ISSN: 0974-5823 Vol. 7 (Special Issue, Jan.-Mar. 2022)

International Journal of Mechanical Engineering

A Novel Framework for Secure Cloud behind Infrastructure as a Service (IaaS) : Performance and Reliability

[1]Krishna Saini, [2]Dr. Abid Hussain

[1]Research Scholar, School of Computer Application & Technology, Career Point University, Kota, Rajasthan

[2]Associate Professor, School of Computer Applications, Career Point University, Kota, Rajasthan

Abstract : With the age of Digitization and rapid growth in the IT companies , cloud services are in essential need. For providing the round the clock services and the stable services , we need the platform should also be stable and full proof. This created the need for the proper and secure Cloud Infrastructure Services and Secure User Validations and authentications. For this purpose we have suggested the Cloud Infrastructure and Role Based Concept for providing the secure and stable cloud services. In cloud-based data storage, securely authenticating users and securing the data with a Role-based access control system is a top priority. Image based authentication can securely govern this process and ensure that only authorized people can access the data.

***Index Terms*–Cloud Computing , Cloud Security ,Role Based Access, Iaas.**

I. INTRODUCTION

Moving organizations to the cloud first is important for the company to be able to transform at scale. This can arise a security storm since you cannot predict what will happen. Even if the default settings may satisfy a business operation, there is no guarantee. [1] The default settings for another public cloud example probably won't work for some organizations. Public mists offer nimbleness, yet it accompanies the potential for security gambles. [1]

A significant barricade to utilizing distributed computing is the gamble that it presents. Under 40% of organizations are getting full worth from their interests in the cloud. The key test is a deficiency in abilities and confusions emerging because of its intricacy. Notwithstanding security concerns, organizations find it challenging to accomplish the maximum capacity of their cloud ventures because of high expertise interest and deficient information about how best to contribute. [2]

Security has frequently been viewed as the greatest inhibitor to a cloud-first excursion — however as a general rule, it tends to be its most prominent gas pedal. [2]

Cloud security empowers better business results by being:

- For quick reaction time, use cloud administrations with local gas pedals to convey security in minutes or hours as opposed to months. With a supplier that considers security, you can profit from fast and secure sending in minutes or hours, rather than months. [2]
- Organizations are able to scale without adding headcount, which reduces the dependency on resources and manual steps.

- It’s important to come up with a safety plan before incidents happen. And the best way to be prepared is by coming up with defenses ahead of time. This means instead of trying to reactive malicious malware, you can avoid it before it happens by using proactive security. [2]
- Cost-effective: Computers can be programmed for security from the beginning, saving you the time wasted in having to redo work. [2]

Cloud security is crucial to organizations that want to protect their data for use in the cloud. Cloud security consists of policies, controls, procedures and technologies that allow you to protect cloud-based systems and infrastructure. The main goal of these is data protection. This allows users to effortlessly access resources as they need them while only paying for what they use.The cloud provides organizations with a variety of security risks. The latest AI-based tools are able to deal with these risks, as they are able to quickly provide the necessary security protocols. [3]

II. Securing using Role Based Access Control

III. Job based admittance control is a technique that awards clients fluctuating degrees of access in light of their jobs, to safeguard delicate information and guarantee representatives can get to data and perform activities they need to take care of their responsibilities. RBAC is many times utilized by enormous associations along these lines. An association can utilize job based admittance the executives to permit a client admittance to the framework and confine consents conceded through their assigned jobs. For instance, assuming you make a director, that singular will actually want to make or change documents, while furnishing somebody with a review consent to explicit assets. Jobs are relegated to a client relying upon their work or level of expert in the organization. [3]

Job based admittance control gives associations the capacity to reinforce their security pose and conform to guidelines. Albeit the execution of job based admittance will be testing, you can break this interaction into steps: [3]

• Assuming that you're thinking about changing your security consents to consider more access for a client, you ought to initially investigate what sort of need the client has that requires extra access. For the necessities examination, you ought to analyze work capabilities, business cycles, and innovation utilization notwithstanding any administrative or review prerequisites. [5]

