Journal of Engineering and Applied Sciences 14 (10): 3359-3365, 2019
ISSN: 1816-949X

An Updated Hybrid Cryptography Based Security for Cloud Computing System

G. Narmadhai and S. Vijay Bhanu
Department of Computer Science and Engineering Annamalai University, Annamalai Nagar, 608002 Chidambaram, India

Abstract: The novel and updated scheme strongly focuses on the data processing, storing and accessing the data which is designed to ensure the users with legal authorities to get corresponding classified data and to restrict the illegal users and unauthorized legal users get access to the data which makes it extremely suitable for the mobile cloud computing. There are different parameters to evaluate the performance of the existing Attribute-Based Encryption (ABE) methods in cloud computing as follows: ciphertext size (communication cost), private key size (storage cost), public key size (required storage to store the public key of authorities in the ABE method), re-keying size (the size of the rekeying message that can be used to recognize the user revocation for each attribute in the ABE system), computation cost on the data owner (required time to encrypt data by a data owner), computation cost on the user (required time to decrypt data by a user). Our research work also analyses the importance of the data security in the cloud. Reason for choosing symmetric encryption algorithms are efficient to handle encryption and decryption for large amount of data and effective speed of storing data and accessing the data in the cloud system. For implementation purpose here are considered the type of file as document file (doc), text file (txt) which can be enhance to sound file, video file, image file with different formats.

Key words: Attribute-based encryption, hybrid cryptography, security, cloud computing system, video and audio file, implementation

INTRODUCTION

Cloud computing: The symmetric key algorithms has been divided into two types: block cipher and stream cipher. The current sizes of each blocks are 64, 128 and 256 bits. Cloud services mainly includes online file storage, social networking sites, webmail and online business applications. To secure the cloud means secure the calculations or data and storage. Security goals of data include three points namely: availability, confidentiality and integrity. Confidentiality of the data in the cloud can be achieved only by cryptography (Ruj *et al*., 2014).

Attribute-Based Encryption (ABE) is a most popular cryptographic technology to protect the security of user's data in cloud computing. Cloud computing is one of the biggest areas because of its high-level features and advantages such as convenience, scalability and cost-saving. Due to the vulnerability, the development of the security model is very very difficult. Consequently, the economic benefits and availability will be affected (Younis *et al*., 2014; Cao *et al*., 2014). The attacker constructs the attacks in mobile application and devices in that place develop the hypervisor to deny the Virtual Machine (VM) side-channel attack and Denial-of-Service (DoS) attack (Modi *et al*., 2013; Singh *et al*., 2016; Yan and Yu, 2015).

Attribute-Based Encryption (ABE): Attribute-Based Encryption (ABE) is a public-key algorithm based one to many encryptions that allows users to encrypt and decrypt the data based on user attributes. Thus, the access structure will contains the authorized sets of attributes. They restrict the attention to monotone access structures (Lacuesta *et al*., 2011).

Cipher text policy attribute-based encryption: Another modified form of ABE (Attribute-Based Encryption) called CP-ABE (Cipher text Policy Attribute-Based Encryption) was introduced by Sahai *et al*. In a modified form of CP-ABE scheme, every ciphertext is associated with an access policy on attributes and every user having private key is associated with a set of attributes. A user is able to decrypt a ciphertext only if the set of attributes associated with the user's private key satisfies the access policy associated with the ciphertext. The CP-ABE (Cipher text Policy Attribute-Based Encryption) works in the reverse way of

Corresponding Author: G. Narmadhai, Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar, 608002, Chidambaram, India

Key Policy Attribute-Based Encryption (KP-ABE) (Ranchal *et al*., 2010; Darwazeh *et al*., 2015; Xu *et al*., 2012; King and Raja, 2012).

Key Policy Attribute-Based Encryption (KP-ABE): KP-ABE (Key Policy Attribute-Based Encryption) is the modified form of new classical model of Attribute-Based Encryptin (ABE). Users are assigned with an access tree based structure over the data attributes. Threshold gates are the nodes of the access tree and the attributes are associated by leaf nodes in a tree. To reflect the access tree structure, the secret key of the user is defined by Changji Wang in the year 2013. Ciphertexts are labeled with a sets of attributes and private keys are associated with monotonic access structures that control which ciphertexts a user is able to decrypt. Key Policy Attribute Based Encryption (KP-ABE) scheme is designed for one-to-many communications in the cloud computing (Fabian *et al*., 2014; Darwazeh *et al*., 2015).

