IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 11, November 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311170|

A Survey on Cloud Migration Security with Authentication and Access Control Techniques

J. Jayasudha[1], Dr. S.Arulselvarani[2]

Assistant Professor, Department of Computer Science, Research Scholar, Shrimati Indira Gandhi College, Trichy, India[1]

Assistant Professor, Department of Computer Science, UDC College, Trichy, India[2]

ABSTRACT: This paper provides an overview of the Cloud migration involves transferring applications, data, and other resources from on-premises environments to the cloud. This process introduces security risks, including unauthorized access and data breaches. Authentication and access control techniques play a vital role in enhancing cloud migration security. Cloud migration has gained significant traction in recent years as organizations seek to leverage the benefits of cloud computing. In the recent literature and provide a summary of related research work of key security risks and challenges specific to cloud migration. Potential threats, such as data leakage, service hijacking, insider attacks, and unauthorized data access. These results have the aim of providing useful insights for DNA cryptography authentication and access control, cloud migration is the process of transitioning an organization's data, applications, and other business elements from on-premises infrastructure to cloud-based services.

I. INTRODUCTION

The growing use of cloud computing has led to the growth of virtualized data centres as an efficient and low-cost platform on which to run business software. An increase in the deployment and utilisation of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) has been seen (SaaS). Users can deploy applications without providing their own server space, IT administration, or ownership of underlying hardware. Through an in-depth examination of each mechanism's strengths, weaknesses, and applicability, organizations can make informed decisions to tailor their access control strategies to meet their unique security requirements. By exploring the intricacies of Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Multi-Factor Authentication (MFA). DNA cryptography is a relatively novel and interdisciplinary field that explores the potential use of DNA (deoxyribonucleic acid) as a medium for secure communication and information storage. The idea behind DNA cryptography is to leverage the unique properties of DNA, such as its information storage capacity, durability, and molecular structure, to encode and protect sensitive information. It consists of four nucleotide bases: adenine (A), thymine (T), cytosine (C), and guanine (G). The sequence of these bases along a DNA strand carries genetic information. Each base can be represented using a binary code (A=00, T=01, C=10, G=11), allowing for the digital encoding of information. n DNA cryptography, information is encoded into DNA sequences using a predetermined mapping between binary data and DNA bases.

II. ROLE-BASED ACCESS CONTROL (RBAC)

Role-Based Access Control (RBAC) plays a crucial role in user authentication during cloud migration, ensuring that the right individuals have access to the appropriate resources and services in the cloud environment.

Benefits of RBAC

- Granular Access Control: RBAC allows administrators to define roles that correspond to specific job functions or responsibilities within the organization.
- Simplified User Management: RBAC simplifies user management by grouping users into roles and assigning permissions to these roles.
- Scalability: RBAC scales effectively as organizations grow and evolve. This scalability ensures that access control remains manageable and efficient, even as the organization expands.
- Enhanced Security: RBAC promotes the principle of least privilege, ensuring that users only have access to the resources necessary to fulfil their roles.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311170|

Attribute-Based Access Control (ABAC)

The ABAC mechanism refers to Attribute-Based Access Control, which is a method of restricting access to resources based on attributes associated with users and resources. ABAC evaluates a wide range of attributes to make access decisions. These attributes can include user roles, department, location, time of access, device used, and any other relevant characteristics.

Benefits of ABAC

Fine Grained Access Control

ABAC enables organizations to define access policies based on a wide range of attributes, such as user roles, department, location, time of access, device type, and more.

Integration with Identity Providers

During cloud migration, organizations may leverage identity providers (IdPs) such as Active Directory, LDAP, or SAML for authentication and user attribute management.

Compliance and Governance

ABAC facilitates compliance with regulatory requirements and internal governance policies during cloud migration.

Adoption of Zero Trust Architecture

ABAC, organizations can implement a Zero Trust approach to access control, verifying each access request based on the attributes of the user, device, and context before granting access to cloud resources.

Policy-Based Access Control (PBAC)

PBAC stands for Policy-Based Access Control, which is a method of access control that focuses on defining and enforcing access policies centrally rather than hard coding access rules into individual systems or applications.

Policy Definition:

PBAC, access control policies are defined based on the organization's requirements, regulatory compliance needs, and business rules. These policies specify who can access what resources under which conditions.

