Secure User Data in Cloud Computing through Prevention of Service Traffic Hijacking and Using Encryption Algorithms

Nilosha Pereira, Vimukthi Elvitigala, Mahesha Athukorala, Piumi Fernando, Dineth Ehelepola, Kosala Sameera, Dhishan Dhammearatchi

Sri Lanka Institute of Information Technology Computing (Pvt) Ltd

Abstract- Cloud computing has become an emerging technology infrastructure in the IT industry. Reasons for the sudden boom of this model were the advantages it offers to the users. Cloud computing is a service over a network connection which shares enormous amount of resources rather than having to build the infrastructure in house. Other than sharing resources cloud computing offers flexibility, reduced capital costs, achieving economies of scale, globalize workforce etc. Cloud computing technology has some serious drawbacks which now has overrun the benefits it offers. The security of the user data is crucial when adopting a cloud computing model. Several methods have been implemented in securing user data such introducing encryption algorithms. Service traffic hijacking creates a major concern on using cloud computing for this allows the hacker to access the credentials of the genuine user hence he or she can eavesdrop on the user’s activities and transactions, manipulate user data, return false information and redirect your client to illegitimate sites. In this paper we propose remediation to prevent intruders of accessing unauthorized data and using and encryption algorithm efficiently to neutralize the security threats.

Index Terms- Cloud Computing, Data Security, Encryption, Algorithms, Service Traffic Hijacking, Issues and Threats.

I. Introduction

Today CLOUD COMPUTING represents one of this era’s most significant shift in the IT industry. This model reaches the point where utilizing the resources among sharing through a virtual network while offering practical benefits to different sets of stakeholders which search upon different needs. By releasing a pool of resources to the network where to access requesting an authentication spanning of organization area has become much simpler than old days. Cloud computing can be referred as a system which provides IT facilities ‘as a service’ to the end user in the network. Achieving economies of scales, flexibility, capital-expenditure free, increased collaboration, competitiveness, globalizing workforce and document control are some major benefits cloud computing has to offer. Carrying all the advantages some concerns make us to rethink using this model. Mainly users are stuck with risks associated with cloud computing when security measurements are not implemented wisely. This results in hijacking the user credentials, data loss, data manipulation and various kind of issues.

II. Background and Related Works

The service model of the cloud computing is distributed into three key groups (a) IaaS (infrastructure as a service), compute properties, enhanced by storage and networking competencies are owned and hosted by a service provider and presented to consumers on-demand. (b) PaaS (plat form as a service), is used for applications, and other development, while providing cloud components to software. (c) SaaS (software as a service) lets the external user to access online applications and software that are hosted by the third party [1] [7].Cloud computing is also can compare to grid computing. By using the cloud computing users can access to the applications from anywhere in the world. Therefor cloud computing infrastructure is also can introduce as a kind of parallel and distributed systems [4]. There are many type of cloud infrastructures implemented. In private clouds; Services are provided exclusively to trusted users via a single-tenant operating environment. An organization’s data center give cloud computing services to clients who may or may not be in the premises [16]. Public clouds are the contradictory: services are offered to individuals and organizations who want to retain elasticity and responsibility without fascinating the full costs of in-house infrastructures [16]. Public cloud users are treated as untrustworthy. There are also hybrid clouds [16] [17].The Cloud Computing has been envisioned to the next-generation design of IT Enterprise. It transports the application software and databases to the integrated huge data cores, where the management of the data and services may not be fully trustworthy. This kind of unique paradigm brings about more new security problems, which have not been well recognized.The Security solutions have to make a trade-off between the amount of security and its performance and impact on the end-user experiences. This is the accentuated in a cloud computing environment users desiring different level of security share the same resources. An important issue for cloud computing is the observation of security, which is beyond the basic technical details of security solutions [18]. And the security is the most important factor in cloud computing. This issue make a threat in securing the consumer data. To make consumer data to be secure, it is necessary to implement an efficient and secure data access control method.There are so many security challenges and threats in cloud computing. These are some of them. Abuse and nefarious use of cloud computing, malicious insiders, shared technology weaknesses, data harm and service traffic hijacking and etc.

