Utilization of Service Traffic Hijacking and Secure APIs for the Security Enhancement of Cloud Computing

Ailapperuma D C R, Kaushalya A H L D C, Bandara H.M.P.M, Ranghadari M.I.T, A.B.M.U.I.Bandara, Mr. Dhammearatchi D

Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka

Abstract- Cloud computing implies the concept of accessing information over the internet as a unit of storage, which enhances the accessibility of a variety of services provided. Emergence of wireless and remote distribution of services all over the world using the technical innovations plays a key role in the global Information Technology (IT) boost, unfolding a new era of communication technology, where cloud computing provides a unique media of controlling and designing enhanced improvements in Security issues. The security of the cloud storages plays an exceptional role in respect of providing reliable services through the cloud. In the aspects of the security; the management of data and its control, the confidentiality over the information which are stored, the privacy of the users and their authentications focus on specific and parallel concentration with respect to each other. Moreover, with the enhancement of the technology over past decades, the security concerns acquire special attention by the users and clients over the internet. Depending on that, the Application Program Interface (API) security and the Service traffic hijacking have become major concerns over the access of cloud computing. Attending on to the overall purpose of this study is to address the improvement of security features over providing a specialized, reliable and a unique service with respect to the security measures. The research problem focusing on the arena of furnishing the improvements required in the research and the development of the required security enhancements concentrating on API security and the Service traffic hijacking through the Cloud computing services. This research paper analyzes on the references over the above addressed issues where the quality of the cloud services depends on. The research study examines on the major findings of the research, utilizing a specific methodology in emphasizing and drawing the necessary attention of the specified research problem, interviewing the exact procedure for the research requirements.

Index Terms- Cloud Computing, Wireless, Remote, Improvements, Communication, Media, Confidentiality, Storage, Security, Confidentiality, Authentications, Internet, API, Service Traffic Hijack

I. Introduction

Cloud computing contains activities such as the use of social networking sites and other forms of interactive computing. However, cloud computing is concerned with accessing online software applications, data storage and processing power. Cloud computing is a way to rise the capacity or add capabilities dynamically without investing in new structure, training new personnel or certifying new software. It extends Information Technology's existing capabilities. In the last few years cloud computing has grown-up from being a promising business concept to one of the fast growing fragments of the IT industry. Information on individuals and companies are positioned in the cloud concerns are beginning to develop about how safe an environment it is. In spite of of all the hype surrounding the cloud customers are still disinclined to deploy their commercial in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security placed first as the greatest challenge issue of cloud computing.

From one point of view, could security improve due to centralization of data and raised security-focused resources. On the other hand, concerns persevere about loss of control over certain sensitive data, and the lack of security for stored kernels entrusted to cloud providers.

The following research papers is based specifically on the service traffic hijacking and the API security views of the cloud computing architecture where the solutions of the approaches are provided through the methodology described in the latter chapters.

II. BACKGROUND AND RELATED WORKS

Kuyoro S. O et.al in 2011 published a paper with regards to the security issues and challenges of the cloud computing technology, where they addressed on the delivery models of the cloud computing infrastructure explaining the deployment models as private, public and hybrid cloud models. Moreover, the research team address on the issues categorizing them under service models as SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). Moving on to the challenges described, the major challenges with respect to security, costing model, charging model, Service Level Agreement (SLA), cloud interoperability issue are described in the point of view of organizations. The research paper does not go into a detail view of the issues addressed, but provides the view with a few examples. [1] Muhammad Kazim and Shao Ying Zhu in 2016, followed a research addressing on some of the dangerous issues of cloud computing technology. The researchers explain the issues on the hardware, virtualization, network, data and service providers which are caused during the implementation of the cloud computing. The effect of cloud computing components over the users and the providers, as well as the solutions that should be taken in order to overcome these issues. The best practices as well as the steps to be followed by the cloud administration are being focused when going into more detail. The analysis is based on the top security threats for cloud computing presented by Cloud Security Alliance (CSA). The behavior of the threats over the cloud, and the suggesting aspects of the control over these threats are described. The following are discussed over these threats, as

