, 'Security Scheduling Method of Cloud Network Big Data Cluster Based on Association Rule Algorithm', presented at the Machine Learning for Cyber Security: 4th International Conference, ML4CS 2022, Guangzhou, China, December 2–4, 2022, Proceedings, Part II, 2023, pp. 495–509.
19. S. Gadde, J. Amutharaj, and S. Usha, 'Cloud Multimedia Data Security by Optimization-Assisted Cryptographic Technique', International Journal of Image and Graphics, p. 2450010, 2023.
20. A.Q. Khan et al., 'Smart Data Placement Using Storage-as-a-Service Model for Big Data Pipelines', Sensors, vol. 23, no. 2, p. 564, 2023.
21. K. Shobowale, Z. Mukhtar, B. Yahaya, Y. Ibrahim, and M. Momoh, 'Latest Advances on Security Architecture for 5G Technology and Services', International Journal of Software Engineering and Computer Systems, vol. 9, no. 1, pp. 27–38, 2023.

22. H. Y. Lin and M.-Y. Hsieh, 'A dynamic key management and secure data transfer based on an m-tree structure with multi-level security framework for Internet of vehicles', Connection Science, vol. 34, no. 1, pp. 1089–1118, 2022.
23. P. Roy and R. Kumar, 'Onion Encrypted Multilevel Security Framework for Public Cloud', presented at the 2022 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), 2022, pp. 1–5.
24. M. Oulaaffart, R. Badonnel, and C. Bianco, 'An Automated SMT-based Security Framework for Supporting Migrations in Cloud Composite Services', presented at the NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, 2022, pp. 1–9.
25. S. Ahmad, S. Mehfuz, and J. Beg, 'Cloud security framework and key management services collectively for implementing DLP and IRM', Materials Today: Proceedings, vol. 62, pp. 4828–4836, 2022.
26. A. Imtiaz, D. Shehzad, H. Akbar, M. Afzaal, M. Zubair and F. Nasim, "Blockchain Technology The Future of Cybersecurity," 2023 24th International Arab Conference on Information Technology (ACIT), Ajman, United Arab Emirates, 2023, pp. 1-5, doi: 10.1109/ACIT58888.2023.10453839.
27. Imtiaz, D. Shehzad, F. Nasim, M. Afzaal, M. Rehman and A. Imran, "Analysis of Cybersecurity Measures for Detection, Prevention, and Misbehaviour of Social Systems," 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS), Abu Dhabi, United Arab Emirates, 2023, pp. 1-7, doi: 10.1109/SNAMS60348.2023.10375405.
28. Bilal, A., Sun, G., Mazhar, S., Imran, A., & Latif, J. (2022). A transfer learning and U-Net-based automatic detection of diabetic retinopathy from fundus images. Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization, 10(6), 663-674. Taylor & Francis.
29. Mahmood, T., Akhtar, F., Rehman, K. U., Azeem, M., Mudassir, A. I., & Daudpota, S. M. (2020). Introducing robustness in DBR routing protocol. International Journal of Communication Networks and Distributed Systems, 24(3), 316-338. Inderscience Publishers (IEL).