Attribute Based Encryption is a technique which we can use to secure consumer data. In encryption technique there are some advanced encryption algorithms that can be applied to the cloud computing to increase the protection of privacy. Attribute-based encryption is one of those algorithms [5]. Another encryption method to secure data in a cloud environment RSA encryption method. RSA encryption method uses a cryptographic algorithm where the encryption key is public and varies from the decryption key which is kept top-secret. DES is another method where it uses symmetric key for both encryption and decryption [1].

RSA is asymmetric encryption and decryption algorithm. How this algorithm does the magic is it encrypts the user data for security purposes so that only the genuine authorized user can access the data. Data will be stored on the cloud and depending on the user requests the data will be delivered. In this scenario the public key is known to everyone but the private key is known only by the authorized user. After the user authentication at the cloud environment data which was encrypted using the public key by the cloud service provider the requested data will be decrypted by the cloud user using the private key. Data encryption standard known as DES encrypt data within blocks with the size of 64 bits each. This produces 64 bits of cipher text. And the same key is used for encryption and decryption which the size of the key of this algorithm goes up to 56 bits. The initial vector size is 64 bit as mentioned above and the security is applied for both provider and user [2].There are some more valuable and high quality encryption algorithms which can be applied into the cloud computing to increase the protection of privacy. ABE, Key-policy (KP-ABE), Ciphertext-policy (CP-ABE), ABE with Non-monotonic Access Structures are some of those algorithms. In the CP-ABE algorithm, it is the alteredmethod of Attribute based Encryption (ABE) scheme to further. In CP-ABE, the policy of the access is converted in to the encrypted data. The set of attributes which are related with the user's private key and the user's access policy which is built in the cipher text. When the situation of set of attributes in the user's private key fascinate the structure of the access of encrypted data, the user can decrypt the encrypted data [6].

In cryptography a fully homomorphism encryption scheme is used. It allows data to be processed without being decrypted. SSL/TLS protocols are used here [10]. In front of every data packet Diffie- Hellman is used as the addition of message header. When a cloud server accepts anapplication for data storage from a user then it individually generate the public and private key with user identification [9] [11].It send the user secret key and unique identification to user. Two task are performed at user end before a user sends the files to cloud by using secret key. At firstly, a message header is added to the data and secondly, data is encrypted in clouding message header, cloud server will pick the SID information and check the message header of received data when a user will make request for data [12].

Blowfish is block cipher 64-bit block- which can be used as a Substitute for the DES algorithm. Its structure is similar to IDEA algorithm [13] [14]. It takes ainconstant length key, fluctuating from 32 bits to 448-bits [15]. Blowfish is successor of two fish. The algorithm waspresented in 1993 by Bruce Schneider, and has not broken until now. It is also noteworthy to point out that this algorithm can be enhanced in hardware applications, is often used in software applications, although it is like most other ciphers. The encryption is almost like feistel network of 16 rounds. Blowfish is a symmetric block encryption algorithm. It can run in less than 5K of memory. It uses XOR, addition, lookup table with 32-bit operands. The length of key is variable, it can be in the range of 32~448 bits and the default 128 bits key length. This is very useful for applications where the key does not change often, or communication link like an automatic file encryption. In Blowfish symmetric block cipher algorithm it encrypts data of 64-bits at a time. It follows feistel network and this algorithm is divided into two parts. Key Expansion and Data Encryption are the two main parts. In Key Expansion it will converts a key of most 448 bits into several sub key arrays which makes totaling 4168 bytes. In Data Encryption, It is having a function to iterate 16 times of network. Every round consists of key-dependent permutation and data dependent substitution and a key. All operations are done in XORs and additions on 32-bit words. Four indexed array data lookup tables for each round is the only additional operations taken place here [13] [14] [15].

Another drawback of cloud computing is service traffic hijacking where an intruder uses the stolen credentials of the authorized user and access their information. This results in eavesdrop on the user's activities, sensitive data, transactions and manipulate user data. There are real world scenarios where intruder has return false information and redirect the client to illegitimate sites. In year 2012 intruders managed to get access of the CEO of CloudFare's personal Gmail account. Another incident occurred in the same year where hackers used usernames and passwords stolen from third-party sites to access Dropbox users' accounts [3].

Insider threat challenges the security of general data security including cloud computing. Insider threat might be caused by a problematic employee of a cloud provider accessing sensitive customer data. Yet despite these security concerns, cloud computing is developing and continues to grow [8].

