

**DESIGN OF THE ATTRIBUTE ORIENTED KEY POLICY FOR THE  
DECENTRALIZATION BASED PRESERVING PRIVACY****Zareena Begum<sup>1</sup>, D.Jamuna<sup>2</sup>**<sup>1</sup>M.Tech Student, Dept of CSE, Jaya Prakash Narayan College of Engineering, Mahabubnagar, A.P, India<sup>2</sup>Professor, Dept of IT, Jaya Prakash Narayan College of Engineering, Mahabubnagar, A.P, India**ABSTRACT:**

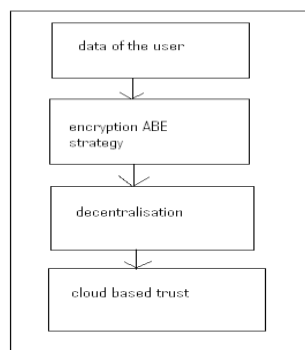
Here an implementation of the system with respect to the scheme of the scenario related to the structural aspect of the ABE based multi authority plays a crucial role In the system based aspect with respect to the strategy of the variant encryption of the attributes well oriented with the strategy of the decentralization plays a crucial role in the system based analysis in a well oriented fashion respectively. Here in the present system related strategy there is an independent user based keys of the secrete issue depending on the authority of the user without the help of the central cooperation respectively. Here the authorities well oriented with the multiple phenomena depending on the interactive system well acquainted with the help of the setup based online authority plays a crucial role in the system based analysis point of view respectively. Here for the purpose of the well accurate design oriented with respect to the system a new scheme is implemented by the name of the ABE plays a crucial role for the effective and efficient decentralization based implementation followed by the well accurate analysis point of view respectively. Here by the implementation of the present system oriented strategy in a well accurate manner there the entire computational cost of the system is completely reduced followed by the complexity is completely nullified respectively. Simulations have been conducted on the present method where the experiments have been conducted on the large number of the datasets in an unknown environment in a well oriented fashion and with respect to the unknown environments in a well oriented scenario respectively.

**Keywords:** *Preservation of the privacy, Data encryption, Extraction of the attributes, Decentralization, Preservation of the privacy and Multi authority based consideration respectively.*

## 1. INTRODUCTION:

Here the schemes related to the control of the access of the strategy related to the authority of the central phenomena for the access of the of the user based control of the data oriented with respect to the sensitivity plays a crucial role in the system in its analysis point of view respectively [1][2]. There is a lot of research takes place in the system in the schemes oriented with respect to the strategies of the control based access and its drawbacks and its analysis in a well oriented fashion respectively.

## BLOCK DIAGRAM



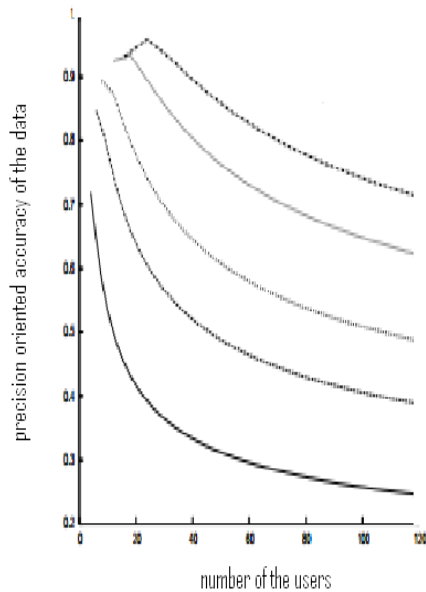
**Fig 1: Shows the block diagram of the present method respectively**

## 2. METHODOLOGY

In this paper a method is designed with a well efficient framework where it is implemented mainly for the purpose of the study of the problems related to the several recent methods which is failed in terms of the outcome based strategy and also the complete degradation of the performance respectively. Here the present designed method is shown in the below figure in the form of the block diagram and which explains in the brief elaborative fashion respectively [3]. Here there is a huge challenge for the present method where it is supposed to accurately analyze the problems related to the several previous methods and also the theoretical aspects related o this particular strategy in order for the controlled degraded performance abase strategy in a well efficient manner [4][5][6]. Here we finally conclude that the present designed method completely overcome the drawback of the several previous methods in a well efficient manner followed by the performance based strategy and also the

entire outcome of the system based aspect respectively [7][8].

### 3. EXPECTED RESULTS



**Fig 2: Shows the graphical representation of the present method respectively**

A comparative analysis is made between the present technique to that of the several previous technique is shown in the below figure in the form of the graphical representation and also explains in the brief elaborative fashion respectively. A lot of analysis is made between the present method and a huge number of the computations have been applied on the large number of the data sets in a well effective fashion for the entire system based outcome aspect. Here we

finally conclude that the present method is effective and efficient in terms of the performance based strategy followed by the efficient outcome in a well oriented fashion.

### 4. CONCLUSION

Here in this paper a method is designed with a perfect framework where there is an accurate analysis takes place in the system where there is an improvement in the performance followed by the outcome of the entire system in a stipulated fashion respectively. In the present method of the analysis there is an implementation of the scheme related to the well acquainted fashion in the terms of the ABE decentralization plays a crucial role and there is a huge amount of the attention for the well effective implementation of the system for the well efficient reduction of the trust related to the authority of the single centralized strategy in a well efficient manner respectively. Here there are a large amount of the problems to be faced by the present implemented system in the form of the attacks therefore a decentralization strategy has to be designed in a well oriented fashion for the accurate strategy of the encryption plays a crucial role for the trust of the user is its major theme of the system

in a well acquainted fashion respectively. Here we finally conclude that the present method is effective and efficient in terms of the improvement in the performance followed by the outcome of the entire system in a well stipulated fashion respectively.

## REFERENCES

- [1] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Theory of Cryptography Conf. (TCC '07), S.P. Vadhan, ed., pp. 515- 534, Feb. 2007.
- [2] S. Müller, S. Katzenbeisser, and C. Eckert, "Distributed Attribute-Based Encryption," Proc. 11th Int'l Conf. Information Security and Cryptology (ICISC '08), P.J. Lee and J.H. Cheon, eds., pp. 20-36, Dec. 2008.
- [3] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure Threshold Multi- Authority Attribute Based Encryption without a Central Authority," INDOCRYPT '08: Proc. Int'l Conf. Cryptology in India, D.R. Chowdhury, V. Rijmen, and A. Das, eds., pp. 426-436, Dec. 2008.
- [4] A. Lewko and B. Waters, "Decentralizing Attribute – Based Encryption," EUROCRYPT '11: Proc. 30th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology, K.G. Paterson, ed., pp. 568-588, May 2011.
- [5] J. Li, Q. Huang, X. Chen, S.S.M. Chow, D.S. Wong, and D. Xie, "Multi-Authority Ciphertext-Policy Attribute-Based Encryption with Accountability," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '11), pp. 386-390, 2011.
- [6] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," CRYPTO '01: Proc. Advances in Cryptology, J. Kilian, ed., pp. 213-229, Aug. 2001.
- [7] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," CRYPTO '84: Proc. Advances in Cryptology, G.R. Blakley and D. Chaum, eds., pp. 47-53, Aug. 1985.
- [8] C. Gentry, "Practical Identity-Based Encryption without Random Oracles," EUROCRYPT '06: Proc. Advances in Cryptology, S. Vaudenay, ed., pp. 445-464, May/June 2006.