Data threats including data breaches and data loss, Network threats including account or service hi- jacking, and denial of service, Cloud environment specific threats including insecure interfaces and APIs, Malicious insiders, Abuse of cloud services, Insufficient due diligence and Technology vulnerabilities. [2]

During the study carried out by Ahmed et. al in 2014 discussed on the issues related to cloud architecture where the team focused on the security issues of cloud computing. The form of the cloud architecture on the views of cloud architecture and the hierarchical arrangement based on which a cloud is perceived in the form of IaaS, PaaS and SaaS from any cloud end-user's viewpoint. Moving forward, the research team describes on the authentication of cloud with regards to sensitive data stored both at clients' end as well as in cloud servers. This research also describes the different kinds of attacks that can be faced by a cloud architecture over the sensitive data, where the importance of taking necessary steps to avoid these issues are provided. Data segregation and session hijacking are pointed as unavoidable threats for the users, which causes Data loss and various botnets that place in action to override security measures of cloud servers. [3]

"Cloud Computing: Security Issues and Research Challenges" is a one of research paper describing what cloud computing is, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry. They describe many concepts to short cloud computing. But in this research paper they do not talk about the API security and the Service traffic hijacking concept [4].

"Security Issues and their Solution in Cloud Computing" is written by Prince Jain. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so that the customer does not face any problem such as loss of data or data thief. In this research paper they list some tips and tricks that cloud security solution. There are Verify the access controls, Control the consumer access devices, Monitor the Data Access, share demanded records and Verify the data deletion. In this research did not attention about API security [5]. "SURVEY PAPER ON SECURITY IN CLOUD COMPUTING" is one of research paper to discuss about cloud computing. It helps to transfer or storage of heavy data easy to be transferred and maintained for usage. In latter organizations are known as Cloud Service Providers (CSP) but it levies high cost on the users and at the same time it gives business to other organizations as well. So, cloud computing is fast becoming popular. There are more Security Concerns in Cloud Computing with low cost. In Cloud Computing they use different algorithms for different task. but they also no use API security or Service traffic hijacking concept [6].

Cloud computing is a complete new technology. It is the development of parallel computing, distributed computing grid computing, and is the combination and evolution of Virtualization, Utility computing, Software-as-a-Service (SaaS), Infrastructure-as-a- Service (IaaS) and Platform-as-a-Service (PaaS). Cloud is a metaphor to describe web as a space where computing has been pre-installed and exist as a service; data, operating systems, applications, storage and processing power exist on the web ready to be shared. To users, cloud computing is a Pay-Per-Use-On- Demand mode that can conveniently access shared IT resources through the Internet [7].

Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is rapidly moving towards cloud based architecture. While it is important to take advantages of could base computing by means of deploying it in diversified sectors, the security aspects in a cloud based computing environment remains at the core of interest. Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology [8].

Security concerns have given rise to immerging an active area of research due to the many security threats that many organizations have faced at present.

Addressing these issues requires getting confidence from user for cloud applications and services. In this paper, we have cast light over the major security threats of cloud computing systems, while introducing the most suitable countermeasures for them. We have also cited the aspect to be focused on when talking about cloud security. We have categorized these threats according to different viewpoints, providing a useful and little-known list of threats. After that some effective countermeasures are listed and explained [9]. The research explains Cloud computing environments are likely to suffer from a number of known vulnerabilities, enabling attackers either to obtain computing services for free (attack against cloud providers), steal information from cloud users (attack against cloud customers' data), or penetrate the infrastructure remaining in client premises through cloud connections (attack against cloud customer infrastructures). Typical examples of these attacks today are VoIP free calls, SQL injection, and drive by downloads. Cloud networking will not change the fact that vulnerabilities will continue to exist and that attackers will continue to exploit them. Big IT giants like Google, Amazon, and salesforce.com are providing computing facility like storage, computation and application by pay as per usage through Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) cloud service models. Since cloud computing supports distributed service oriented architecture, multiusers and multi- domain administrative infrastructure, it's more prone to security threats and vulnerabilities. Security issues are of more concern to cloud service providers who are actually hosting the services. In clouds rather than other issues security is the biggest issue. By Securing the Saas, PaaS and IaaS security issues indirectly we can secure the cloud system [10].