In this proposed research work, Hybrid Hierarchical Attributes Based Encryption (H-HABE) algorithm is developed for securing the data stored in the cloud storage system. An attribute encryption scheme with additional authority is more adaptable for data access control cloud storage systems because the user can be helded by multiple institutions to manage property. Traditional single authority to manage all user attributes dense hack, easy to degrade the system performance. In addition, a single authority solution wants a completely honest authorized body it is not easy to meet the security requirements of cloud computing environments. Weighted Attribute-Based Encryption (WABE) is hybridized with the Hybridized Hierarchical Attributes Based Encryption (H-HABE) for encryption purposes for imroving the performance. Encryption, key generation and decryption are ensured with the AES and blowfish algorithm. A key contribution in this research paper is summarized as follows.

Here the propose a novel data collaboration scheme for secure read and write operations in cloud computing that allows a symmetric encryption algorithm for effective key management to reduce computational overhead. A full delegation approach-based Hybridized Encryption (H-HABE) that is employed for the outsourced data should be secure.

Here, provide a verification method for the outsourced encryption and decryption. If the cloud environment returns incorrect results, users can notice it immediately by running the corresponding verification algorithm. Therefore, the user can access the data anywhere and anytime by using any device. The computational cost is very low which is introduced by ABE in the user side. Here, provide a security and performance analysis of our proposed and newly desinged scheme which shows that our scheme is both secure and highly efficient.

Literature review: J. Benelux has proposed the scheme in which a file can be uploaded without key distribution and it is highly and appreciable efficient. But it is a single data owner scenario and thus it is not an easy to add categories (Ruj *et al*., 2012; Wang *et al*., 2014; Li *et al*., 2014).

C. Dong has explored that the data encryption scheme does not requires a trusted data server. The data server can perform encrypted searches and updates on encrypted data without knowing the plaintext or the keys to decrypt. But in this scheme the server knows the access pattern of the users which allows it to infer some of information about the queries. To realize the fine grained access control, the traditional Public Key Encryption (PKE) based schemes and either incurred high key management overhead, or require encrypting multiple copies of a file using different users keys. To improve the scalability of the solutions, one-to-many encryption methods such as Attribute Based Encryption (ABE) can be used (Chu *et al*., 2014; Choi *et al*., 2014; Wei *et al*., 2014; Li *et al*., 2013).

Sashay and Waters first introduced the Attribute Based Encryption (ABE) for enforced access control through public key cryptography. The main aim for these models is to provide high security and access control. The main aspects these models are to provide flexibility, scalability and fine grained access control. In the classical model, these system can be reached only when user and server are in a trusted domain server. So, the new access control scheme that is Attribute Based Encryption (ABE) scheme was introduced which consist of Key Policy Attribute Based Esncryption (KP-ABE). As compared with the classical model, KP-ABE provided the fine grained access control. However, this model is fails with respect to flexibility and scalability when authorities at multiple levels are considered. In the ABE scheme both the user's secret key and the cipher text are associated with a set of attributes. ABE scheme is implemented for one-to many encryption in which cipher-texts aren't necessarily encrypted to one particular user, it may be for more than one number of users (Do *et al*., 2011).

Akinyele investigated using ABE to generate self-protecting EMRs which can either be stored on mobile phones or cloud servers so that, EMR could be accessed when health provider is in offline also, (Jiang *et al*., 2017; Samanthula *et al*., 2015; Hong and Sun, 2016).

Limitations of ABE: The use of a single Trusted Authority (TA) in the ABE system. Single Trusted Authority (TA) is not only creates a load bottleneck. But also have key escrow problem and hence, the trusted authority can access all the encrypted data. This opens the door for potential privacy exposure.

MATERIALS AND METHODS

Problem statement: A number of cryptography techniques have been proposed in the recent scenario. There are many advantages and disadvantages in those algorithms. Cryptography is the one of the main categories of cloud security that converts information from its normal form into an unreadable form by using encryption and decryption techniques. Unsecured data that travels through different cloud networks are open to many types of attack. The cryptography ensures that the files in the cloud server should be sent without any alternations and only the authorized person can be able to open and read the files.