III. Service TRAFFIC HIJACKING

Service Traffic Hijacking Process

Account hijacking is carried out by the stolen credentials of the genuine user. Using the credentials the hacker can access sensitive data and manipulate data as per his likeness. Service traffic hijacking involves in hacker eavesdropping on activities, manipulating data, accessing data and returning falsified information.There are three states where the security breach can be occurred.

1. Transmission of sensitive data to the cloud server.
2. Transmission of sensitive data from cloud server to the client's computer.
3. The storage of sensitive data of the client's on the cloud servers which are remote and not owned by the client.

Fig 1, shows how the service traffic hijacking is occurred.

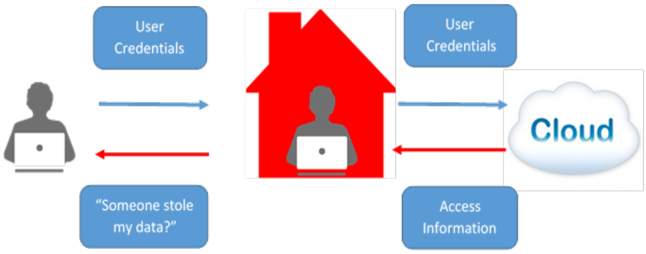

Fig. 1. – Service Traffic Hijacking

In fig 1, the left most side picture is where the genuine user enters the credentials to log in to the cloud server. This is where the intruder hacks and retrieve or eavesdrop on the activities and uses the sensitive data.

Security is the most essential aspect of the cloud computing technology. As this model's approach sensitive data can be stored on both client as well as cloud server sides. This is why identity management and authentication are crucial in cloud computing.

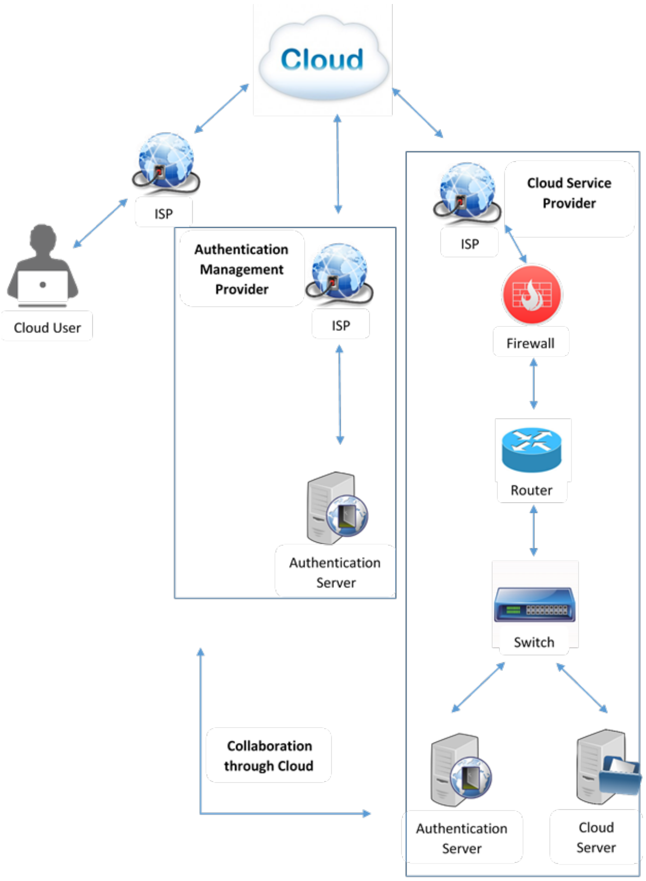

Fig. 2. –Cloud Authentication Process

Fig 2, explains the process of authenticating the user by the cloud service provider as well as the collaboration between a third party authentication management providers to strengthen the security in the cloud infrastructure.

Areas of business to personal life can be ruined by the hackers manipulating or retrieving sensitive information stored on cloud. There are real life incidents where pictures of individual's life events were published to the internet after hacking into their personal cloud account by hijackers. Attacker uses the stolen account data to conduct unauthorized activities. One instance is where an attacker uses a stolen credentials to act as the genuine account owner. Company integrity and reputations can be destroyed. Confidential data can be leaked or manipulated thus generating significant cost to industries or their consumers.