In this research paper describe security has always been the main issue for IT executives when it comes to cloud adoption. In two surveys carried out by IDC in 2008 and 2009 respectively, security came top on the list.

Cloud computing is an agglomeration of technologies, operating systems, storage, networking, virtualization, each fraught with inherent security issues. For example, browser based attacks, denial of service attacks and network intrusion become carry over risks into cloud computing. There are potentials for a new wave of large-scale attacks via the virtualization platform. Chow et al. Research paper described the “Fear of the Cloud” by categorizing security concerns into three traditional concerns, availability and third party data control. Research firm Gartner posited seven security risks ranging from data location and segregation to recovery and long-term viability. The European Network and Information Security Agency also published a list of 35 issues in cloud computing in 4 categories. Organizations such as ISACA and Cloud Security Alliance publish guidelines and best practices to mitigate the security issues in the cloud Cheap data and data analysis [11].

D. Mukhopadhyay, G. Sonawane, research paper expresses that Cloud computing allows consumers and corporate structures to use all the applications by the cloud without the extra effort of installation and also offers to access personal files from any computer with Internet access. According to the paper, technology offers access to a huge number of sophisticated super computers and their resulting processing power, connected at numerous locations around the world, thus contribution speed in the tens of trillions of computations per second. This paper solves the problem of most of the threats that data stored in the cloud faces. AES (Advanced Encryption Standard) is one of the most secure encryption algorithms and not many attacks are effective on data which is encrypted using AES. This framework also suggests the use of login id and password to confirm authentic and authorized access to a user’s data [12].

Cloud computing is a trendy technology that captured all around world. Day by day cloud applications becoming more and more popular. With the evolution of technology, security issue is the main problem for cloud based technologies. Encrypting and adding security passwords to a cloud system is a common solution for this. According to S.Sharma and A.Chugh they proposed an encrypted file system to overcome this problem on cloud storages. Since cloud storage is only one area of cloud computing, encrypted file system does not satisfy all security risks. Session hijacking attacks can gain access to cloud systems. Creating back door access to a cloud system can be very dangerous since all the data and files stored in these systems. If something happen to data it will be a big issue. This research suggests ways to avoid data modifying [13].

S. Khan, R. Tuteja focuse on the Benefits of cloud storage by access anyplace, anyhow, anytime, scalability, resilience, cost efficiency, and high reliability of the data. The proposed work plan is to eliminate the concerns regarding data privacy using cryptographic algorithms to increase the security in cloud as per different perspective of cloud customers. From this paper to encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms used. This research provides a shared pool of properties, including data storage space, networks, computer processing power, and specialized corporate and user applications [14].

III. OUR APPROACH

Account capturing is done by the stolen certifications of the bona fide client. Utilizing the accreditations the programmer can get to delicate information and control information according to his similarity. Administration movement capturing includes in programmer listening stealthily on exercises, controlling information, getting to information and returning adulterated information. There are three states where the security break can be happened. 1. Transmission of delicate information to the cloud server. 2. Transmission of delicate information from cloud server to the customer's PC. 3. The capacity of delicate information of the customer's on the cloud servers which are remote and not claimed by the customer. Fig 1, demonstrates how the administration activity commandeering is happened.