• Arranging the extent of execution — distinguish the extent of your RBAC necessities, limited your concentration to frameworks or applications that store delicate information, and plan your execution as indicated by how the association oversees changes. [3]

• Characterizing jobs following the requirements examination will assist you with setting up jobs with the suitable degrees of granularity, keep away from cross-over and award consents all the more effectively. [3]

• Begin by carrying out your RBAC to a center gathering of clients. Ensure you start with coarse-grained admittance control prior to moving onto better grained control. Gather criticism from your clients and screen your current circumstance for things you want to remember while arranging future periods of execution. [3]

IV. Secure IAAS

Infrastructure-as-a-Service is a popular form of cloud computing. It provides the end user with access to basic compute, network, and storage resources on demand, over the internet, and on a pay-as-you-go basis. It allows users to scale and shrink their resources based on their immediate needs rather than keeping them running all the time without even using them. [4]

With the rise of many new technologies, traditional IaaS computing is in a much more crowded field than it previously was. Although IaaS remains foundational, it relies primarily on data center infrastructure that is shared with multiple workloads. [4]

IaaS are made up of different types of resources, giving users access to the resources for running applications and workloads in the cloud.

- Physical Data Centers: IaaS providers run physical data centres all around the world. The physical machines that power the multiple levels of abstraction on top of them can be made available through the internet, and most IaaS models don't require end users to interface with the equipment directly.

- Compute as a virtual computer with IaaS. Clients use compute to provide virtual instances with the computation and memory resources they require. For different sorts of workloads, IaaS companies often offer both CPUs and GPUs. Supporting services are also available from providers, which give the scalability and performance qualities that make cloud so appealing in the first place. [4]

- Through Software Defined Networking, traditional hardware can be made available programmatically through APIs. One example is Networking in the cloud. Multi-zone regions and virtual private clouds are also an example of advanced networking. [4]

- Storage : The three main types of cloud storage are block storage, file storage, and object storage. Each type of storage has its own set of pros and cons. Block and file storage can be hard to scale, but object storage is highly distributed, cost-effective, it scales linearly with the size of the cluster, and it’s accessible over HTTP. [4].

V. LITERATURE REVIEW

Aklamati et al. 2021 described that Cloud-based video surveillance systems are vulnerable to attacks by defining vulnerabilities, threats, and various attacks which can be employed to exploit these technologies. Similar to how they described the security of these systems, they also proposed a taxonomy of attacks which an attacker could employ when attacking cloud-based video surveillance systems. They then used their AWS environment where they were able to eavesdrop on video camera feeds. They then implemented various related attacks in order to test the efficient defense mechanism against unauthorized IP access and other protocols. Authors hope that their work will serve as a reference for cyber security research and practitioners who wish to conduct research on this field. [5]

Researchers Kumar, P. et al. (2021) shows in their paper that cloud computing is not only used for data storage but also to provide access to different software and services. IT companies rely on it because it is easy to scale up and down; however, the benefits of cloud computing stem from the pay-per-use services through providers and its usage facilities, requiring no maintenance or upgrades. Furthering these benefits, cloud computing analyzes an analytical comparative assessment of the two service models: Infrastructure-as-a-Service and Platform-as-a-Service without any parameters or descriptions. [6] Li et al., (2021) argues that blockchain is a new and promising paradigm of decentralized data. The data integrity and capabilities with unrestricted transactions makes it an ideal candidate for designing a cloud-based, distributed trust architecture. [7] In 2021, Lu et al. created a project management device for students that managed both PaaS and IaaS services to reduce administrator maintenance. They also provided container management, image management, and other key functions for teaching/teaching requests. [8] Sun, X., et al. (2021) stated that Three mechanisms are proposed for allocating resources to various classes of customers: a best-effort service, a differentiated service, and a guaranteed minimum rate. Allocating by manipulating two parameters (a minimum rate

guarantee and utility weight) provides the desired quality of service or rate allocation for a given flow. PACCP supports both large scale simulation and small testbed implementation which has been verified with real datacenter workloads. The results demonstrate that PACCP provides fair rate allocation. [9]