Prevention of Service Traffic Hijacking

There are few alternatives to be used to prevent service traffic hijacking. Observing user behavior can help to identify suspicious activities. Cloud user's normal behavior stays as the same with the time. Proactively monitoring user behavior detect unusual events such as downloading massive amount of data in a short period of time. Some cloud service providers use this technique. Blocking the account for a period of time when suspicious activity occurs helps the genuine user to save his sensitive data.

Implementing a two factor authentication ease the security breach which the cloud technology currently undergo. Hijacker needs two authentications to enter in to the user information. One authentication will not satisfy the requirements to enter thus this way hacker would not be able to penetrate the system and manipulate sensitive data.

Prohibiting the sharing of the credentials between user and the service closes the door to hijackers on stealing the account credentials. This is where hijacker can easily access and retrieve the credentials.

Understanding cloud provider service polices as well as service level agreements can help to reduce the threats. At the contract level before signing the agreement the consumer should seek satisfying requirements to ensure the sensitive data is at a safe place.

To do so some recommendations should be followed. Check the security standard of the service provider and your ability to audit their compliance. The consumer should have the right to remove data which is been stored and the right to get them back whenever desired. The right to discontinue the service and remove all the information permanently should be done at the hands of the user and whenever there is a security breach customer should know how the information is protected as well as the remedies for failure.

IV. Encryption in Cloud Computing

Encryption Process

Nowadays, cloud computing acts a very important role in modern IT technology. But there are so many security challenges and threats in cloud computing. As a solution for this cloud data encryption mechanism is introduced. In cloud encryption customer's data in cloud service converted in to cipher text. Many organizations in the world, which already have basic protection also consider about implementing encryption solutions.

There are certain steps of process of data encryption .The data pass through a mathematical formula called algorithm which converts it into encrypted data called cipher text. Encapsulate the message with key create a key by these algorithms .There are two types of encryption and they are asymmetric and symmetric.

Firstly we talk about asymmetric encryption. There are two mathematically-related keys which are used. In public key (asymmetric) encryption: one to encrypt the message and the other to decrypt it. These two keys combine to form a key pair both data encryption and parties of the communicating identities validation and is measured more protected than symmetric encryption which is delivered by asymmetric encryption but is computationally slower.

Major parts of a public key are Plaintext: text message applied by to an algorithm, Encryption algorithm: performs scientific processes to manner substitutions and transformations to the plaintext; Private and Public key: pair of keys where one is used for decryption and the other for encryption; Cipher text: by using the algorithm to the plaintext message using key scrambled or encrypted message produced, Decryption Algorithm: this algorithm generates the marching key and the cipher text to produce the plaintext.

These are the steps of asymmetric data encryption process: using mathematical generated code formula encryption begins by converting the text to a pre-hash code; Using the senders private key this pre-hash code is encrypted by the software; Using the algorithm used by the software private key would be generated; The encrypted message and the pre-hash code are encrypted again using the senders private key; Then to retrieve the public key of the person this information is intended for sender of the message. The sender encrypts the secret key with the recipient's public key, therefore only the receiver can decrypt it using the private key, thus concluding the encryption process.

Private Key encryption also mentioned to as orthodox or single-key encryption is rest on secret key that is shared by both communicating parties to share a common key it enquires all parties that are communicating the distribution party uses the secret key as share of the scientific process to encrypt (or encipher) plain text to cipher text. The same secret key uses the receiving party to decrypt (or decipher) the cipher text to plain text.