Existing system: Senders encrypt message with certain attributes of the legal and authorized receivers. The Hierarchical Attribute-Based Encryption (HABE) based access control method uses several tags to mark the attributes that a specific authorized user needs to possess. The users with certain tag sets can get access to the specific encrypted data and decrypt it.

Lots of research works introduced the scheme about the attribute based encryption access control method in the cloud computing environments. In the mobile cloud computing environment, there are incredible data which needs to be processed and marked with attributions for the convenient attributing access before storing the data. At in the same time, the hierarchical structure of the application users need an authentication center entity to control their attributes.

Proposed design; hybrid hybridized weight attribute-based encryption: This research work proposed a Hybrid Hierarchical Attributes Based Encryption (H-HABE) scheme by taking advantages of Attributes Based Encryption (ABE) and Hierarchical Identity Based Encryption (HIBE) access control processing. The proposed access control method using H-HABE is designed to be utilized within a hierarchical multiuser data-shared environment which is extremely suitable for a mobile cloud computing model to protect the data privacy and defend unauthorized or illegal access. Compared with the original HABE scheme, the new scheme can be more adaptive technique for mobile cloud

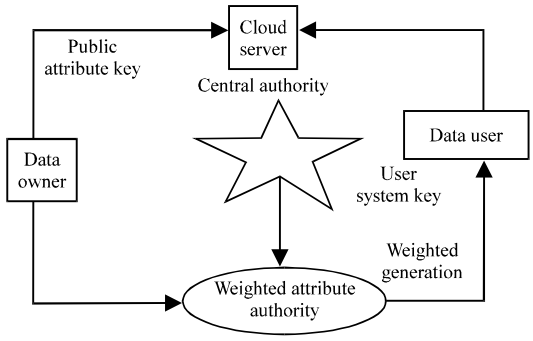

Fig. 1: Proposed AES and Blowfish Hybridized Attribute-Based Encryption (H-HABE) scheme

computing environment to process, store and access the huge data and files while our new system can let different privilege entities access their permitted data and files. Our new scheme not only accomplishes the hierarchical access control of mobile sensing data in the mobile cloud computing model but protects the data from being obtained by an entrusted third party.

In cloud computing, a secure and efficient data collaboration is achieved by the proposed Hybrid H-HABE approach. Most of the conventional ABE methods only have a single Authority (TA) to handles both the secret and public keys. However, in many circumstances, the consumers hold attributes from multiauthority and the data holders share the data with consumers who are managed by a distinct authority. Many different multiauthority attribute-based access control structures have been developed to resolve this problem. In access control systems with the intention of updating of the ciphertext, a data holder has presented online for all time, besides the attributes that are given similar status. In the proposed scheme, the weighing of attributes is given by the AES and blowfish algorithm to provide secure data in cloud computing. The system involved the five basic things: the data holder, who encodes the data before uploading the data to the cloud under an access control policy; a cloud server environment who provides data storing; a Weight Attribute Authority (WAA) to authorize the above, update and validate the attributes of users that are assigning different weights with respect to their prominence; a Central Authority (CA) which allocates a global user identifier for each consumer as well as allots user public key to the weight attribute authority and the data consumers, as illustrated in Fig. 1. In the proposed system, a AES and Blowfish algorithm is hybridized with weighted attributed authority as illustrated in Fig. 1.

In the proposed H-HABE system model, the hybrid of AES and Blowfish algorithm is applied to encrypt and

decrypt data and to generate keys randomly. Moreover, an image matching technique is employed for more security purposes.The system generates weight value for users based on its attributes. For example, if user A = Narmadha from the HR department and user B = Banu from the Research and Development Department, both users initially encounter the security phase. In case that the system acknowledges that user A is valid, then the system generates weight values for user A based on its attributes. According to the weight value, user A can decrypt the file which is assigned to its corresponding weight. Without the permission, user B cannot decrypt the document of user A. Though user B is a valid user, their weight rate does not match the weight rate of user A but user B can decrypt its corresponding document based on its weight value. This new approach is more prominent, reliable and more secure; besides, it is more applicable for real-time applications than the conventional methods in a cloud computing environment. Hybrid HABE encryption deals fine-grained access control, multiauthority security and collusion resistance. The proposed scheme is represented in two phases: the algorithm phase and the system phase. At the algorithm phase, the updated and combined AES and blowfish algorithm is described along with system-level operations. Conversely, at the system level, the high-level operations such as system setup, user annulment, new file creation, new user admit, file access and deletion are explained.

System level process: System level processes in the proposed system are described as.

System setup: The challenger execute a global setup algorithm to obtain the global public parameters. The data holder selects a security parameter, subsequently sends a request to algorithm phase interface setup as a consequence it yields the secret key S_K. The data holder then ciphers each S_K component and sends the encrypted components along with the signature to the Central Authority (CA).

Key generation: When a new user demands to connect to the system, the CA will allocate a unique user ID to the consumer. However, the consumer then ciphers its attribute set and sends it along with its signature to WAA.

Encryption: Before uploading a data file to the cloud environment, the data holder initially logs in with a unique ID and then randomly chooses a symmetric data file encryption key to encode the data.

Decryption: The data consumer initially downloads the data file from the cloud environment to the local and then requests the decryption algorithm to decrypt the data.

RESULTS AND DISCUSSION

Experimental setup: The algorithms are implemented using the Java (Eclipse Platform Version: 3.3.1.1) Experiments are performed on Intel Pentium processor with a 2.34 GHz and 1 GB of memory. In our research, we are used different size of text files in our experiments. The computational cost of encryption and decryption is computed.

Experimental result: All of these systems not only provide data security but also accomplish the access control of encrypted data ona cloud network environment. While comparing the data collaboration schemes of ABE and HABE, the proposed H-HABE achive partial signing and full delegation with less workload and also accomplishes lightweight key management in a large-scale consumer.

In the proposed scheme, various input files of different sizes (in kB or MB) are encrypted and decrypted by hybrid of AES and blowfish algorithm. Key generation and weight generation are also, done by our new algorithm. This algorithm is generated for security purpose and also it yields less execution timings for the "encryption and decryption process". The security aspect of our new encryption approach has been enhanced. The final outcome of the proposed scheme is illustrated in Table 1. The time taken for encryption and decryption

Table 1: Experimental results of execution time of encryption/decryption, throughput for ABE, BH-WABE and H-HABE

	Experimental results of execution time of encryption/decryption					
	ABE		BH-WABE		H-HABE	
Text file (kB)	Encryption time (sec)	Decryption time (sec)	Encryption time (sec)	Decryption time (sec)	Encryption time (sec)	Decryption time (sec)
18186.24	960.00	900.00	840.000	921.000	810.00	800.00
8739.626	2060.00	2120.00	2036.000	2135.000	1998.00	2078.00
8949377.024	3040.00	3100.00	3051.000	3158.000	3012.00	3008.00
Total time	6060.00	6120.00	5927.000	6214.000	5820.00	5886.00
Average time	2020.00	2040.00	1975.667	2071.333	1940.00	1962.00
Throughput	4443.71	4400.15	4543.42	4333.590	4626.96	4575.07

Table 2: The output of the testing

	ABE					BH-WABE					H-HABE				
	Encryption					Encryption					Encryption				
File Size	IE	Chrome	Opera	FireBox	Netsc	IE	Chrome	Opera	FireBox	Netsc	IE	Chrome	Opera	FireBox	Netsc
18186.24	960	936	990	1024	950	955	932	912	954	935	924	902	905	900	914
8739.626	2060	2004	2095	2150	2045	2100	1998	2100	2014	2010	1997	1932	1997	1845	1997
8949377.024	3040	2998	3120	3225	3005	3250	3122	3210	3015	3025	2985	2910	2898	2850	2942
Total time	6060	6045	6124	6185	6050	6120	6320	6124	6015	6010	5596	5874	5845	5750	5885
Average time	2020	1979.333	2068.333	2133	2000	2101.667	2017.333	2074	1994.333	1990	1968.667	1914.667	1933.333	1865	1951
Throughput	740.6191	749.0865	728.0642	713.3108	744.9214	722.4389	725.5337	727.0616	748.1499	749.274	780.4124	772.6203	770.8289	791.2123	7647217

