Securing Fog Storage Nodes using an Attribute-based Encryption Scheme and Multi-Factor Authentication

J.Velmurugan, S.Manjula

Abstract - Fog computing is an extended and distributed infrastructure where the application processes are managed between the end devices and the edge of the grouped system for better and reliable services. Fog computing is a non-insignificant augmentation of cloud which comes in to the same security and production difficulties of cloud computing. Existing conventional techniques like digital certificates and signature verification schemes suffers due to the advancement of cyber criminals in revoking the certificates. To enable authentication and confidentiality among a group of gathered fog nodes, in this paper, a novel CP-ABE based scheme along with multi-factor user authentication (CP-ABE-MA) is proposed. Further, the paper uses some obfuscation technique which obscures the data to evade the illegal user access. In general, the cloud is a RAW data type which consists of any data format, hence respective on the data type the encryption conversion can be used. CP-ABE can be connected to letters in order and alphanumeric sort of information and jumbling can be connected to a numeric kind of information. Applying encryption methods on the cloud information will give more security against unapproved use. Privacy could be accomplished with a blend of encryption and confusion. In order to evaluate the efficiency, the proposed protocol is implemented and tested in AVISPA and compared with the certificate-based schemes. Further, the proposed protocol outflanks the existing certificate based schemes with 97% accuracy.

Keywords: Fog computing, CP-ABE, CP-ABE-MA, Multifactor Authentication, AVISPA

I. INTRODUCTION

Fog is the need to end horizon computing widely used to distribute the services such as compute, storage, network which is closer to the user as well as to the cloud end points. Recent advancement in Cloudification of internet connected gadgets leads the opinion of centralized cloud services are not capable to provide the satisfactory administrations to the end user [11]. On the other hand the fog computing is efficient enough to handle the services from the end user by distributing the centralized workloads over a wide range of geographical locations [14]. Hence fog computing plays a promising function in the technologies such as IoT, IoE, CPS etc., by providing the better services and support in all the conditions. The fog is associated to the cloud which provides the maximum computing services to the fog devices such as Access point, home gateway, fog routers etc.,. However, the potential security issues available in the cloud platform is also present in the Fog computing [12].

Revised Manuscript Received on October 05, 2019
J.Velmurugan*, Department of Information Technology,
Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai, India.
Affiliated to Anna University, Chennai, [E-mail:vel.jme@gmail.com]
S.Manjula, Department of Electronics and Communication Engineering
Rajalakshmi Institute of Technology

When ever the IoT smart devices trying to communicate or share any data or services with the other devices which is connected to the cloud. In general, all the smart devices are power constrained due to its limited battery backup [15]. Whereas the cloud resources are having an unlimited backup and resources with high processing capabilities. The recent advancement in the technologies also pave a pathway towards development of cloud technologies in terms of scalability, accessibility, high availability etc.,[13]. But when the case comes to the internet connected devices which is directly connected to the Fog devices, the resources are very limited and require a massive burden of limited resource constrain [10]. For example, an IoT devices require a low latency, fast and reliable data access with high data transfer rate along with mobility support [8]. To achieve this with the security as the major concern it is very hard for the technologies like Fog. Hence to address this issue, a novel CP-ABE based scheme along with multi-factor user authentication is proposed.

Cipher text - Attribute Based Encryption (CP-ABE) is a generic one to many encryption scheme widely used in the IoT devices for attribute level encryption. The robust characteristics of CP-ABE scheme is that it enables an access control from the encrypted data by defining the various access policies for each attributes which a devices is about to transfer to the Fog end points. Further, it gives a clear insight about the data owner to the user who is in need to possess and decrypt the encrypted ciphers. By applying this approach the major concern in cryptography has been addressed [4-6].

The existing CP-ABE techniques as given in [1-3] presents the insight and overview of the scheme and accountability about the CP-ABE scheme has been elaborated in [7][14]. From the observation, it is clear that the practical possibility of using the CP-ABE is much better to secure the end point devices which are associated to Fog end points. In order to enhance the security mechanism among the user policies, the proposed method incorporates the multi factor authentication mechanism to achieve better security and additional security[9][21]. By applying the proposed scheme CP-ABE-MA, the key point of secure cipher text update is that the client who restores the cipher text should be able to prove to the cloud service provider (CSP) that he is a valid user. Further, the scheme can be scalable to add additional number of users with privacy preserving concern whereas the conventional CP-ABE scheme suffers in runtime addition of users.

II. LITERATURE REVIEW

Q. Huang et al proposed a secure data access control using CP-ABE update scheme. Here the authors scheme uses two basic blocks i) encrypting the
IoT data using ABE scheme ii) multiple policies for access control. Here the authors outsourced the entire fog data to cloud ISPs. The authors used ABE signatures technique to authorize the user to satisfy the update policy and renewal policy. Here the authors signed computations from the fog devices so that the data owners can encrypt and the end users can decrypt and re-encrypt the attributes based on the security policies [15-16].