Umamaheswari and Shobana (2021) propose a defensible, role-based case management system that can be used for remote investigations. The novel system aims to provide a process in which data collection, data preservation and analysis can occur without disrupting regular operations. Along with a virtual machine snapshot for crime scene recreation and cloud forensics, the proposed system is tested against state-of-the art systems, presenting a more efficient case management system. [10] Belkhiria, H., (2020) With Structured Lighting, there is a need for proper security access. RBAC, or Role Based Access Control, is an efficient way to meet authorization needs. In order for RBAC to be executed successfully, third party evaluators must properly evaluate different requests and determine user authorization levels. The paper will show how RBAC can better satisfy needs of device users as well as improve performance across multiple devices. [11] Kim et al. (2020) used Role-Based Access Control with Mandatory Access Control to increase the security of their data. This has been cited three times and they suggest ways their approach could be more impactful. Thakare et al (2020) proposed a model to manage scheduling in an organization and efficiently compare it's potential pros and cons by using other models of management. [12]

Sanjay Kumar et al. (2020) suggested that the Cloud based Computing is a widely adopted technology prevalent in the present IT scene. Organizations store data across the world in heavily dispersed and networked environments. There are many benefits to these new technologies, one being that they allow users to access resources in the way they need them and at the time they need them. However, identification methods and authentication must be rigorously carried out to avoid security breaches. The authors of this report on security challenges faced in the cloud have introduced a new advanced 2-factor authentication, which will be exponential for both usability and for detecting phishing threats. Added features include AES encryption, admin verification, and encryption/decryption based on different tiers, which is exponential for both usability and as an added defence against phishing attacks. [13]

V. Proposed Concept

The proposed model is governed with the following diagram, as shown in the fig 5.1

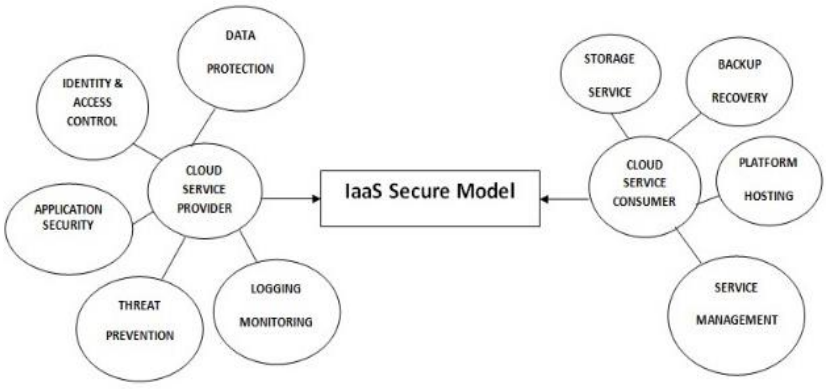

Fig 5.1 Novel Framework for Secure Cloud Behind IaaS

The concept of blockchain is also used. Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain contains all the transactions that have ever occurred and can be accessed by many different people. Whenever a new transaction occurs, it is recorded to every copy of the ledger, effectively creating a shared database of information. This technology is

know as Distributed Ledger Technology. So if one block in a chain had been tampered with, it would be immediately known. If hackers wanted to corrupt a blockchain system, they would have to change every block across all of the versions of the distributed chain. The Role-Based Access Control means that credentials are related to a certain group and have rights corresponding to those of other users in that group. They are managed with the ZigZag Image Authentication. With the cloud growing, security is now a top concern. With the role-based access control, the data can only be communicated to those with the correct credentials. An additional security measure is a graphical authentication to ensure that only those with appropriate or proper access are given information on private subjects.

We created a new end-to-end encryption technique for the app by putting a person's mobile number and their IMEI on the same page to form an image pattern. For example, using the grid of the images, you can use 5x4, which allows for more variety to cater to a larger size screen on mobile devices. The app will analyze the selected images and then extract the IMEI number for validation. The last two digits of the IMEI number are combined with characters from each image's SHA-512 code to generate a pattern, which is sorted in the database.