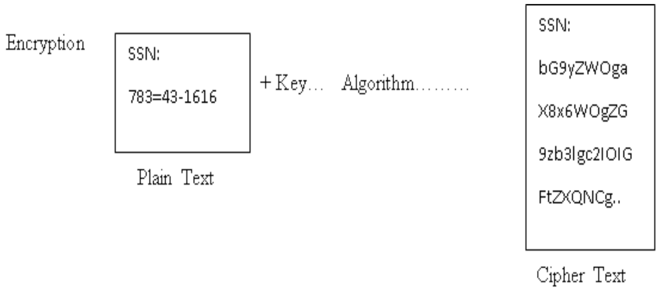

Fig. 3. –Encryption Process

Fig 3, describes the process of the encryption where the sub processes creates the cipher text and how the key is been used. It is required that the sender and receiver have a way to exchange secret keys in a secure manner when using this form of encryption. Communications will be insecure if someone knows the secret key and can figure out the algorithm. There is also the need for a strong encryption algorithm. They would be unable to determine the encryption algorithm, means of this is that if someone were to have a cipher text. Cryptanalysis is a method of attack that attacks the features of the algorithm to reduce whichever a specific plaintext or the key used. Brute force is just as it conveys; using a method to find every imaginable mixtures and finally decide the plaintext message one would then be able to symbol out the plaintext for whole past and upcoming communications that continue to use this compromised setup.

There are so many advantages in encryption. As one of a major advantage can take that encryption protect the cloud data completely. After encrypting the data it is very difficult to decode the information. And also provides the security for the encrypted data during transmission. This also can take as one of a major advantage in data encryption. Encryption supports to accomplish secure multi-tenancy in the cloud. Encryption key services avoid service providers from accessing and manipulating customer data. When the service providers have both client's encrypted information and encrypted keys, they will able to access to data. To avoid this problem, gives customer's own encrypted keys. Encryption allows customers to secure their remote offices.

Although there is having so many advantages in cloud data encryption there are some disadvantages too. The main basic purpose of encrypting data is that someone can decrypt it when it needed. The encrypted keys are the most necessary thing in encryption. If customer lose these keys, it will take uncountable time to access their data. Although with using data encryption can supply more security to cloud data, some of hackers and thieves will able to access the cloud data. Therefore as a solution for this problem can use a strong username and a strong password for decryption process. And also can encrypt the data more than one time. This will make more difficult for hackers to access to the encrypted cloud data.

Breach of the data also a major problem in cloud computing. When it comes to data encryption breach of data also can be happen. Most of organizations must be more specifically concern about this. As a solution for this can use advanced parity checking mechanism to check data while in encryption, transmission and decryption.

Proposed Encryption Method to Increase Security

Current encryption methods were able to reduce the security threat but have not completely removed the issue. To increase the efficacy of the encryption a new approach can be used.

Fig 4, conveys the process of using a symmetric encryption key in cloud computing infrastructure. Client will have two keys which the key one will be used to encrypt the symmetric key and the second key will be used to decrypt the symmetric key. Encrypting the encoded text and decrypting the text will be done by the above created symmetric key.

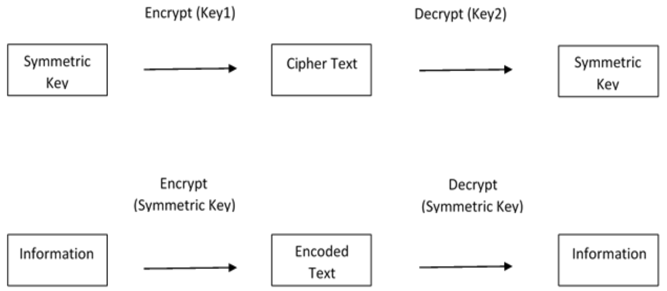

Fig. 4. –Proposed Encryption Method

V. Conclusion

This paper describes the process of encryption as well the process of service traffic hijacking. Based on the findings and discussed cloud computing is becoming an emerging technology which contribute individuals to the government level in various area.With massive amount of advantages breach of security in cloud system makes the user rethink of using the cloud technology. One disadvantage of the infrastructure is service traffic hijacking where the credentials of the user is stolen and sensitive data is manipulated and used by a hijacker. By implementing a two factor authentication and observing user behavior to identify malicious activities can ease the security threats. Prohibiting the sharing of user credentials as well as understanding service legal agreement can help business whenever there is a security breach. Using encryption methods to encrypt the user data makes it harder to decrypt for private key is with the genuine user and it is not published. Various encryption methods can be used to maximize the security in cloud infrastructure based on the current requirements and even third party authentication server can be used. By using two keys to encrypt and decrypt the symmetric key increased security status can be achieved. Symmetric key can be used to encrypt and decrypt the information thus the hacker needs to have more than one key to retrieve information.