Xianglong Wu et al proposed the multiauthority cloud system along with data access control scheme in order to ensure the cloud storage security. They investigated their method by introducing two novel attack patterns i) they initiated the user revocation which can eavesdrop the updated user keys along with the respective token to decrypt any secret information. Secondly, they focused on ciphertext update key where they regain its ability to decrypt the secret key information. In addition, they compared their method with DACC schemes and claimed that their method is better than the DACC schemes [2].

Bin Feng et al proposed the novel scheme on multi owner data sharing schemes. Here the author the secure and dynamic auditing protocol which rejects all the user requests which are unauthenticated. The author key idea is deployed as a privacy preserving protocol which supports data operations, bidirectional authentication and statistical analysis [3]. J.K.Liu et al proposed a robust two factor authentication scheme with factor revocability. Here the key idea is to allow the sender only needs to know the identity of the receiver. From the receiver side, the receiver has two know two important things namely i) a secret key and ii) unique personal security device. The author utilized the concept in case of device theft and achieved better reliability [4][17].

The literature review reveals the challenges and limitations of the existing protocols as reviewed in [1-5][18-20]. The existing schemes are robust for the direct attacks but present day adversaries are possessing different strategies to get into the system. Hence, based on the literature it is observed that the need for the CP-ABE with multi factor authentication is desirable.

III. PROPOSED METHODOLOGY

The work flow of the proposed methodology is shown in the Fig 3.1. The proposed methodology is built as an entire framework to ensure the storage security in Fog storages. The
proposed Fog Security Framework (FSF) consists of five major actors. 1) User interface 2) Back-end 3) Data Processors 4) Middleware Libraries 5) Cloud Storage servers. The detailed explanation for the each actors are given as follows:

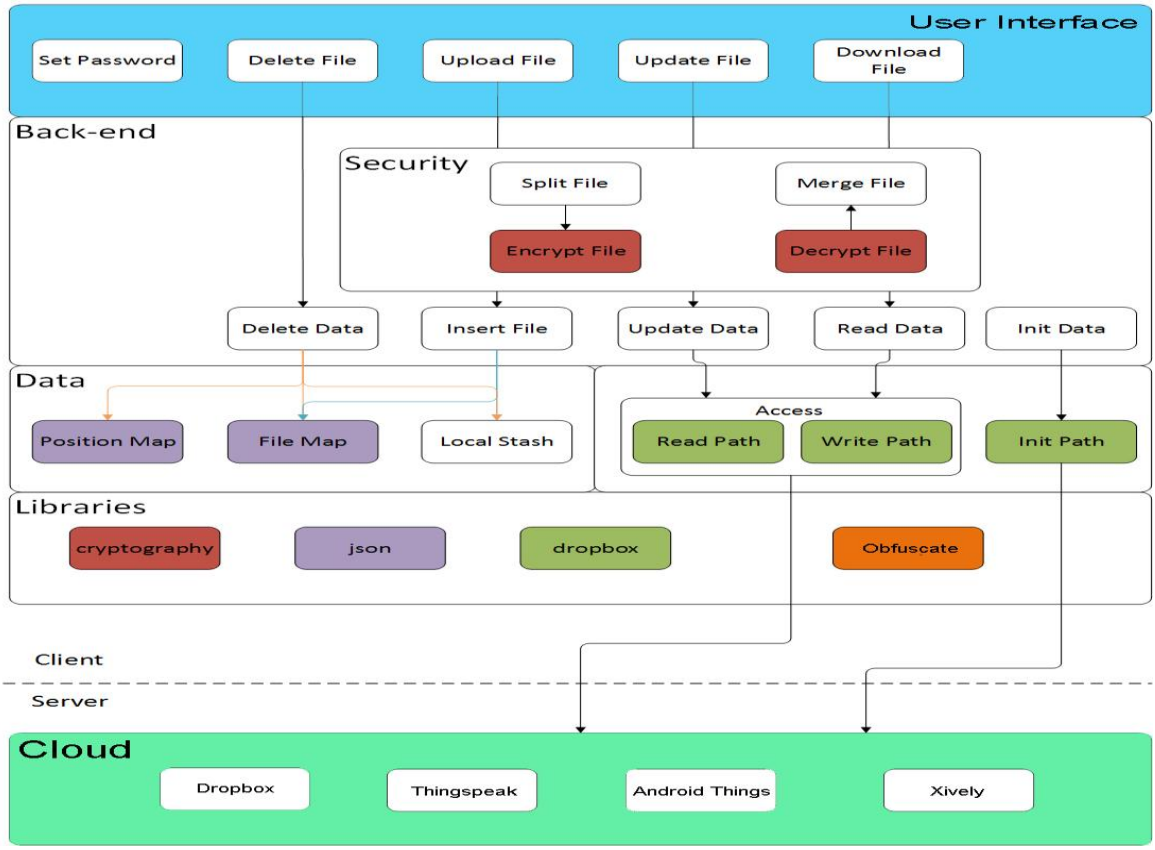

Fig3.1: Architecture of the proposed CP-ABE based Fog storage

Multi-factor authentication

In this framework, two or more credential is combined to achieve multi factor authentication. Here the security token is considered into two phases, initial token with user input as key and second phase of token as auto-generated and randomly generated token. Hence, in multifactor authentication, additional inclusion of security credentials leads to better assurance and security for the system and user as well.