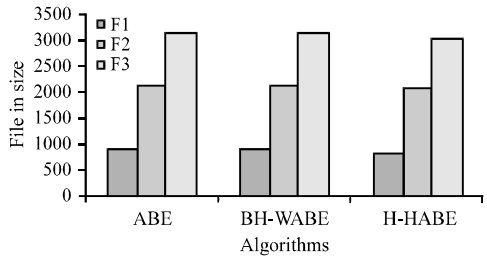

Fig. 2: Experimental results of execution time of encryption

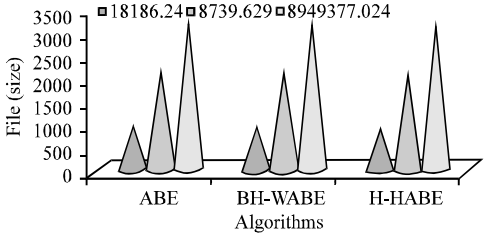

Fig. 3: Experimental results of execution time of decryption

process by the proposed H-HABE is compared with the conventional HABE scheme by considering the performance metrics. The performance metrics are calculated based on the following tasks:

- Calculate the encryption and decryption time for each algorithm using different sizes of input files
- The effect of changing the file size on encryption/decryption time
- Compute the power consumption for each algorithm in kB/sec (Fig. 1 and 2)

Comparison of web browser speed test: Different latest versions of web browsers are used in this research. The following factors affect the response time and speed of web browsers:

- Web browser's version
- Depends on the operating system installed in the computer
- Depends on the computer configuration

The first test focuses on how long it takes for each browser to launch from the time the user decides to open it until it appears on public display, ready for action. The

Fig. 4: Different popular web browsers available in the software market

test has been slightly changed from previous versions and is only timed up until it is ready for user communication. The graphics show that Chrome is unquestionably faster with Internet Explorer (in second place) followed by opera and finally Firefox which lagged behind by approximately 1 sec.

There are lot of web browsers that are available in the market but these five are known to be the most popular among the top. They are Internet Explorer (IE), Mozilla Firefox, Opera, Netscape Navigator (NN) and Google Chrome (Fig. 3).

The second test is all about how quickly each browser could open up with ten tabs that enabled with each tab containing a different URL with varying content ranging from the rediff money website to Facebook and Indian Express. Having nine tabs open from the beginning, will obviously place an increased load on the browser but Opera seems to have no problems at all as it finishes the processing task miles ahead of the competition with IE and Firefox achieves the objective at the same rate and Chrome is surprisingly in being in the distant fifth place.

The output of the testing will project the response time i.e., the encryption process and the time taken by the five web browsers, namely Internet Explorer (IE), Mozilla Firefox, Opera and Netscape Navigator (NN) and Google Chrome after performing the encrypting scripts timed in millisecond onto the computer screen (Table 2).

Advantages of proposed system:

- One ciphertext can be decrypted by several rounds keys

- Both precise level description and user attribute should be supported in the access structure of our new scheme /method
- The keys in the authentication center have to the same hierarchical structure just as the structure of users privilege levels

CONCLUSION

In this study, we introduced a new hybrid technique for cryptography using two algorithms (AES and Blowfish). This new technique gathering between symmetric and a symmetric encryption. This combination of using symmetric and a symmetric technique will give us the high security and everyone have his private key that can be used for decryption process by many people at the same time. In a cloud environment, user authentication and data security are the main challenging issues. Therefore, an efficient and scalable access control scheme has been proposed in this research paper. Further, this scheme employs a updated AES and blowfish hybridized weight attribute-based encryption mechanism not only to provide data security against the semi-trusted cloud service provider but also the Weight Attribute Authority (WAA) and the Central Authority (CA) provides lightweight key management in large scale-consumers.

The result shows that the proposed method H-HABE is efficient in terms of security, reliability and efficiency, as well as performing well when it is juxtaposed to the conventional HABE scheme by means of confidentiality, flexible access control, data collaboration, full delegation, partial decryption, verification and partial signing.

RECOMMENDATIONS

Futuremore, extent of the proposed work can be accessible, quality-based encryption and protection-saving property-based information-sharing with re-encryption.

REFERENCES

Cao, N., C. Wang, M. Li, K. Ren and W. Lou, 2014. Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE. Transac. parallel Distrib. Syst., 25: 222-233.

Choi, C., J. Choi and P. Kim, 2014. Ontology-based access control model for security policy reasoning in cloud computing. J. Supercomput., 67: 711-722.

Chu, C.K., S.S. Chow, W.G. Tzeng, J. Zhou and R.H. Deng, 2014. Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEE. Trans. Parallel Distrib. Syst., 25: 468-477.

Darwazeh, N.S., R.S. Al-Qassas and F. AlDosari, 2015. A secure cloud computing model based on data classification. Procedia Comput. Sci., 52: 1153-1158.