Policy Evaluation:

When a user attempts to access a resource, the access request is evaluated against the predefined access control policies.

Policy Enforcement:

The enforcement of access control request satisfies the conditions specified in the access control policies, access is granted, otherwise, access is denied.

III. BLOCK CHAIN TECHNOLOGY

Using block chain technology to secure DNA cryptography represents an innovative approach to enhancing the security and privacy of genetic data. DNA cryptography involves encoding sensitive information into DNA sequences, which are then stored or transmitted securely. Block chain can complement this process by providing a decentralized, tamper-proof ledger for managing access, ensuring data integrity, and facilitating secure transactions. Block chain enables fine-grained access control mechanisms, allowing users to specify who can access their genetic data and under what conditions. Smart contracts can be utilized to enforce access permissions and privacy preferences, ensuring that only authorized parties can decrypt and access the encoded DNA information. Block chain operates on a decentralized network of nodes, eliminating single points of failure and reducing the risk of data breaches or cyber attacks. Unlike traditional centralized cloud environments, where a breach in one central location can compromise the entire system, block chain-based cloud solutions distribute data across multiple nodes, making it more resilient to attacks and unauthorized access.

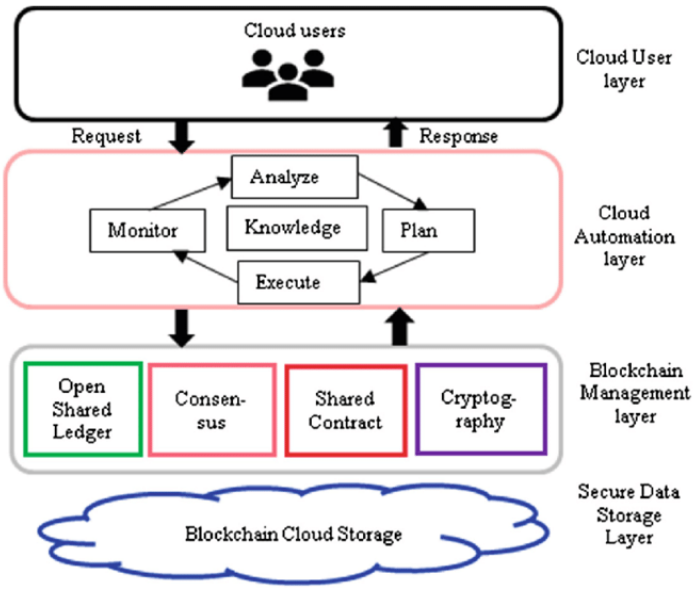
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311170|



IV. DNA CRYPTOGRAPHY

The idea behind DNA cryptography is to leverage the unique properties of DNA, such as its information storage capacity, durability, and molecular structure, to encode and protect sensitive information. It consists of four nucleotide bases: adenine (A), thymine (T), cytosine (C), and guanine (G). The sequence of these bases along a DNA strand carries genetic information. Each base can be represented using a binary code (A=00, T=01, C=10, G=11), allowing for the digital encoding of information. n DNA cryptography, information is encoded into DNA sequences using a predetermined mapping between binary data and DNA bases. This encoding process allows digital information to be translated into a biological form that can be synthesized and stored within a DNA molecule. NA cryptography aims to provide a secure means of storing and transmitting information. The unique biological nature of DNA, combined with the complexity of its sequence, can act as a form of encryption. Additionally, the use of advanced cryptographic techniques can enhance the security of DNA-encoded information. DNA cryptography, information is encoded into DNA sequences using a predetermined mapping between binary data and DNA bases. This encoding process allows digital information to be translated into a biological form that can be synthesized and stored within a DNA molecule. Potential applications of DNA cryptography include secure data storage, long-term archival of information, and secure communication in environments where traditional cryptographic methods may be impractical.