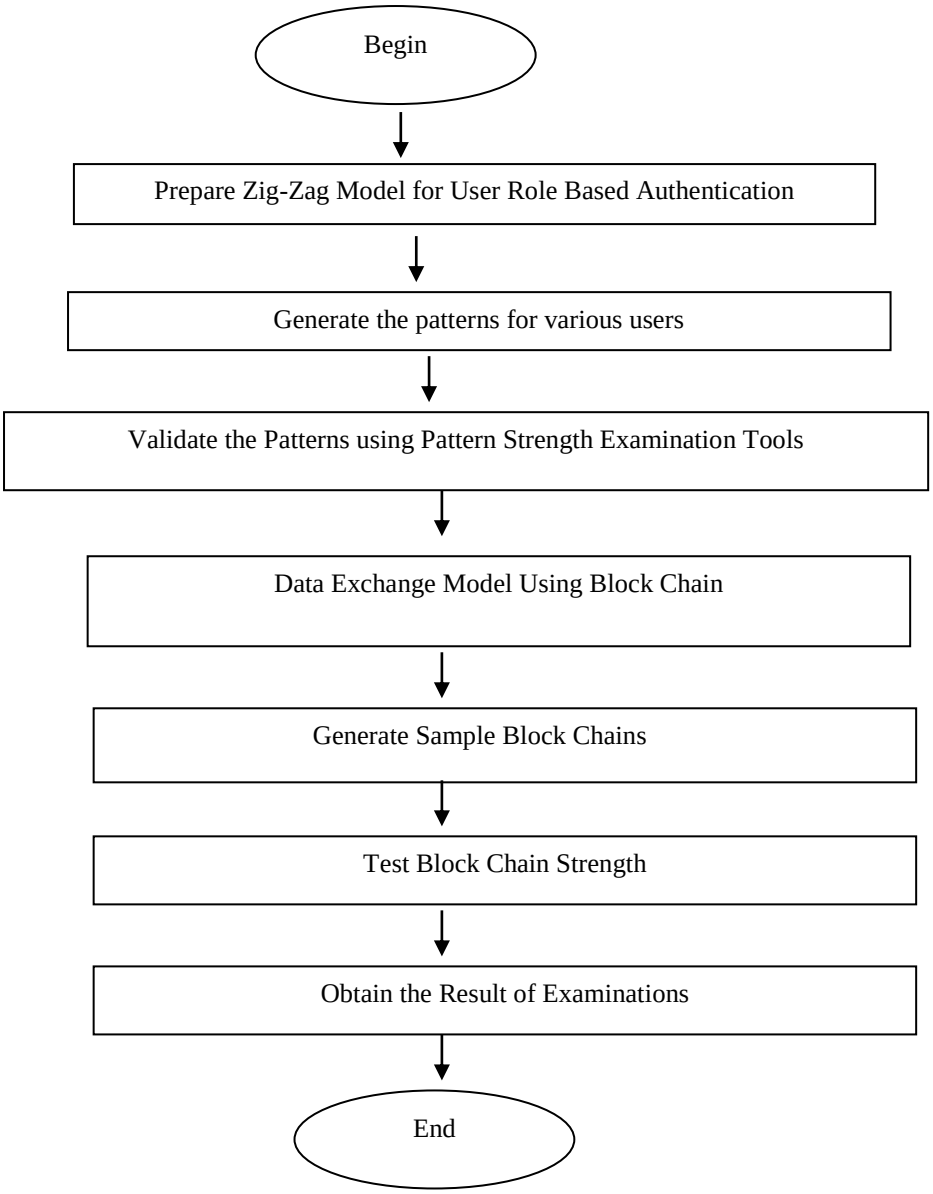

Fig 5.2 Blockchain based Data Security

We would like the new user to register with us. In order to do this we will take a grid pattern and draw it on a screen and segment the Picture into these segments. Once the Pictures are drawn in their corresponding positions, they form an Picture of the shape that was desired in the grid,