Future Work

The main drawback of the encryption process is the complexity of the algorithm as well as the process of implementation. Information should be decrypt and encrypt in matter of seconds thus increasing the number of key needs to be optimized well to increase the efficiency. Prevention of hijacking should also be a responsibility of the cloud user as well. There need to be more steps done by the cloud user to prevent hackers obtaining the credentials which we did not discussed in this paper.

Acknowledgement

Our sincere thanks go to our supervisor Dhishan Dhammearatchi of Sri Lanka Institute of Information Technology Computing (Pvt) Ltd as well as all the authors whom we have referred in this research paper.

References

[1] A. Soofi, M. Khan and F. Amin, "Encryption Techniques for Cloud Data Confidentiality", International Journal of Grid and Distributed Computing, vol. 7, no. 4, pp. 11-20, 2014

[2] Rachna Arora, AnshuParashar, “Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications, vol. 3, no. 4, pp. 1922-1926, 2013

[3] C. Barron, H. Yu and J. Zhan, "Cloud Computing Security Case Studies and Research", in World Congress on Engineering, London, 2013.

[4] K. Goodarzi and A. karimi, "Cloud Computing Security by Integrating Classical Encryption", Procedia Computer Science, vol. 42, pp. 320-326, 2014

[5] V. Ashktorab and S. Taghizadeh, "Security Threats and Countermeasures in Cloud Computing", www.ijaiem.org, 2012. [Online]. Available: http://www.ijaiem.org/volume1Issue2/IJAIEM-2012-11-3-076.pdf. [Accessed: 19- Feb- 2016]

[6] R. Nallakumar, S. Ayyasamy and M. Nithya, "An Assessment on Attribute Based Encryption Techniques in Cloud Computing", www.ijsetr.org/, 2014. [Online]. Available: http://ijsetr.org/wp-content/uploads/2014/10/IJSETR-VOL-3-ISSUE-10-2607-2611.pdf. [Accessed: 19- Feb- 2016]

[7] S. Singla and J. Singh, "Cloud Data Security using Authentication and Encryption Technique", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 2, no. 7, 2013

[8] A. Mahajan and S. Sharma, "The Malicious Insiders Threat in the Cloud", International Journal of Engineering Research and General Science, vol. 3, no. 2, 2015

[9] V. Alangar, "Cloud Computing Security and Encryption", International Journal of Advance Research in Computer Science and Management Studies, vol. 1, no. 5, 2013

[10] R. Padhy, M. Patra and S. Satapathy, "Cloud Computing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), vol. 1, no. 2, 2011

[11] U. Somani, K. Lakhani and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing," Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on, Solan, 2010, pp. 211-216.

[12] S. Han and J. Xing, "Ensuring data storage security through a novel third party auditor scheme in cloud computing," Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on, Beijing, 2011, pp. 264-268.

[13] K. Ughade and N. Chopde, "Survey on Security Threats and Security Algorithms in Cloud Computing", International Journal of Science and Research (IJSR), vol. 4, no. 4, 2015

[14] M. P. Leong, O. Y. H. Cheung, K. H. Tsoi and P. H. W. Leong, "A bit-serial implementation of the international data encryption algorithm IDEA," Field-Programmable Custom Computing Machines, 2000 IEEE Symposium on, Napa Valley, CA, 2000, pp. 122-131

[15] V. Vinaya and P. Sumathi, "Implementation of Effective Third Party Auditing for Data Security in Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, 2013

[16] A. Adamov and M. Erguvan, "The truth about cloud computing as new paradigm in IT," Application of Information and Communication Technologies, 2009. AICT 2009. International Conference on, Baku, 2009, pp. 1-3

[17] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis and A. Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research," in IEEE Internet Computing, vol. 13, no. 5, pp. 10-13, Sept.-Oct. 2009

[18] K. Hamlen, M. Kantarcioglu, L. Khan and B. Thuraisingham, "Security Issues for Cloud Computing", International Journal of Information Security and Privacy, vol. 4, no. 2, pp. 39 - 51, 2010

Authors

First Author – Nilosha Pereira, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd

Second Author – Vimukthi Elvitigala, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Third Author – Mahesha Athukorala, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Fourth Author – Piumi Fernando, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Fifth Author – Dineth Ehelepola, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Sixth Author – Kosala Sameera, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Seventh Author – Dhishan Dhammearatchi, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd