International Journal of Research in Advent Technology, Special Issue, March 2019
E-ISSN: 2321-9637
International Conference on Technological Emerging Challenges (ICTEC-2019)
Available online at www.ijrat.org

Secure Scalable Explosion Management Data Outline in Computing Networks

[1]K.Ravi Chand, [2]Battula Siva Kondaiah
[1]*Associate Professor & HOD , N.V.R College of Engineering & Technology*
[1] *email: ravickopila@gmail.com.*
[2] *Asst. Professor, T.J.P.S. College (PG Courses),* [2]*email: sivakondaiah@gmail.com*

Abstract: The cloud computing paradigm that extends the edge of networks. This computing is appropriate for Electronic Medical Record (EMR) systems are latency-sensitive in nature. We aim to achieve two goals: (1) Managing and sharing Electronic Health Records (EHRs) between multiple fog nodes and cloud, (2) Focusing on security of EHR, which contains highly confidential information. We provide contemporary evident characteristics associated to. examine the technologies is implement the models and architectures and analyze them with respect to security and resilience requirements. The lightweight two-level session key is generated using the Hash Message Authentication Code (HMAC) and Exclusive OR (XOR) operations. The Advanced Encryption Standard (AES) key and session key are required to download and decrypt the file. The users using the cloud is update their access patterns are recorded. Every person who is trying to access the data is made to answer the security questions. Also an OTP is provided to avoid shoulder sniffing of password. We focus on reducing the storing and processes in fog nodes to support low capabilities of storage and computing of fog nodes and improve its performance. The theoretical analysis shows the good performance and functionality requirements while the implementation results demonstrate the feasibility of our proposal.

Index Terms: Fog computing, Electronic Medical Record (EMR), Electronic Health Record (HER), mobile edge computing, fog computing, cloud security, Genetic Algorithm (GA), Lightweight Key Management

1. INTRODUCTION

Cloud Computing is considered a promising prototype of computing since it can provide users with elastic computing resources based on shared computing techniques, virtualization the universality of Internet of Things (IoT) applications is changing the main factor of computing [1]. The data owner is upload the data to the cloud service provider and access the stored data using the software provided by the service provider. As the data received from the data owner is not enough to fill the storage space of the server, it leads to a lot of storage waste [2]. The providers specialize in both hardware and software technologies, cloud users can be relieved of the need to have in-house teams to conduct maintenance operations on the infrastructure [3]. Motivated primarily by economies of scale, cloud environments are also being used by sectors operating in the area of critical infrastructures [4]. The developing applications are computing resources is critical because it includes heterogeneous resources different levels of network hierarchy to provide low latency and security requirement for new applications [5]. We know smart devices usually face challenges rooted from computation power, battery, storage and bandwidth, which in return hinder quality of services (QoS) and user experience [6]. A privacy-focused service may wish to promptly and securely delete the data once they have served their purpose secure data deletion simply to comply with regulations regarding their users' sensitive data forgotten forces companies to store users data in a manner that supports secure data deletion upon request. Meanwhile California's legislation enforces similar requirements [7].

Fig. 1. An example of fog/cloud architecture

2. RELATED WORKS

Cloud computing is considered as a level in the middle of the cloud and end users are formed by fog nodes, such as routers, switches hardened and immediate for end users that servers in the cloud and some of the workloads and services that the cloud transfers to fog nodes [8]. The set of secret keys is aggregated to form a single compact key that can be transmitted conveniently or stored in a smart card without requiring more secure storage and proposed novel modifications to the ABE scheme for enabling authorized access of the cloud data in control is achieved based on the satisfaction of required attributes [9]. Mobile wireless communication has received a lot of attention and has become hugely popular during the past decade these devices are usually equipped with multi-core processors, various sensors as well as running a plethora of applications that managed to improve the productivity of mobile users [10]. They proposed a schema consists of decentralized hierarchical key agreement protocol to securely establish a hierarchy of crypto keys with the privilege levels of the team member's data confidentiality but it must be guaranteed that hierarchical keys are unique and fresh for each run of the protocol which requires high computation [11]. Reputation based trust model is successful peer-to-peer (P2P), user reviews and online social networks is proposed a robust reputation system for resource selection in P2P networks using a distributed polling algorithm to assess the reliability of a resource before downloading [12].

3. SYSTEM MODEL

We consider adversaries whose main goal is to obtain the data which they are not authorized to access to attackers is eavesdrop all the communications in the system and unauthorized users may collude to compromise the encrypted data are deleted; adversaries try to recover the deleted data [13]. Secure fine-grained access control: As mentioned previously, fine-grained data access control is always desirable in many applications. In the security model of assured deletion the adversary chooses an access structure is beginning of the game, such that the data key encrypted under the access structure A $*$ is deleted in the end [14]. We support to implementing part of EHR in suitable and nearest fog nodes and we propose that Attribute Based Access Control (ABAC) that depends on attributes of object action attributes and environment conditions [15].

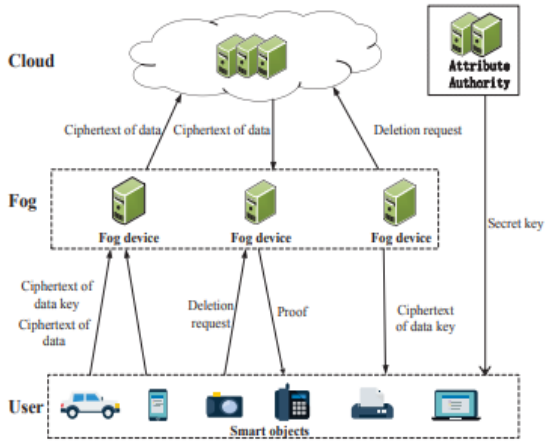

Fig. 2: System model

4. PROPOSED LIGHTWEIGHT HYBRID KEY MANAGEMENT SCHEME

The data owner employs the AES algorithm to encrypt and decrypt the input data file to sends the session key generation request to the cloud service provider through the TPA. Message authentication code (MAC) value of the ID and nonce is computed [16]. The attribute authority is a fully trusted party which is in charge of generating system parameters as well as secret key for each user and also helping users to decrypt the cipher text from the CSP they assist end users to sign the cipher text update request [17].

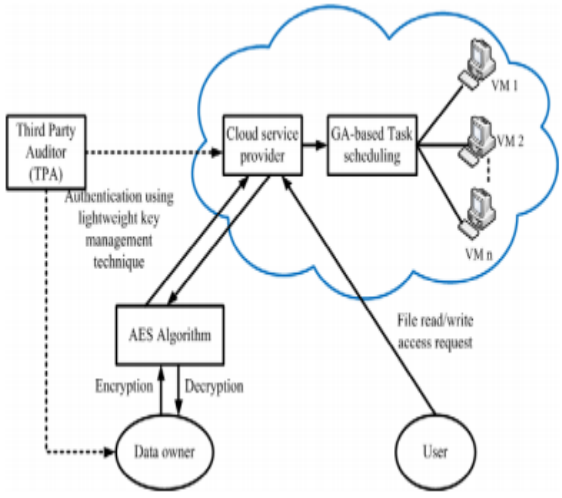

Fig.3 System architecture of the proposed key management scheme

A. Security and Privacy Models

We admit that security and privacy should be addressed in every layer in designing fog computing system is ask ourselves new fog computing security

and privacy to the characteristics of fog computing to may need future work to tackle those problems [18].

Security Key Generation

Phase 1: System Setup

1) Setup 1: The attribute authority takes as input security Parameter k, and outputs the system public key (PK) and master secret key (MK).

Phase 2: Key Generation

2) Key Gen (PK, MK, S). The attribute authority takes as input PK, MK, a set of attributes S, outputs the secret key SK for the user.

Phase 3: Data Symmetric Encryption

3) Fog. Encrypt (PK, T). The fog node takes as input PK, an access policy T, outputs a partial cipher text CT'.

4) 4) Owner. Encrypt (PK, M, Tu, CT). The data owner takes as input PK, a data M, an update policy Tu, a partial cipher text CT', and outputs the cipher text CT.

Phase 4: Data Decryption

5) Fog. Decrypt (PK, CT, SK'). The fog node takes as input PK, a cipher text CT and a user's SK', and outputs a partial decrypted cipher text T if the attributes satisfy access policy T.

6) User. Decrypt (T, SK). The user takes as input a partial decrypted cipher text T and SK, then recovers the MK and outputs the plaintext M.

Phase 5: Cipher Text Update

7) Fog. Sign (PK, U, Tu, SK'). The fog node takes as input PK, a user's cipher text update request U and SK', update policy Tu.

8) User. Sign (PK, ST', SK). The user takes as input PK, a partial signature ST' and SK, outputs the signature ST.

9) Verify (Public key, ST, GK). The CSP takes as input PK, a signature ST and a global key GK

The workflow of our scheme is shown in the figure [21]. Generating keys with the algorithm, the authority attribute generates secret keys for owners and users of the data [19].

B. AES Algorithm

The AES algorithm is used encrypting plaintext into cipher text and decrypting it back into the plaintext. It is a symmetric block cipher with the fixed block size of 128 bits. The size of the cryptographic keys is 128, 192 and 256 bits. A 128-bit round key is required separately for each encryption and decryption round [20].

1. **Sub-Bytes:** The substitution box is used for replacing each byte in the array by another byte.
2. **Shift Rows:** Every row is shifted left to about 'k' bytes in a cyclical manner. The 'k' value depends on the key and number of the rows.
3. **Mix Columns:** The linear mixing operation mixes the four bytes in each column.
4. **Add Round Key:** The XOR operation is applied for adding a unique round key to each byte
5. **Inverse Sub-Bytes:** The inverse of the substitution box is used.
6. **Inverse Shift Rows**: The row operation is inversed by shifting the elements in the row to the right side.
7. **Add Round Key:** This process is same as the encryption process.
8. **Inverse Mix Columns:** In this process, linear mixing is performed but with different matrix

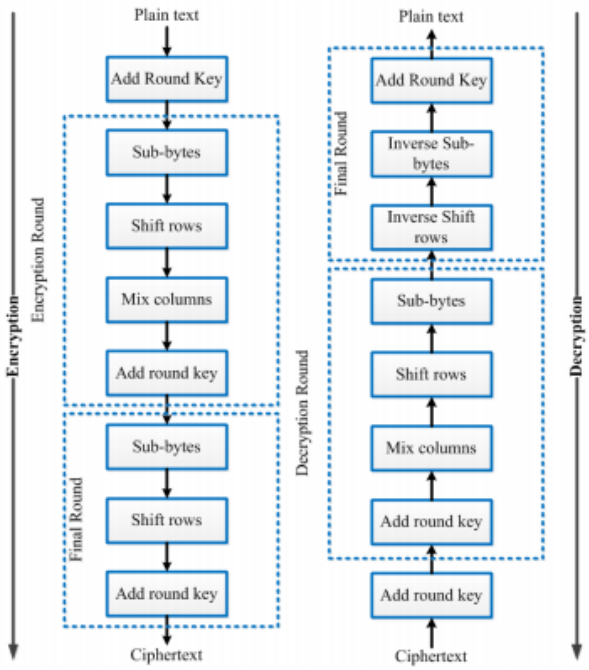

Fig.4. Operation of the AES algorithm

5. PERFORMANCE ANALYSIS

Security Analysis is proposed scheme a session key is established to secure the communication data owner and cloud service provider. As the session key is changed after every data transaction it is difficult for the brute force attacker to find the correct session key. File uploading time includes the time required to security the file as requested by the client. It is the

time points when the data owner requests the cloud service provider to upload the file, the finishing time of the encryption and key generation tasks and the encrypted file is stored in the cloud data storage. Our proposed LHKMS scheme requires minimum encryption time than the existing cryptographic schemes.

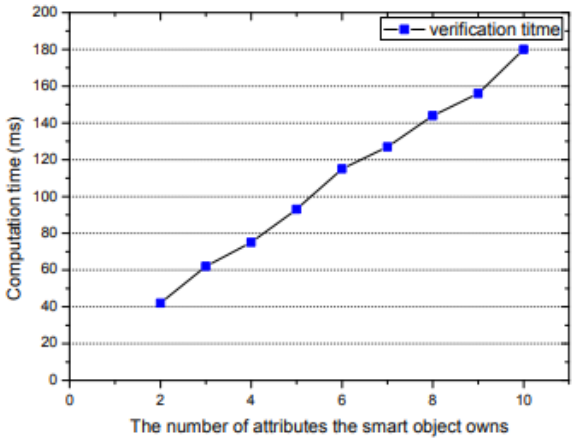

Fig.5 Encryption time of the proposed and existing key management schemes

6. CONCLUSION AND FUTURE WORK

We provided to prevent unauthorized access to consider in our solution the low capabilities of storage and computing of fog nodes by focusing on reducing the storing and processes in fog nodes to serve to improve its performance and efficiency. We proposed new protocol smart objects encrypt the data with an access structure and only the users with intended attributes is decrypt it correctly.. We also highlight privacy issues in data privacy, usage privacy and location privacy is new think to adapt new challenges and changes. This is mostly due to existing similarities between the cloud and the new software-driven communication technologies; the latter rely heavily on, the requirements posed by emerging services strongly suggest the need to re address security and resilience, and to investigate them in their new application contexts. The security analysis states the proposed key management scheme yields high security and scalability due to the two-level session key establishment key management scheme is compared with the existing cryptographic schemes. In our future work is simulate our solution increasing number of attributes, which is suitable for the resource constrained IoT devices in fog computing.

REFERENCES

[1] Data collaboration in cloud computing," in Proc. IEEE/ACM 21st International Symposium on Quality of Service, Montreal, QC, 2013, pp.195-200.
[2]. F. Zhao, T. Nishide, and K. Sakurai, "Realizing finegrained and flexible access control to outsourced data with attribute-based cryptosystems," in Proc. Information Security Practice and Experience - 7th International Conference, Guangzhou, China, 2011, pp. 83-97.
[3]J. Li, M.H. Au, W. Susilo, D. Xie, and K. Ren, "Attributebased signature and its applications," in Proc. 5th International Symposium of Information, Computer and Communications Security, Guangzhou, China,2010, pp. 60- 69.
[4]Y. Jiang, W. Susilo, Y. Mu, and F. Guo. (2017, Jan.).Cipher text-policy attribute-based encryption against keydelegation abuse in fog computing. Future Generation Computer Systems.
[5]L. Yeh, P. Chiang, Y. Tsai, and J. Huang. (2015, Oct.). Cloudbased fine-grained health information access control framework for lightweight IoT devices with dynamic auditing and attribute revocation. IEEET transactions on Cloud Computing.
[6]C. Zuo, J. Shao, G. Wei, M. Xie, and M. Ji. (2016, Nov.). CCAsecure ABE with outsourced decryption for fog computing. Future Generation Computer Systems.
[7]Y. Yang, X. Zheng, and C. Tang. (2016, Nov.). Lightweight distributed secure data management system for health internet of things. Journal of Network and Computer Applications.
[8]A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques Aarhus, Denmark, 2005, pp. 457-473
[9] B. Parno, M. Raykova, and V. Vaikuntanathan, "How to Delegate and Verify in Public: Verifiable Computation from Attribute-Based Encryption," in TCC, 2012, pp. 422-439.
[10] Y. Tang, P. P. Lee, J. C. Lui, and R. Perlman, "Secure overlay cloud storage with access control and assured deletion," IEEE Transactions on dependable and secure computing, vol. 9, pp. 903-916, 2012.
[11] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security, 2010, pp. 735-737.
[12] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Infocom, 2010 proceedings IEEE, 2010, pp. 1-9.

[13] Y. Zhu, H. Hu, G.-J. Ahn, M. Yu, and H. Zhao, "Comparison-based encryption for fine-grained access control in clouds," in Proceedings of the second ACM conference on Data and Application Security and Privacy, 2012, pp. 105-116.
[14] H. Pang, J. Zhang, and K. Mouratidis, "Scalable verification for outsourced dynamic databases," Proceedings of the VLDB Endowment, vol. 2, pp. 802-813, 2009.
[15] A. Singh and L. Liu, "Sharoes: A data sharing platform for outsourced enterprise storage environments," in IEEE 24th International Conference on Data Engineering, 2008. ICDE 2008., 2008, pp. 993-1002.
[16] H. Wang and L. V. Lakshmanan, "Efficient secure query evaluation over encrypted XML databases," in Proceedings of the 32nd international conference on Very large data bases, 2006, pp. 127-138.
[17] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy, 2007. SP'07., 2007, pp. 321-334.
[18] S. Fugkeaw and H. Sato, "An extended CP-ABE based Access control model for data outsourced in the cloud," in IEEE 39th Annual Computer Software and Applications Conference (COMPSAC), 2015, pp. 73-78.
[19] A. Logic, "The changing state of cloud security," Tech. Rep., 2015.
[20] M.A.C.Dekker, "Critical cloud computing: A CIIP perspective on cloud computing services," European Network and Information Security Agency, Tech. Rep., 2012.
[21] S. Berman, L. Kesterson-Townes, A. Marshall, and R. Srivathsa, "The power of cloud. driving business model innovation," IBM Institute for Business Value, Tech. Rep., 2012.