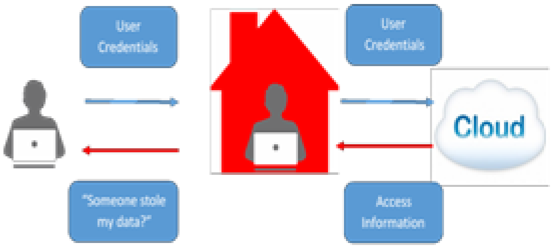

Fig. 01. – Service Traffic Hijacking

In fig 01, the left most side picture is the place the bona fide client enters the certifications to sign into the cloud server. This is the place the gatecrasher hacks and recover or listen stealthily on the exercises and uses the delicate information. Security is the most crucial part of the distributed computing innovation. As this current model's methodology delicate information can be put away on both customer and in addition cloud server sides. This is the reason character administration and validation are vital in distributed computing.

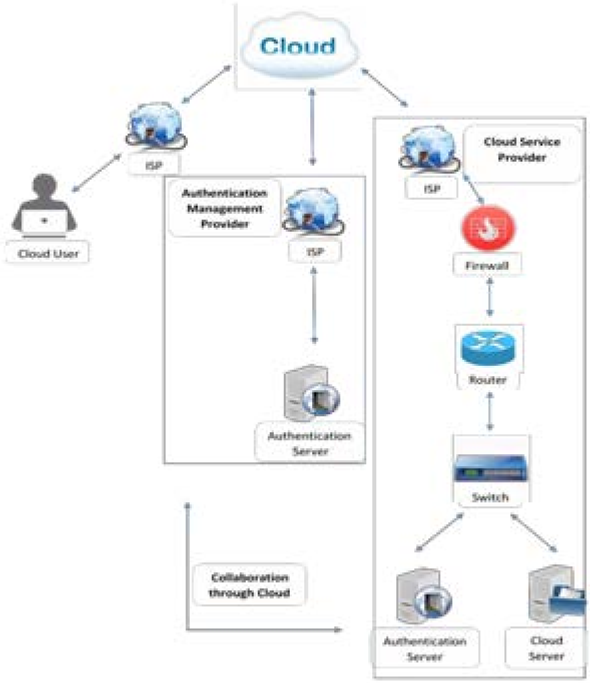

Fig. 02. –Cloud Authentication Process

Fig 02, clarifies the way toward verifying the client by the cloud administration supplier and in addition the coordinated effort between an outsider verification administration supplier to fortify the security in the cloud base. Zones of business to individual life can be demolished by the programmers controlling or recovering touchy data put away on cloud. There are genuine occurrences where photos of individual's life occasions were distributed to the web subsequent to hacking into their own cloud account by ruffians.

Assailant utilizes the stolen account information to lead unapproved exercises. One example is the place an assailant uses a stolen accreditations to go about as the certified record proprietor. Organization honesty and notorieties can be obliterated. Private information can be spilled or controlled along these lines producing huge expense to ventures or their customers. B. Counteractive action of Service Traffic Hijacking There are couple of contrasting options to be utilized to avoid administration movement commandeering. Watching client conduct can distinguish suspicious exercises. Cloud client's typical conduct stays as the same with the time. Proactively observing client conduct identify strange occasions, for example, downloading gigantic measure of information in a brief timeframe. Some cloud administration suppliers utilize this method. Hindering the record for a timeframe when suspicious movement happens helps the honest to goodness client to spare his delicate information. Executing a two component confirmation facilitate the security rupture which the cloud innovation as of now experience. Robber needs two verifications to enter into the client data. One confirmation won't fulfill the necessities to enter along these lines thusly programmer would not have the capacity to infiltrate the framework and control touchy information. Denying the sharing of the qualifications amongst client and the administration shuts the way to robbers on taking the record certifications. This is the place thief can without much of a stretch get to and recover the qualifications. Understanding cloud supplier administration polices and administration level assertions can decrease the dangers. At the agreement level before consenting to the arrangement the purchaser ought to look for fulfilling necessities to guarantee the delicate information is at a protected spot. To do as such a few suggestions ought to be taken after. Check the security standard of the administration supplier and your capacity to review their consistence. The buyer ought to have the privilege to evacuate information which is been put away and the privilege to get them back at whatever point sought. The privilege to stop the administration and evacuate all the data for all time ought to be done on account of the client and at whatever point there is a security rupture client ought to know how the data is ensured and in addition the solutions for disappointment