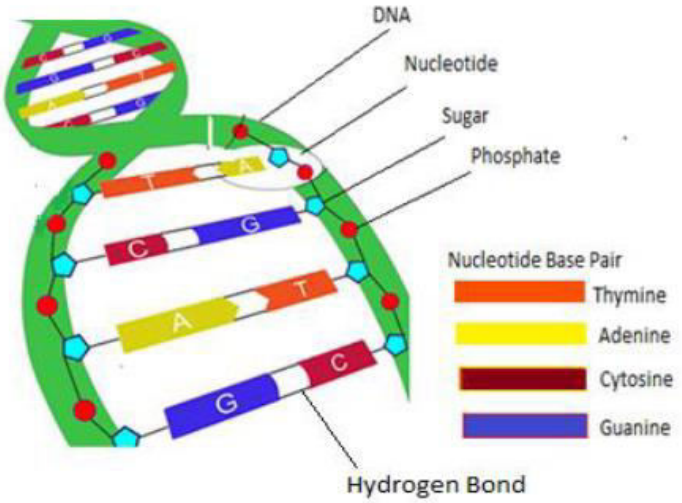
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311170|



DNA Structure	Binary Value
A	00
C	01
G	10
T	11

Identity and Access Management

- **Resource Access Control:** Identity and access management (IAM) will allows you to manage the permissions to the resources in the AWS cloud like users who can access particular service to which extent and also instead of maintain the permissions individually you can manage the permissions to group of users at a time.
- **Managing permissions:** For example of want to assign an permission to the user that he/her can only perform restart the instance task on AWS EC2 instance then you can do using AWS IAM.
- **Implementing role based accesscontrol:(RBAC):** Identity and Access Management(IAM) will helps you to manage the permissions based on roles Roles will helps to assign the permissions to the resources in the AWS like which resources can access the another resource according to the requirement.
- **Enabling single sign-on (SSO):** Identity and Access Management will helps you to maintain the same password and user name which will reduce the effort of remembering the different password.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

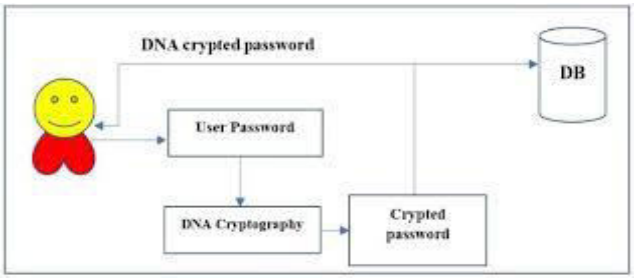
|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311170|

S.No	Alphabet	codon	S.No	Alphabet	Codon
1	A	CCA	14	N	TCT
2	B	GTT	15	O	CGG
3	C	TTG	16	P	ACA
4	D	GGT	17	Q	CAA
5	E	TTT	18	R	ACT
6	F	TCG	19	S	GCA
7	G	CGC	20	T	CTT
8	H	ATG	21	U	GTC
9	I	AGT	22	V	TCC
10	J	CGA	23	W	GCC
11	K	GAA	24	X	ATC
12	L	CGT	25	Y	AAA
13	M	CCT	26	Z	TCA

User Assigned Password Converted into DNA Crypted Password



V. CHALLENGES IN THE DNA CRYPTOGRAPHY

- DNA cryptography is a relatively new and interdisciplinary field that explores the potential of using DNA molecules for cryptographic purposes. While it holds promise for novel encryption techniques, there are several challenges associated with DNA cryptography
- DNA sequencing technologies are not error-free. The presence of errors in the sequencing process can result in the misinterpretation of the encoded information, leading to decryption errors.
- Handling DNA materials introduces biological hazards, and the use of DNA in cryptographic systems may raise safety and ethical concerns. There is a need for robust safety protocols to address potential risks associated with the manipulation and storage of biological materials.
- DNA-based operations may be slower compared to traditional cryptographic methods. The time required for encoding, decoding, and other operations involving DNA may limit the feasibility of certain applications, especially those requiring real-time processing.
- Scaling up DNA-based cryptographic systems for large-scale applications poses challenges. Managing the complexity and resources required for encoding, decoding, and storing vast amounts of information encoded in DNA could be a bottleneck.
- Integrating DNA cryptography with existing computational systems and technologies poses interoperability challenges.