User Interface

The User interface is the initial and primary component used by the client to interact with the storage server. The key role of the client is to authenticate himself to perform cloud drive I/O operations. The operations include File Access, Modification, Deletion, upload and download. Cipher text-Policy Attribute Based Encryption is used to authorize the users and user data

Back-end

Back-end is the place where the data transaction takes place. The tricky cryptography comes in this part.

Encryption

The Elliptic curve equation is $E_p(a, b) : y2 = x^3 + ax + b \pmod p$ over a finite field F_p.

p : prime order

a, b ϵ F_p

System Initialization:

- S selects a large prime number p and the base point P ϵ E_p
- S selects cryptographic hash function h(.)
- x and y are two numbers of 128-bit and 64-bit length.

Registration

The Registration phase is for System 'A' and System 'B'. The servers should follow the steps during their registration.

- System 'A' chooses its identity ID_A, a Password PW_A, one random number r_A. A computes $h(PW_A \| r_A)$ and privately send it to System 'B'.
- S generates a random value e_A and computes $XA = h [ID_A \| h(PW_A \| r_A)] \oplus h(x \| e_A)$, $Y_A = h[ID_A \| h(PW_A \| r_A) \| h(x \| e_A)]$ and $Z_A = h [h(PW_A \| r_A) \| ID_A] \oplus e_A$.
- Generate a token using $\{X_A, Y_A, Z_A, h(.)\}$ and send it to System A through a secure channel.
- Upon receiving the token, the System 'B' does the following:
- Inserts $P_A = h(ID_A \| PW_A) \oplus r_A$ into the token hence the token becomes $T_A = (X_A, Y_A, Z_A, P_A, h(.)\}$.

Login

To login with the system 'B', System 'A' sends its login request:

- Insert the token into the reader or some authenticated server and provide the login credentials ID_A, PW_A.
- The card / token gets $r_A = P_A \oplus h(ID_A \| PW_A)$, $h(x \| e_A) = X_A \oplus h(ID_A \| h(PW_A \| r_A))$ and checks if Y_A is equal to $h[ID_A \| h(PW_A \| r_A) \| h(x \| e_A]$. card / token check the match, if it is correct proceed otherwise disrupts the session.
- It receives (AS) $e_A = Z_A \oplus h(PW_A \| r_A) \| ID_A]$ and creates a nonce n_A. Then it computes $TID_A = h[h(x \| e_A)] \oplus (ID_A \| n_A P)$, and $T_A = h[ID_A \| h(x \| e_A) \| n_A . P]$.
- It transmits $\{TID_A, T_A, e_A\}$ to B.

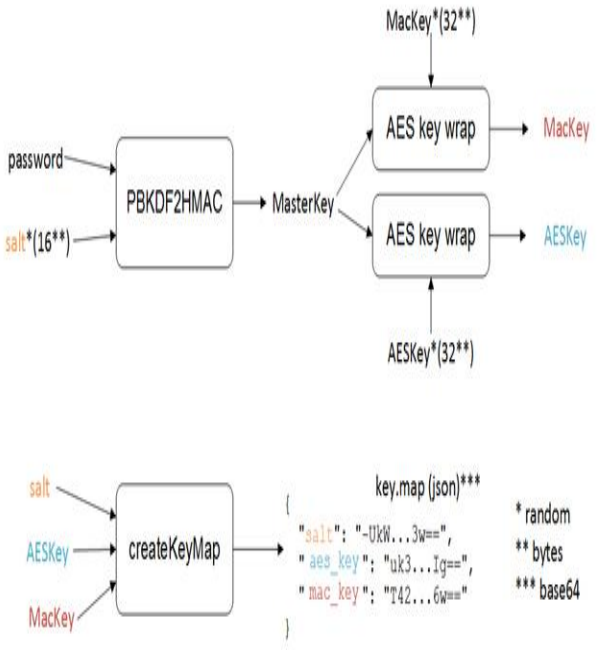

Fig 3.2: Key map generation using MacKey and AESkey Mutual Authentication

This step is processed over a public channel for mutual authentication and session key agreement protocol between Systems 'A' & 'B'. Once receiving the credentials from 'A' System 'B' executes the following steps:

- System 'B' checks if T_i is equal to $h[ID_A \| h(x \| e_A) \| (n_A P]$. The validity and the credentials of system 'A' proved, then B proceeds.
- B generates a new nonce n_B and computes $n_B . P = h[n_2.P \| h(x \| e_A) \| (n_A . P) \| ID_A]$. Then B transmits $\{n_B. P, V_B\}$ to A.
- After receiving the values, System A checks whether the V_B is equal to $h[n_B P \| h(x\|e_A) \| ID_A]$. If it is correct match, B authenticated successfully with A.

B computes the session key $SK = h[n_B . (n_A P) \| h(x \| e_A) \| ID_A]$ and check the M_A value is equal to $h[SK \| h(x \| e_A) \| ID_A]$. If it is authenticated System B grants A to access the services.

IV. Experimental Setup

From this part, the performance of the proposed CP-ABE-MA mechanism is evaluated. As shown in Table 4.1 the experimental evaluation was conducted by implementing the CP-ABE-MA scheme in Open nebula, an open source cloud computing platform for the 100 users and assuming each user shares 25 files on average in a span of 10 minutes, with the defined groups and cloud managers. The real time deployment was carried out in Lenova tower Server with 64 B RAM, Intel Xeon processor which runs in Cent OS as host and dedicated Virtual Desktop Interface (VDI) with Ubuntu server as guest. The opennebula has been deployed in Guest OS. The real time deployment of the proposed scheme consists of five different components: the owner side, the manager side, the CA side, the service provider side, cloud user which is re-sorted in the private cloud's storage.

The entire process of the storage is carried out in the owncloud, a private cloud storage unit dedicated with 8GB RAM, 1 Tb for storage, 1 Tb for mirroring copy, 8GB RAM and Intel I7 processor for computation. A dedicated backup server is also configured using Amanda. Three virtual machines (VM1, VM2 and VM3) have been created for storage from the 1Tb disk. The functionality of the CA is presented in VM1, the verification process of the GM is implemented in VM2 and cloud-storage and service-provider functionality are represented in VM3. The whole owner and user process is carried out in a physical machine. In order to achieve the entire deployment, a few libraries has been used. They are listed as follows: Pairing-Based Cryptography Library, the OpenSSL crypto library and the CP-ABE toolkit for all of our cryptographic operations.

Table 4.1: Experimental evaluation parameters

User count	100
Files Share	25 / user
Groups #	20
Manager #	20
Simulation Components	5 [Owner, Manager, CA, Cloud and User]

The CP-ABE-based cryptographic access control is also enforced in the manager's program. For key management, we use the CA and allocate the space to keep keys for each owner. Both the manager and owner programs are implemented in single threads for measuring the proposed scheme's time consumption.

Performance analysis

The proposed CP-ABE-MA mechanism is practically tested using two runtime storage server running in Cent OS with 4 tower servers running in Ubuntu server OS. 30 data storage owners with 200 clients each are taken into consideration for testing and validating the proposed protocol. Default configuration of Role based Access Control mechanism is configured and deployed in all the server roles. Further a third party auditor as a CA is logically defined and deployed, where CA is responsible to ensure the integrity and checks the availability of the storage server. The lifetime of the CA token is maximized to 12 hours. The experimentation was carried out in both Cloud and local server and the results were collected and represented in the Table4.1 and Table4.2. Fig 4.1 – 4.4 shows the various parametric statistics of the storage server while running our proposed CP-ABE-MA approach. Fig 4.5 shows the performance analysis of various cryptographic algorithm.

Table 4.2: CP-ABE-MA in Cloud environment

	Communication time (ms)	**Data processing time (ms)**		**Data length (bytes)**		**Network time (ms)**
CA Communication	27.892 ± 0.052	**Owners** **CA**	36.995 ± 0.105 0.053 ± 0.028	**REQ_CA** **RES_CA**	115 400	1.042 ± 0.020
SS Communication	3.86 ± 0.070	**Owners** **SS**	2.782 ± 0.023 1.440 ± 0.028	**REQ_SS** **RES_SS**	800 700	1.001 ± 0.021
CS Communication	3.175 ± 0.019	**Owners** **AS**	2.349 ± 0.021 3.180 ± 0.033	**REQ_CS** **RES_CS**	500 100	0.685 ± 0.011

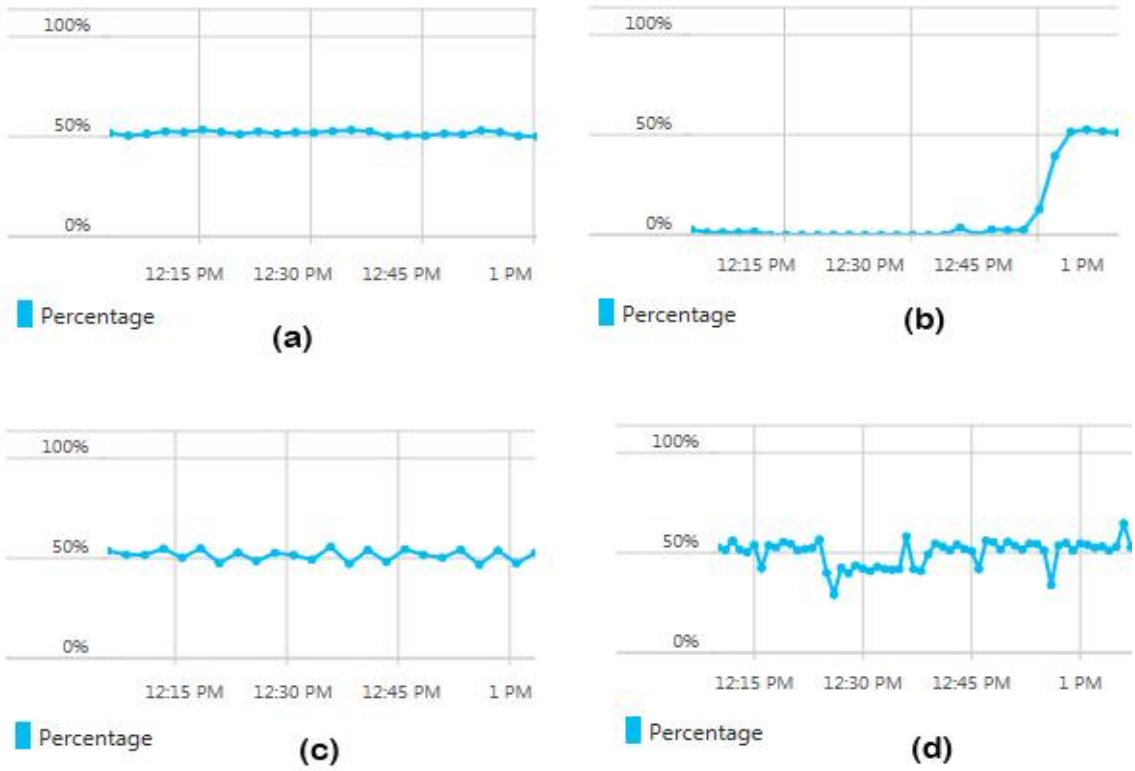

Fig 4.1: Health statistics - CPU (avergae) at storage server

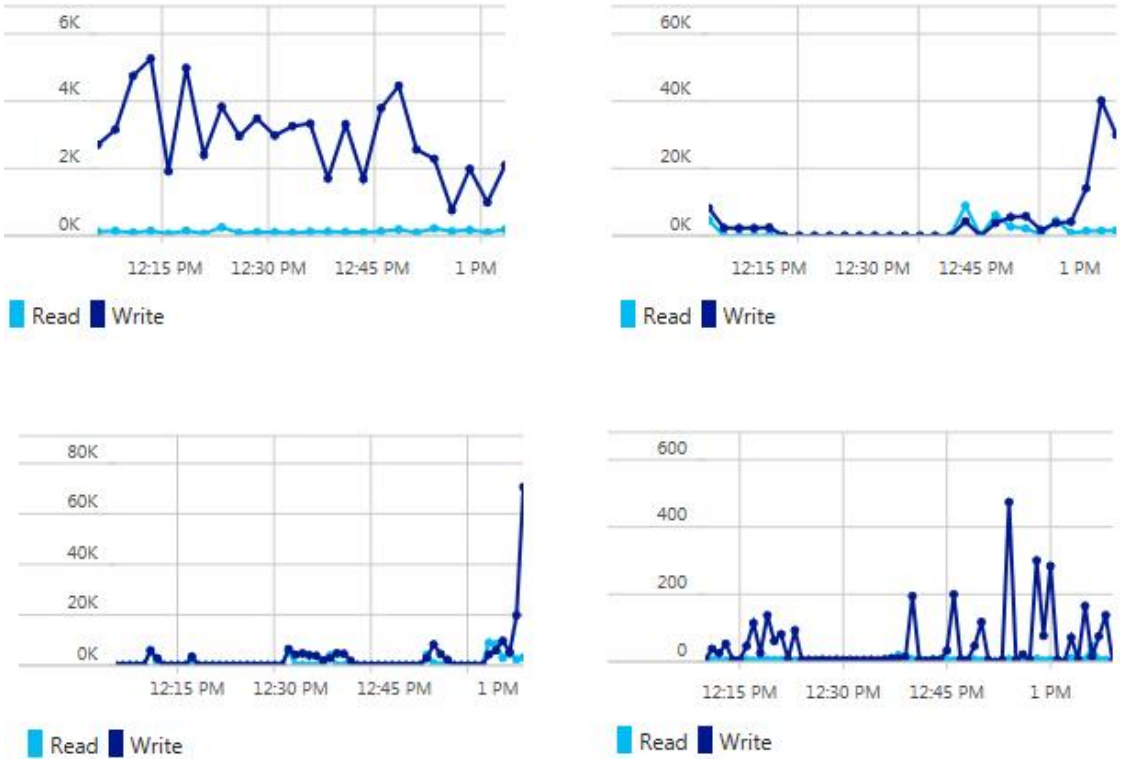

Fig 4.2: Health statistics -Disk Bytes (total in GB) at storage server

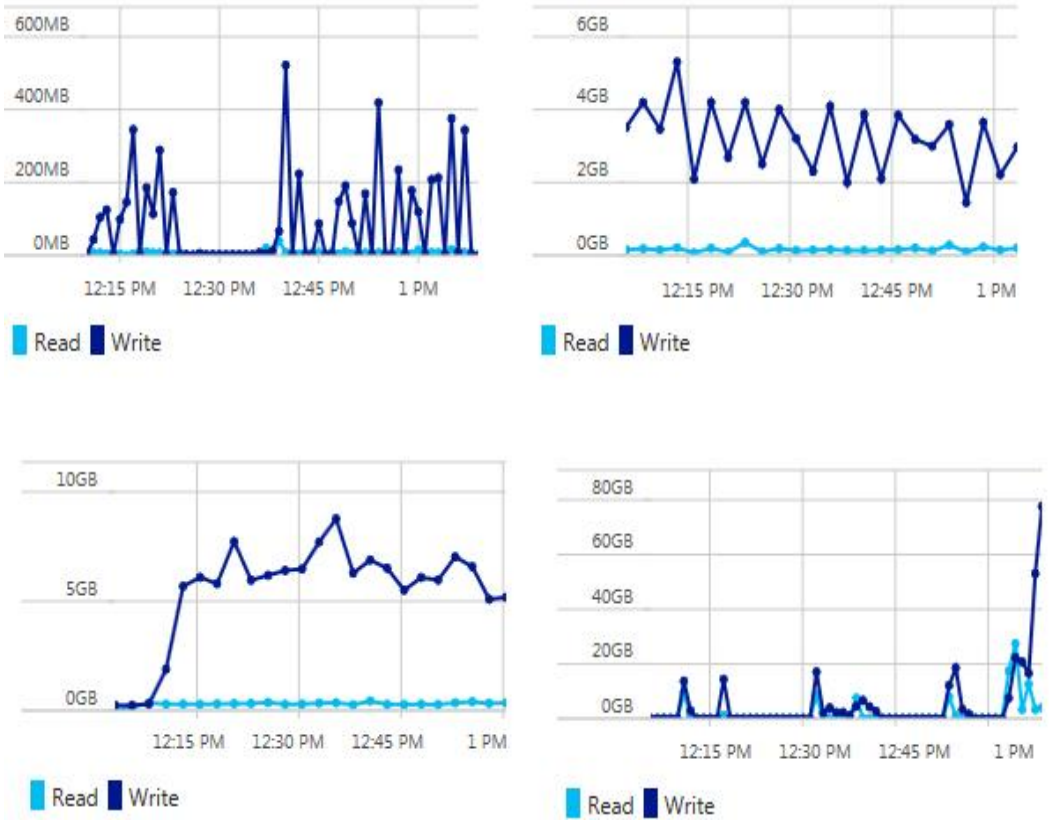

Fig 4.3: Health statistics -Disk operation/second at storage server

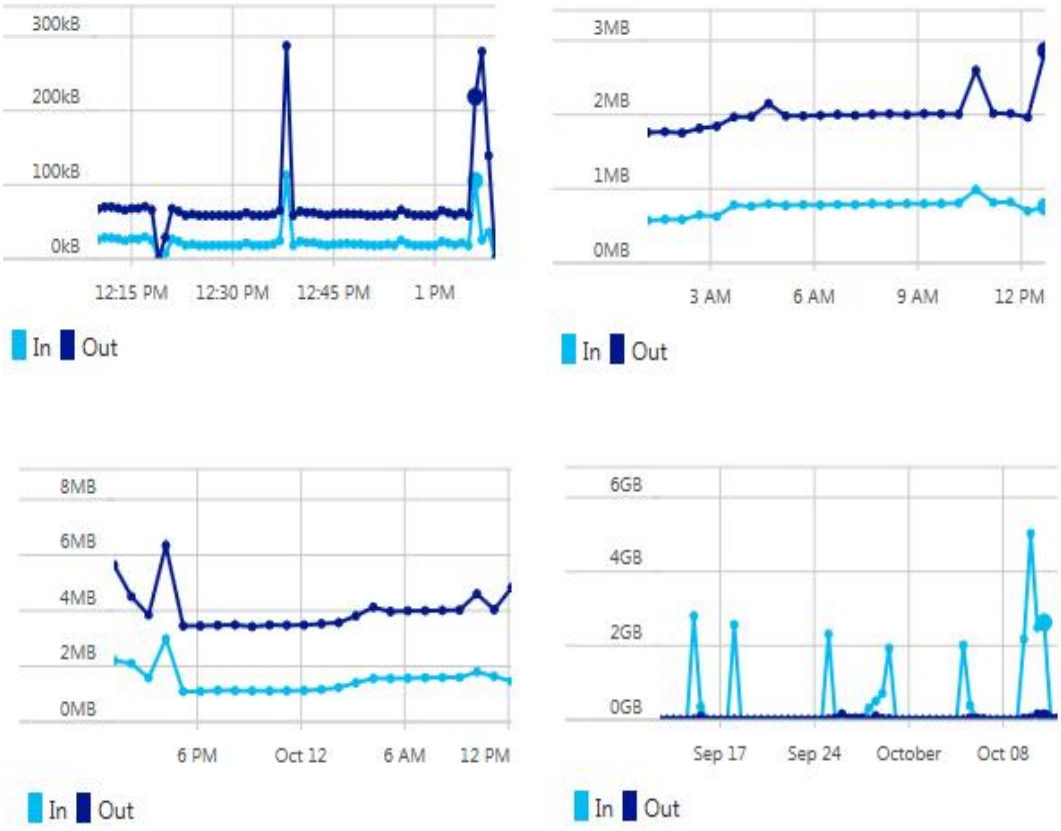

Fig 4.4: Health statistics -Network time at storage server

Algorithm\Properties	Key Size	Data Size	Encription Time
CP-ABE (DES)	8 Bytes	128 KB	Execution time of DES : 0.00250
CP-ABE (ECC)	16 Bytes	128 KB	Execution time of DES3 : 0.00684
CP-ABE (AES)	128 bits	128 KB	Execution time of AES : 0.00137
AES'	256 bits	128 KB	Execution time of AES : 0.00173
RSA	1024 bits	128 KB	Execution time of RSA : 0.10503
RSA'	2048 bits	128 KB	Execution time of RSA :0.10880

Fig 4.5: Performance comparison of various cryptographic algorithms

Table4.3: CP-ABE-MA in Local network

	Communication time (ms)	**Data processing time (ms)**		**Data length (bytes)**		**Network time (ms)**
CA Communication	52.052 ± 0.265	**Owners** **GM**	45.854 ± 1.0 11.941 ± 1.236	**REQ_CA** **RES_CA**	215 596	1.853 ± 0.041
SS Communication	9.08 ± 0.070	**Owners** **SM**	3.782 ± 1.423 8.310 ± 1.418	**REQ_SS** **RES_SS**	968 623	2.958± 0.254
Local Storage server Communication	7.875 ± 0.019	**Owners** **LN**	4.852 ± 1.285 **6**.180 ± 1.719	**REQ_LN** **RES_LN**	531 142	5.852 ± 1.006

V. Conclusion

Further, we conclude this paper by proposing a novel CP-ABE-MA scheme. The proposed scheme is robust and optimal with an additional security to Fog devices. Furthermore, the initial data of the users, managers etc., are encrypted using CP-ABE-MA and then the resources transferred to cloud through the Fog devices which satisfies the user attributes with ABE scheme using ECC. In addition to address the data outsourcing and to verify the outsourced data from the Fog devices the CSP will check the signature, to ensure that only the users whose attributes satisfy the update policy can renew the cipher text. The experimental observation had proven that the proposed CP-ABE-MA scheme has both fine grained access control and better cipher suite when compared to conventional CP-ABE scheme. In future the proposed schemes can be extended to hybrid schemes based on personal health attributes and data and further the proposed algorithm can be implemented using GPU based parallel processing units in order to minimize the execution time and to improvise the architecture in the way towards fast processing.

References

1. Q. Huang, Y. Yang and L. Wang, "Secure Data Access Control With Ciphertext Update and Computation Outsourcing in Fog Computing for Internet of Things," in *IEEE Access*, vol. 5, pp. 12941-12950, 2017.
2. X. Wu, R. Jiang and B. Bhargava, "On the Security of Data Access Control for Multiauthority Cloud Storage Systems," in *IEEE Transactions on Services Computing*, vol. 10, no. 2, pp. 258-272, March-April 1 2017.
3. B. Feng, X. Ma, C. Guo, H. Shi, Z. Fu and T. Qiu, "An Efficient Protocol With Bidirectional Verification for Storage Security in Cloud Computing," in *IEEE Access*, vol. 4, pp. 7899-7911, 2016.
4. J. K. Liu, K. Liang, W. Susilo, J. Liu and Y. Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System," in

5. *IEEE Transactions on Computers*, vol. 65, no. 6, pp. 1992-2004, June 1 2016.
6. J. Ni, Y. Yu, Y. Mu and Q. Xia, "On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 10, pp. 2760-2761, Oct. 2014.
7. B. Z. Abbasi and M. A. Shah, "Fog computing: Security issues, solutions and robust practices," *2017 23rd International Conference on Automation and Computing (ICAC)*, Huddersfield, 2017, pp. 1-6.
8. H. Madsen, B. Burtschy, *Reliability in the Utility Computing Era: Towards Reliable Fog Computing*, pp. 43-46, 2013.
9. I. Stojmenovic, S. Wen, "The Fog Computing Paradigm: Scenarios and Security Issues", *Proc. 2014 Fed. Conf. Comput. Sci. Inf. Syst*, vol. 2, pp. 1-8, 2014.
10. T. H. Luan, L. Gao, Z. Li, Y. Xiang, L. Sun, *Fog Computing: Focusing on Mobile Users at the Edge*, pp. 1-11, 2015.
11. W. Wang, Z. Lu, "Cyber security in the Smart Grid: Survey and challenges", *Comput. Networks*, vol. 57, no. 5, pp. 1344-1371, 2013.
12. R. Chaudhary, N. Kumar and S. Zeadally, "Network Service Chaining in Fog and Cloud Computing for the 5G Environment: Data Management and Security Challenges," in *IEEE Communications Magazine*, vol. 55, no. 11, pp. 114-122, NOVEMBER 2017.
13. C. Huang, R. Lu and K. K. R. Choo, "Vehicular Fog Computing: Architecture, Use Case, and Security and Forensic Challenges," in *IEEE Communications Magazine*, vol. 55, no. 11, pp. 105-111, NOVEMBER 2017.
14. S. Rathore, P. K. Sharma, A. K. Sangaiah and J. H. Park, "A Hesitant Fuzzy based Security Approach for Fog and Mobile-Edge Computing," in *IEEE Access*, vol. PP, no. 99, pp. 1-1.
15. H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren and A. Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography," in *IEEE Access*, vol. 5, pp. 22313-22328, 2017.
16. M. Mukherjee *et al*., "Security and Privacy in Fog Computing: Challenges," in *IEEE Access*, vol. 5, pp. 19293-19304, 2017.
17. B. Jia, H. Hu, Y. Zeng, T. Xu and Y. Yang, "Double-matching resource allocation strategy in fog computing networks based on cost efficiency," in *Journal of Communications and Networks*, vol. 20, no. 3, pp. 237-246, June 2018.
18. S. N. Shirazi, A. Gouglidis, A. Farshad and D. Hutchison, "The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective," in *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2586-2595, Nov. 2017.
19. M. Sookhak *et al*., "Fog Vehicular Computing: Augmentation of Fog Computing Using Vehicular Cloud Computing," in *IEEE Vehicular Technology Magazine*, vol. 12, no. 3, pp. 55-64, Sept. 2017.
20. D. S. Linthicum, "Connecting Fog and Cloud Computing," in *IEEE Cloud Computing*, vol. 4, no. 2, pp. 18-20, March-April 2017.
21. E. Baccarelli, P. G. V. Naranjo, M. Scarpiniti, M. Shojafar and J. H. Abawajy, "Fog of Everything: Energy-Efficient Networked Computing Architectures, Research Challenges, and a Case Study," in *IEEE Access*, vol. 5, pp. 9882-9910, 2017.
22. J. Kang and H. Yu, "Mitigation technique for performance degradation of virtual machine owing to GPU pass-through in fog computing," in *Journal of Communications and Networks*, vol. 20, no. 3, pp. 257-265, June 2018.
23. C. Chang, S. Narayana Srirama and R. Buyya, "Indie Fog: An Efficient Fog-Computing Infrastructure for the Internet of Things," in *Computer*, vol. 50, no. 9, pp. 92-98, 2017.

Author Bibliography

Mr.J.Velmurugan Received B.E degree in Computer Science and Engineering from Vel Sri Rangarajan Sakunthala College of Multimedia, Affiliated to Madras University, India, in 2004. Received M.E degree in Sathyabama University, India, in 2007 and Pursuing Ph.D in Anna University, Chennai, India. Presently working as a Assistant Professor in IT Department at Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala of Engineering college, Chennai, India. His current research interest is to improve security performance in cloud computing.

Dr.S.Manjula was born in 1984 in Chennai, India. She received the B.E. degree in Electronics and Instrumentation Engineering from Kamaraj College of Engineering and Technology, Virudhunagar, Tamilnadu, India in 2005, the M.E degree in Applied Electronics from Velammal Engineering College, Chennai, India in 2008 and the Ph.D. degree in the area of low power RF Integrated Circuit design from Anna University, Chennai, India in 2016. She has teaching experience of more than 5 years. She is currently working as an Associate Professor in Rajalakshmi Institute of Technology. She published 6 national conferences, 6 international conferences and 12 international journals. Her research interests are low power integrated circuit design, Transceiver design and VLSI circuit design.