



# **FOGAUTH: An Efficient Authentication and Key Management Framework for Cloud Security**

**B. Sujith Kumar, R. Viswanathudu, C. Irfan, S. Subhahan Ali**

Lecturer, Department of Computer Science, Loyola Degree College (YSRR), Pulivendula, AP, India

U.G Student, Department of Computer Science, Loyola Degree College (YSRR), Pulivendula, AP, India

U.G Student, Department of Computer Science, Loyola Degree College (YSRR), Pulivendula, AP, India

U.G Student, Department of Computer Science, Loyola Degree College (YSRR), Pulivendula, AP, India

**ABSTRACT:** The rapid growth of internet devices creates a major need for very fast data sharing. However, old cloud systems use one main server, which makes them too slow to handle the quick speed needed for modern smart applications. Old cloud networks are too slow and cannot provide the fast data sharing those modern applications require. Also, current systems cannot check if users in fog networks are real or fake. To keep the network safe, the new system checks the identity of every user and fog server across three levels: the main cloud, the fog nodes, and the device teams. When a device or fog server registers with the main cloud, it gets a special, unique ID number.

**KEYWORDS:** Fog Computing, Cloud Security, Key Management, Mutual Authentication

## **I. INTRODUCTION**

The fast growth of smart devices creates a big need for instant data sharing, but old cloud setups with one central server are too slow to do this well. Traditional centralized cloud computing setups face significant challenges in achieving the rapid and efficient communication required by modern smart applications.

The main purpose of this network framework is to build a quick and secure method for connected smart devices to check identities and exchange secret keys.

## **II. LITERATURE SURVEY**

Decentralized environments require robust frameworks for efficient asset management, a concept extensively evaluated by Petri et al. [1] through the lens of dynamic broker emergence within social cloud topologies. Their methodology demonstrates that orchestrated broker coordination effectively streamlines resource distribution across geographically dispersed participants, offering a viable architectural alternative for managing dense, decentralized node setups. Similarly, analyzing public infrastructure capabilities remains crucial; Li et al. [2] introduced CloudCmp, a sophisticated benchmarking suite designed to evaluate performance variance across major cloud vendors. While standard execution threads showed high competency across standard workloads, data-heavy pipelines exhibited distinct performance degradation tied closely to specific provider infrastructure, allowing the authors to accurately map service quality using targeted latency and throughput matrices.

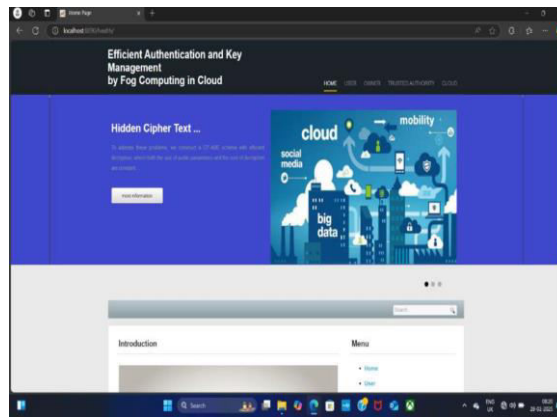
Complementing these cloud evaluation models, Lenk et al. [3] focused on standardizing performance benchmarks specifically for Infrastructure-as-a-Service (IaaS) configurations. Their framework systematically charts system execution metrics against corresponding operational expenditures to determine overall commercial viability. The analytical outcomes indicate that conventional virtual instances frequently suffer from operational inconsistency when subjected to high-intensity computational stress. Consequently, this volatility highlights the critical importance of embedding stringent, continuous monitoring protocols within contemporary enterprise cloud strategies to guarantee sustained reliability.

### III. METHODOLOGY

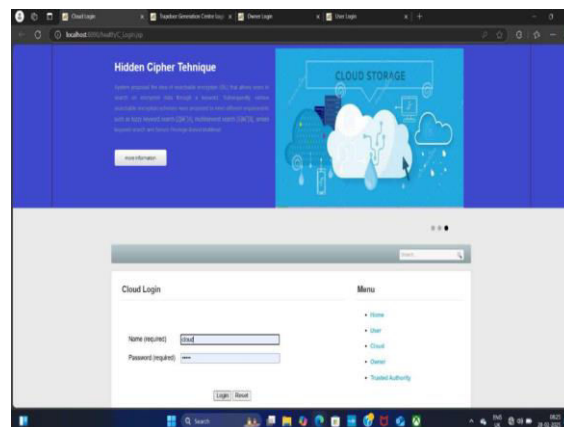
A hybrid security design combining Elliptic Curve Cryptography (ECC) and Lightweight Mutual Authentication enhances data protection from the edge to the cloud. Additionally, Dynamic Key Agreement Protocols analyze session requests in real time to prevent unauthorized access and stop communication leaks. By organizing fog nodes into a hierarchical network, the system handles heavy traffic smoothly, reducing processing delays and server strain. Security and system speed improve significantly when multiple optimization factors are handled together Computation Cost, Storage Space, and Data Transmission Speed.