Picture(PictureNumber)_part(partnumber1)_sizeofPicture_Picture(PictureNumber)_part(partnumber2)_sizeof Picture_

::::

Picture(PictureNumber)_part(partnumberN)_sizeofPicture_

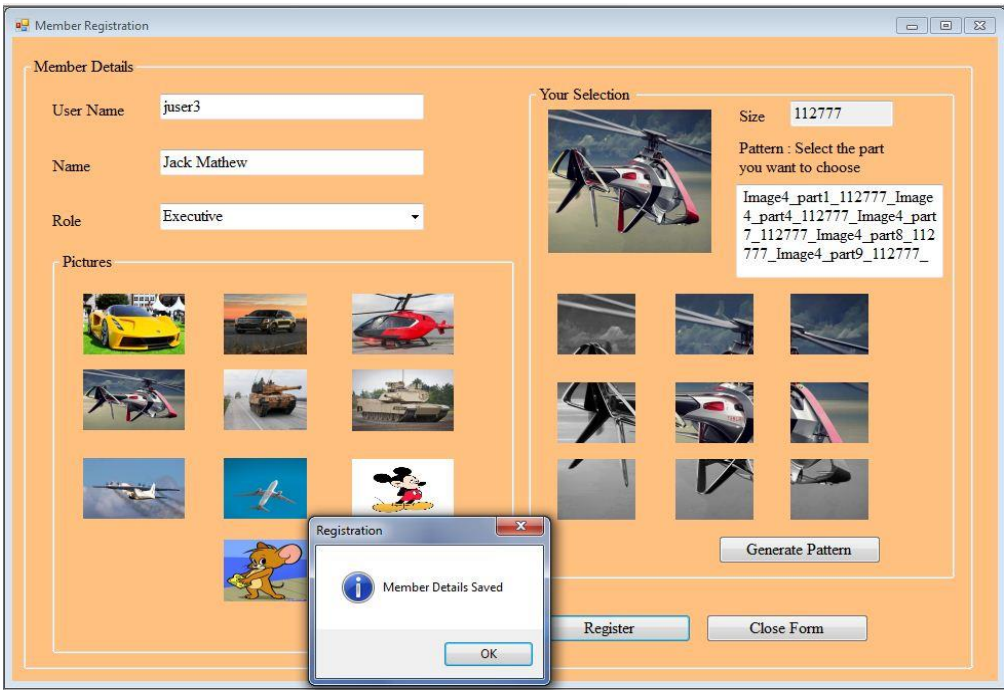

Fig 5.3 Registering Users of Cloud Services

VI. Result Analysis

6.1 Device 1: Rumkin Test

A first use of this secret word checker is to evaluate the quality of your secret phrase, given any letters that are higher than the others in frequency and considering the likelihood of letters being typed after each other. If your score is usually low, your secret key may not be as 'secret' as you think it is.

Authentication Key:

Picture4_part1_112777_Picture4_part4_112777_Picture4_part7_112777_Picture4_part8_112777_Picture4_part9_112777_

Access Key:

e127ea23e40121c0186fB0BE79A29AB851C21553

Base Paper ,Sankaj Kumar , et.al 2020 makes use of access key as based on AES 10 round key e.g

28FBBEG86DA4244BCCC0A4FF3B346F26

Table 6.1 Analysis of Keys Test 1

	Authentication Key	Access Key
Proposed Approach	508.2	168.8

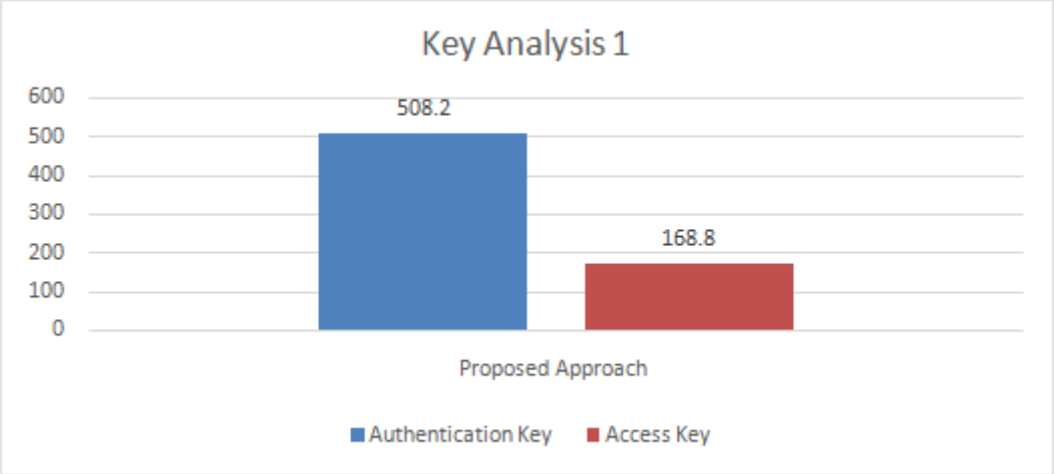

Fig 6.1 Key Analysis 1 Graph

Table 5.2 Analysis of Keys Test 1 Base Key

	Access Key
Base Paper Sankaj Kumar , et.al 2020	127 bits

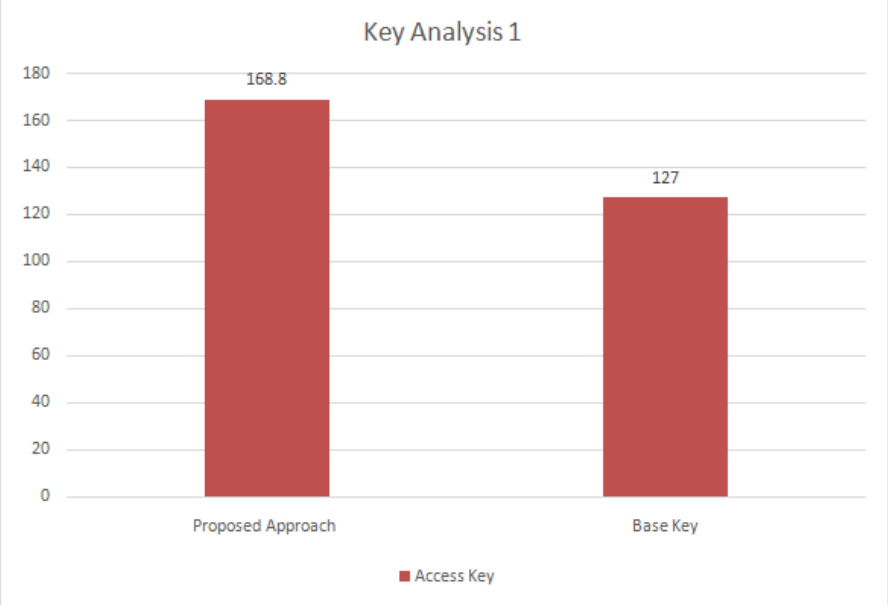

Fig 6.3 Key Analysis 1 Base and Proposed Graph

6.2 Device 2: zxcvbn Test

This is a secret word meter that measures entropy by using zxcvbn by Dropbox. It tests for words like reference words, leet-talk, etc. which can deduce the entropy accurately.

Generators will not secure your account if you use the generated information as a password. Many utilities will not assess complexity and irregularities in passwords because it is difficult to visually decrypt them.