IV. ENCRYPTION IN CLOUD COMPUTING

Encryption Process Nowadays, distributed computing acts an imperative part in current IT innovation. As it moves forwards, there are such a large number of security difficulties and dangers in distributed computing. As an answer for this cloud information encryption instrument is presented. In cloud encryption client's information in cloud administration changed over into figure content. Numerous associations on the planet, which as of now Fundamental insurance likewise consider about executing encryption arrangements. There are sure strides of procedure of information encryption .The information go through a numerical equation called calculation which changes over it into scrambled information called figure content. Embody the message with key make a key by these calculations .There are two sorts of encryption and they are hilter kilter and symmetric. Firstly we discuss hilter kilter encryption. There are two numerically related keys which are utilized. Out in the open key (awry) encryption: one to encode the message and the other to unscramble it. These two keys consolidate to shape a key pair both information encryption and gatherings of the imparting personalities approval and is measured more ensured than symmetric encryption which is conveyed by hilter kilter encryption yet is computationally slower. Significant parts of an open key are Plaintext: instant message connected by to a calculation, Encryption calculation: performs experimental procedures to way substitutions and changes to the plaintext; Private and Public key: pair of keys where one is utilized for decoding and the other for encryption; Cipher content: by utilizing the calculation to the plaintext message utilizing key mixed or encoded message delivered, Decryption Algorithm: this calculation creates the walking key and the figure content to create the plaintext.

These are the means of unbalanced information encryption process: utilizing numerical created code equation encryption starts by changing over the content to a pre-hash code; Using the senders private key this pre-hash code is encoded by the product; Using the calculation utilized by the product private key would be created; The scrambled message and the pre-hash code are scrambled again utilizing the senders private key; Then to recover people in general key of the individual this data is expected for sender of the message.

The sender encodes the mystery key with the beneficiary's open key, hence just the collector can unscramble it utilizing the private key, in this way finishing up the encryption procedure. Private Key encryption additionally said to as universal or single-key encryption is lay on mystery key that is shared by both conveying gatherings to share a typical key it enquires all gatherings that are imparting the appropriation party utilizes the mystery key as offer of the investigative procedure to encode (or encipher) plain content to figure content. The same mystery key uses the getting party to unscramble (or decode) the figure content to plain content.

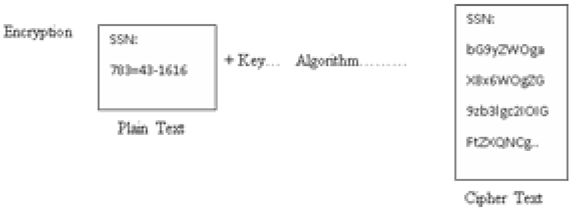

Fig. 03. –Encryption Process

Fig 03, portrays the procedure of the encryption where the sub forms makes the figure content and how the key is being utilized. It is required that the sender and collector have an approach to trade mystery keys in a protected way when utilizing this type of encryption. Interchanges will be shaky in the event that somebody knows the mystery key and can make sense of the calculation. There is additionally the requirement for a solid encryption calculation. They would be not able decide the encryption calculation, method for this is if somebody somehow happened to have a figure content. Cryptanalysis is a technique for assault that assaults the components of the calculation to diminish whichever a particular plaintext or the key utilized. Savage power is generally as it passes on; utilizing a technique to locate each comprehensible blends lastly choose the plaintext message one would then have the capacity to image out the plaintext for entire past and up and coming correspondences that keep on using this traded off setup. There are such a variety of points of interest in encryption. As one of a noteworthy favorable position can take that encryption ensure the cloud information totally. In the wake of encoding the information it is extremely hard to decipher the data. Furthermore gives the security to the scrambled information amid transmission. This additionally can take as one of a noteworthy preferred standpoint in information encryption. Encryption backings to achieve secure multi-tenure in the cloud. Encryption key administrations maintain a strategic distance from administration suppliers from getting to and controlling client information.