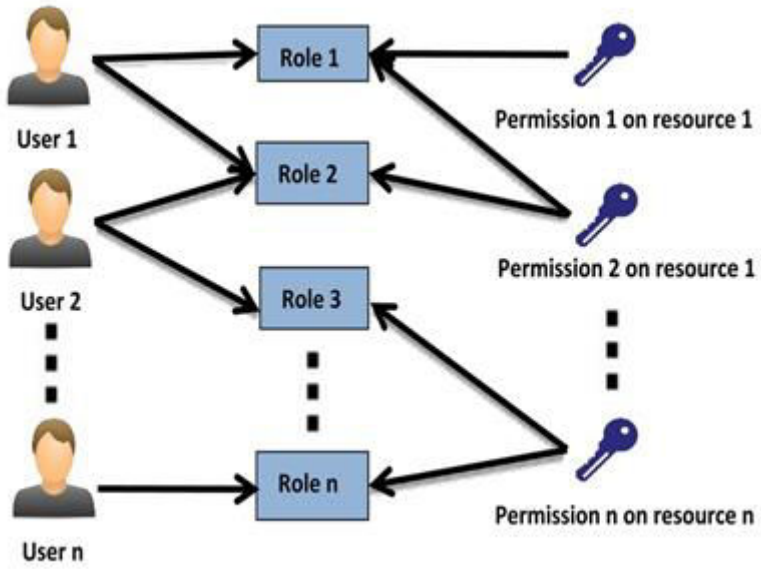
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311170|



VI. ROLE-BASED ACCESS CONTROL

Role-Based Access Control (RBAC) is a widely used mechanism in information security to manage access to resources based on the roles that users have within an organization. While RBAC is traditionally associated with computer systems and databases, its principles can be adapted to different domains, including DNA cryptography. Assign unique DNA sequences or markers to represent each role. These DNA sequences act as cryptographic keys associated with the roles.

The DNA sequences should be securely generated, stored, and distributed to individuals based on their assigned roles. When a user attempts to access encrypted data or perform a specific action, their DNA sequence is used for authentication. Establish access control policies based on roles. Define what actions each role is permitted to perform and what data they can access. Due to the potential for errors in DNA sequencing, the system should incorporate error-checking and correction mechanisms to ensure accurate authentication.

VII. CONCLUSION

Effective access control strategies are indispensable for ensuring the security, compliance, and performance of cloud deployments. By adopting a comprehensive approach that incorporates role-based access control, automation, continuous monitoring, and organizations can successfully navigate the complexities of cloud migration and achieve their strategic objectives while safeguarding their assets and data. DNA cryptography offers a high level of security, DNA cryptography and ensuring its seamless integration into the broader landscape of cloud security landscape.

REFERENCES

S.NO	Author Name	Title of the paper	Journal/Year	Review
1	Shirpa Jain	A novel DNA sequence dictionary method for securing data in DNA using spiral approach and framework of DNA cryptography	IEEE - August 01-02,2014	Spiral Transportation, Encryption time is minimum

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311170|

2	Shweta,Sanjeev Indora	CASCADED DNA CRYPTOGRAPHY AND STEGANOGRAPHY	IEEE-2015	MATLAB-PSNR & MSE, %bit changes are reduced (MSE)
3	Y.Pruthi,S.Dixit	A Dynamic DNA for Key-based Cryptography	IEEE -2018	DNA digital code is converted in to Unicode. Unicode to original
4	Awatef Balobaid, Debatosh Debnath	An Effective Approach to Cloud Migration for Small and Medium Enterprises	IEEEXplore-2020	Small to Medium Enterprise
5	Rubina Ghazal,Ahmad Karman Malik,NAuman Qadeer	Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments	IEEE Access, 2020	RBAC Framework
6	Anuj Kumar	Data Security and Privacy using DNA Cryptography and AES Method in Cloud Computing	IEEE-2021	DNA-based algorithm and the AES Algorithm
7	Choragudi Sasidhar and Dr. Sunita Gond	Security Techniques For Protecting Data In cloud Computing	IEEE Access, 2021	Protecting data
8	Ishu Gupta	Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments	IEEE Access,2022	Sharing Techniques
9	KaipingXue	Efficient and Secure Attribute-Based Access Control with Identical Sub-Policies Frequently Used in Cloud Storage.	IEEE Access,2022	ABAC Techniques
10	Aya Khaled Yousef Sayed Mohamed, Josef Kung	A systematic literature review for authorization and access control: definitions, strategies and models	Web Information system,2022	Access control techniques
11	Liang Yan	Access control scheme based on block chain and attribute -based searchable encryption in cloud environment, Springer Journal of Cloud Computing, 2023	Springer , 2023	Block chain technology

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details