Table 5.3 Analysis of Keys Test 2

	Authentication Key	Access Key
Proposed Approach	320	131

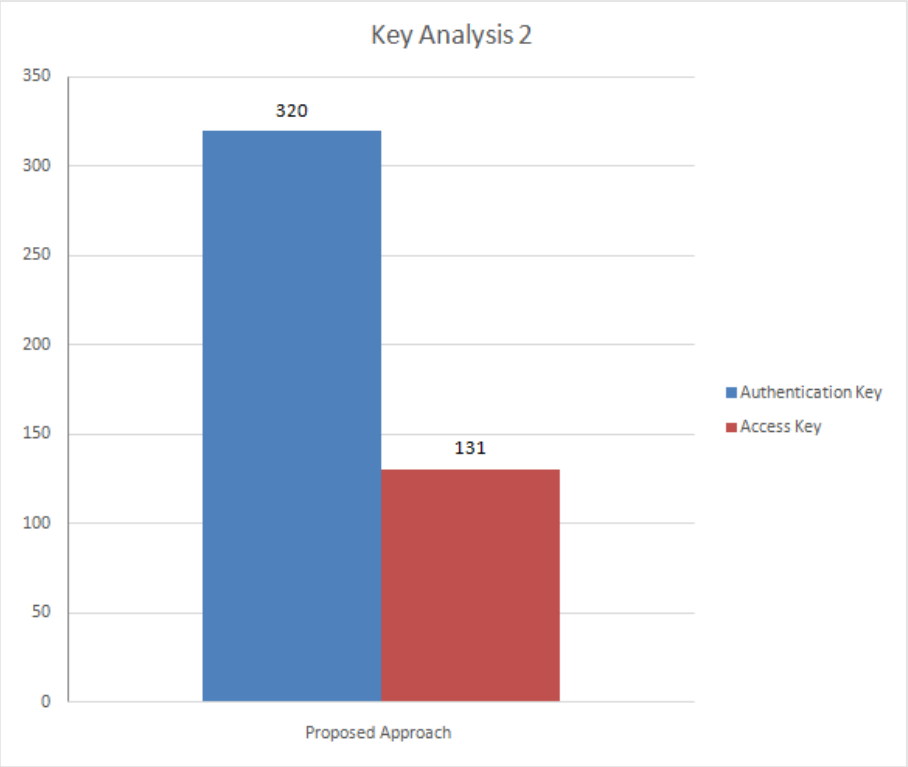

Fig 6.4 Key Analysis 2 Graph

Table 5.4 Analysis of Keys Test 2 Base Key

	Access Key
Base Paper Sankaj Kumar , et.al 2020	104

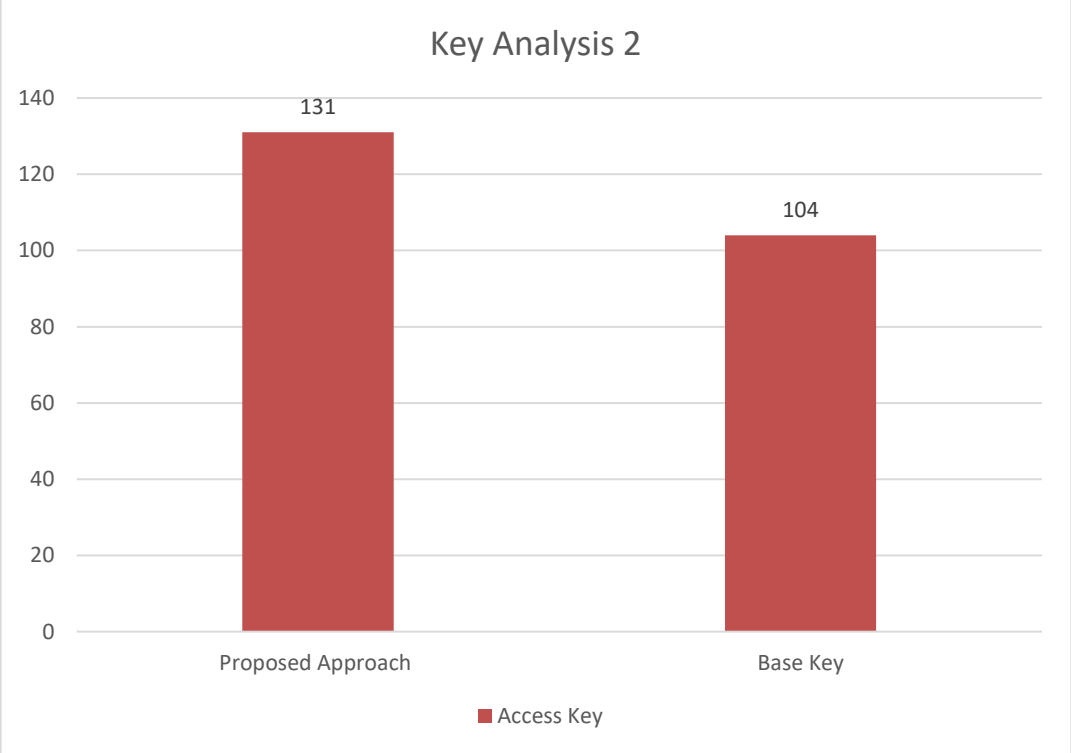

Fig 6.5 Key Analysis 2 Base and Proposed Graph

VII. CONCLUSION

Securing data in the cloud environment is a difficult task. As this information is shared on the server, it requires that the user to be authenticated and also secure. With the growth of cloud data, there is a need to secure information that is communicated. At this time, we are working on role-based access control, which determines what the user can view by specifying their role. We also have a graphical way to authenticate users with an innovative combination of sliding. We used Zig-Zag Image-based authentication to manage access and authentication of users. With the comparison with the existing approaches , the cloud security suggested found to be more secure.

REFERENCES

1. Ma, Y., Ni, H.- J. furthermore, Li, Y. (2021) "Data security practice of canny information biological networks with distributed computing," in 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE). IEEE, pp. 242-245.
2. Montero, R. S. (2012) "Building IaaS Clouds and the specialty of virtual machine the executives," in 2012 International Conference on High Performance Computing and Simulation (HPCS). IEEE, pp. 573-573.
3. Na, S.- H., Park, J.- Y. what's more, Huh, E.- N. (2010) "Individual distributed computing security structure," in 2010 IEEE Asia-Pacific Services Computing Conference. IEEE, pp. 671-675.
4. Nandina, V. et al. (2014) "Provisioning security and execution streamlining for dynamic cloud conditions," in 2014 IEEE seventh International Conference on Cloud Computing. IEEE, pp. 979-981.