Darwazeh, N.S., R.S. Al-Qassas and F. AlDosari, 2015. A secure cloud computing model based on data classification. Procedia Comput. Sci., 52: 1153-1158.

Do, J.M., Y.J. Song and N. Park, 2011. Attribute based proxy re-encryption for data confidentiality in cloud computing environments. Proceedings of the 1st ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering, May 23-25, 2011, IEEE, Jeju Island, South Korea, ISBN:978-1-4577-0180-1, pp: 248-251.

Fabian, B., T. Ermakova and P. Junghanns, 2014. Collaborative and secure sharing of healthcare data in multi-clouds. Inform. Syst., 48: 132-150.

Hong, H. and Z. Sun, 2016. An efficient and traceable KP-ABS scheme with untrusted attribute authority in cloud computing. J. Cloud Comput., 5: 1-8.

Jiang, T., X. Chen, Q. Wu, J. Ma and W. Susilo *et al*., 2017. Secure and efficient cloud data deduplication with randomized tag. IEEE. Trans. Inf. Forensics Secur., 12: 532-543.

King, N.J. and V.T. Raja, 2012. Protecting the privacy and security of sensitive customer data in the cloud. Comput. Law Secur. Rev., 28: 308-319.

Lacuesta, R., J. Lloret, M. Garcia and L. Penalver, 2011. Two secure and energy-saving spontaneous ad-hoc protocol for wireless mesh client networks. J. Netw. Comput. Appl., 34: 492-505.

Li, J., X. Huang, J. Li, X. Chen and Y. Xiang, 2014. Securely outsourcing attribute-based encryption with checkability. IEEE. Trans. Parallel Distrib. Syst., 25: 2201-2210.

Li, M., S. Yu, Y. Zheng, K. Ren and W. Lou, 2013. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans. Parallel Distrib. Syst., 24: 131-143.

Modi, C., D. Patel, B. Borisaniya, A. Patel and M. Rajarajan, 2013. A survey on security issues and solutions at different layers of Cloud computing. J. Supercomputing, 63: 561-592.

Ranchal, R., B. Bhargava, L.B. Othmane, L. Lilien and A. Kim *et al*., 2010. An approach for preserving privacy and protecting personally identifiable information in cloud computing. Proceedings of the 29th IEEE International Symposium on Reliable Distributed Systems (SRDS 2010), October 31-November 3, 2010, IEEE, New Delhi, India, pp: 368-372.

Ruj, S., M. Stojmenovic and A. Nayak, 2012. Privacy preserving access control with authentication for securing data in clouds. Proceeding of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), May13-16, 2012, IEEE, Ontario, Canada, ISBN:978-1-4673-1395-7, pp: 556-563.

Ruj, S., M. Stojmenovic and A. Nayak, 2014. Decentralized access control with anonymous authentication of data stored in clouds. Parallel Distrib. Syst. IEEE. Trans., 25: 384-394.

Samanthula, B.K., Y. Elmehdwi, G. Howser and S. Madria, 2015. A secure data sharing and query processing framework via. federation of cloud computing. Inf. Syst., 48: 196-212.

Singh, S., Y.S. Jeong and J.H. Park, 2016. A survey on cloud computing security: Issues, threats and solutions. J. Network Comput. Appl., 75: 200-222.

Wang, H., S. Wu, M. Chen and W. Wang, 2014. Security protection between users and the mobile media cloud. IEEE. Commun. Mag., 52: 73-79.

Wei, L., H. Zhu, Z. Cao, X. Dong and W. Jia *et al*., 2014. Security and privacy for storage and computation in cloud computing. Inf. Sci., 258: 371-386.

Xu, Z., W. Kang, R. Li, K. Yow and C.Z. Xu, 2012. Efficient multi-keyword ranked query on encrypted data in the cloud. Proceedings of the IEEE 18th International Conference on Parallel and Distributed Systems, December 17-19, 2012, Singapore, pp: 244-251.

Yan, Q. and F.R. Yu, 2015. Distributed denial of service attacks in software-defined networking with cloud computing. IEEE. Commun. Mag., 53: 52-59.

Younis, Y.A., K. Kifayat and M. Merabti, 2014. An access control model for cloud computing. J. Inf. Secur. Appl., 19: 45-60.