### IV. EXPERIMENTAL RESULT

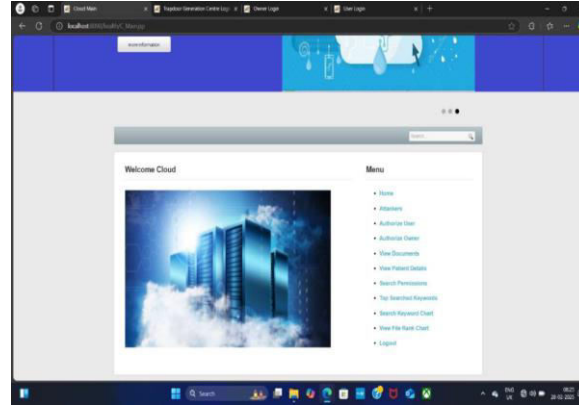
Figures shows that a Home page of frontend. Fig 1(a) Shows home page. (b) Shows Cloud Login. (c) Shows Cloud Dash Board.



(a)

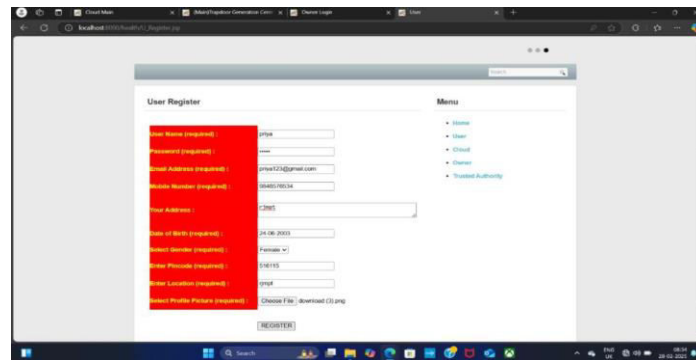


(b)

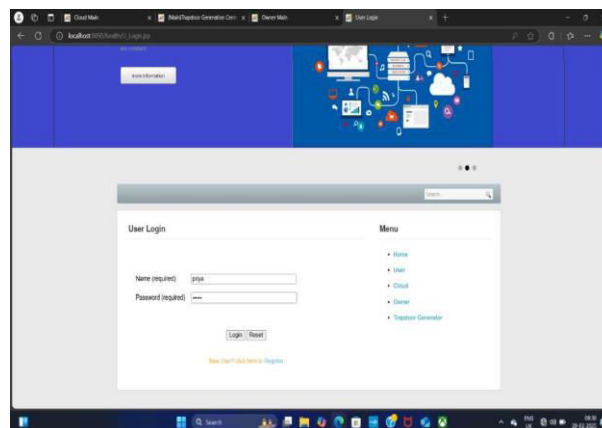


(c)

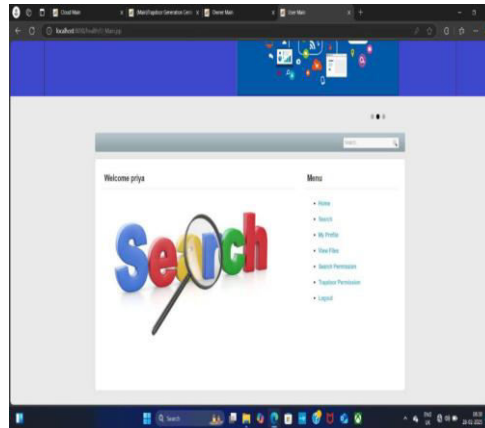
Fig.2. Shows User Registration process (a) Shows User registration. (b) Shows User Login. (c) Shows User Dash Board.