5. Abuhussein, A., Bedi, H. furthermore, Shiva, S. (2013) "Towards a partner situated taxonomical methodology for secure distributed computing," in 2013 IEEE Sixth International Conference on Cloud Computing. IEEE, pp. 958-959
6. Kumar, P. et al. (2021) "An Analytical Evaluation of Cloud Computing Service model IaaS and PaaS utilizing Market Prospective," in 2021 International Conference on Technological Advancements and Innovations (ICTAI). IEEE, pp. 537-540.

7. Li, W. et al. (2021) "Blockchain-based trust the executives in distributed computing frameworks: a scientific categorization, survey and future bearings," Journal of Cloud Computing Advances Systems and Applications, 10(1). doi: 10.1186/s13677-021-00247-5.
8. Lu, X. et al. (2021) "Plan and development of code facilitating stage in light of distributed computing," in 2021 International Conference on Intelligent Computing, Automation and Applications (ICAA). IEEE, pp. 677-681.
9. Sun, X. et al. (2021) "A cost mindful blockage control convention for cloud administrations," Journal of Cloud Computing Advances Systems and Applications, 10(1). doi: 10.1186/s13677-021-00271-5.
10. Umamaheswari, K. furthermore, Shobana, G. (2021) "A solid job based case the board framework for distant legal examination," in 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). IEEE, pp. 232-238.
11. Belkhiria, H., Fakhfakh, F. also, Rodriguez, I. B. (2020) "Settling multi-client clashes in a brilliant structure utilizing RBAC," in 2020 IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). IEEE, pp. 181-186.
12. Kim, D.- K., Ming, H. also, Lu, L. (2020) "Reflection on building mixture access control by arranging RBAC and MAC highlights," in 2020 IEEE 27th International Conference on Software Analysis, Evolution and Reengineering (SANER). IEEE, pp. 522-526.
13. Sanjay Kumar, Syed Akbar Abbas Jafri, NishitArun Nigam, Nakshatra Gupta, Gagan Gupta1 and S K Singh,"A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing",IOP Conf. Ser.: Mater. Sci. Eng. ,2020