(a)

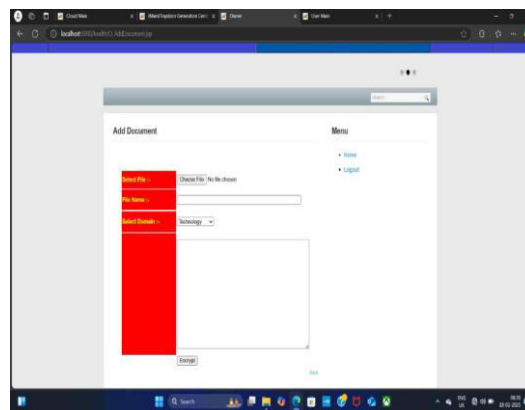


(b)

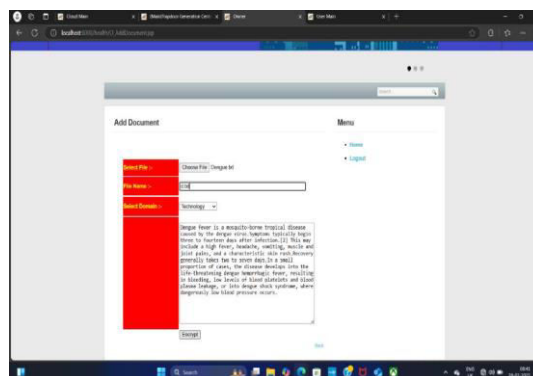


(a)

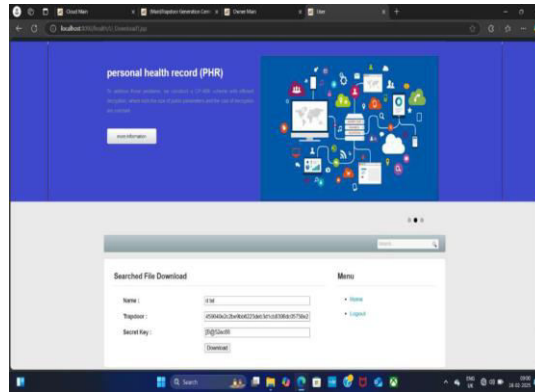
Fig.3. Shows User uploading a file and encryption of file. (a) Shows User Uploading a file and text. (b) Shows a file ready to encrypt. (c) User have to give Security code to get the required file.



(a)



(b)



(c)

Fig .4Shows User reuired file after giving the security key

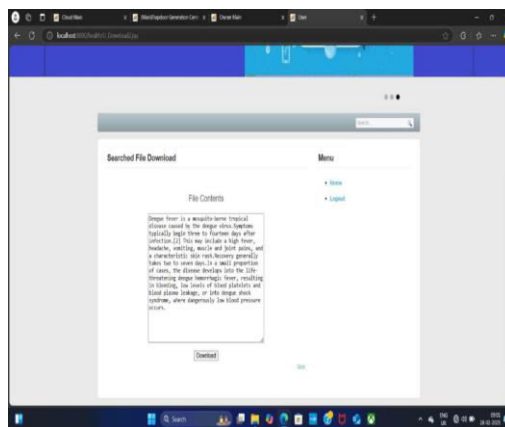


Fig.4

## V. CONCLUSION

In conclusion This paper introduced a highly secure login and private key management system that runs on decentralized fog computing methods. The main goal of this project is to protect shared information and verify the identities of users very quickly and with excellent accuracy.

By shifting the heavy workload from central cloud servers to local fog nodes, the system eliminates slow delays and cuts down communication traffic significantly. The strong security protocols and encryption steps built into this architecture help regular cloud users, network service companies, and smart digital industries keep their confidential files safe from online hackers

## REFERENCES

- [1] I. Petri, M. Pun Ceva, and O. F. Rana, “Broker emergence in social clouds,” 2013 6th International Conference on Cloud Computing, pp. 669–676, 2013.
- [2] A. Li, X. Yang, S. Kandula, and M. Zhang, “CloudCmp: comparing public cloud providers,” in IMC ’10: Proceedings of the 10th ACM SIGCOMM conference on Internet measurement. New York, New York, USA: ACM Press, 2010, pp. 1–14.
- [3] A. Lenk, M. Menzel, J. Lipsky, S. Tai, and P. Offermann, “What are you paying for? performance benchmarking for Infrastructure-as a-Service offerings,” in 2011 IEEE International Conference on Cloud Computing (CLOUD), 2011, pp. 484–491.



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details