At the point when the administration suppliers have both customer's encoded data and scrambled keys, they will ready to access to information. To stay away from this issue, gives client's own encoded keys. Encryption permits clients to secure their remote workplaces. In spite of the fact that there is having such a large number of favorable circumstances in cloud information encryption there are a few detriments as well. The fundamental essential reason for encoding information is that somebody can decode it when it required. The scrambled keys are the most fundamental thing in encryption. On the off chance that client lose these keys, it will take uncountable time to get to their information. In spite of the fact that with utilizing information encryption can supply more security to cloud information, some of programmers and hoodlums will ready to get to the cloud information. Accordingly as an answer for this issue can utilize a solid username and a solid secret word for decoding process. Furthermore can scramble the information more than one time. This will make more troublesome for programmers to access to the encoded cloud information. Rupture of the information likewise a noteworthy issue in distributed computing. With regards to information encryption rupture of information additionally can be happen. The greater part of associations must be all the more particularly worry about this. As an answer for this can utilize propelled equality checking system to check information while in encryption, transmission and unscrambling. B. Proposed Encryption Method to Increase Security Current encryption strategies could diminish the security risk yet have not totally expelled the issue. To build the viability of the encryption another methodology can be utilized. Fig 04, passes on the way toward utilizing a symmetric encryption key as a part of distributed computing foundation. Customer will have two keys which the key one will be utilized to encode the symmetric key and the second key will be utilized to decode the symmetric key. Scrambling the encoded message and decoding the content will be finished by the above made symmetric key.

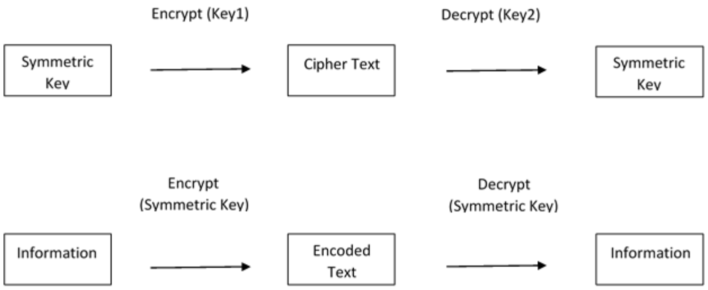

Fig.04. –Proposed Encryption Method

V. CONCLUSION

This paper portrays the procedure of encryption too the procedure of administration movement capturing. In view of the discoveries and talked about distributed computing is turning into a developing innovation which contribute people to the administration level in different area with enormous measure of focal points rupture of security in cloud framework makes the client reevaluate of utilizing the cloud innovation. One burden of the foundation is administration activity commandeering where the accreditations of the client is stolen and touchy information is controlled and utilized by a robber. Executing a two variable confirmation and watching client conduct to distinguish malignant exercises can facilitate the security dangers. Restricting the sharing of client accreditations and comprehension administration lawful understanding can help business at whatever point there is a security rupture. Utilizing encryption techniques to scramble the client information makes it harder to unscramble for private key is with the authentic client and it is not distributed. Different encryption strategies can be utilized to expand the security in cloud base in light of the present necessities and even outsider confirmation server can be utilized. By utilizing two keys to encode and decode the symmetric key expanded security status can be accomplished. Symmetric key can be utilized to scramble and decode the data hence the programmer needs more than one key to recover data.

VI. FUTURE WORK

The principle disadvantage of the encryption procedure is the unpredictability of the calculation and in addition the procedure of usage. Data ought to be decode and encode in matter of seconds accordingly expanding the quantity of key should be streamlined well to build the proficiency. Anticipation of seizing ought to likewise be a duty of the cloud client also. There should be more strides done by the cloud client to counteract programmers acquiring the certifications which we didn't talked about in this paper.

AKNOWLEDGEMENT

Authors are very much thankful to Sri Lanka Institute of Information Technology for doing research work in Computer Networking as well as all the authors whom team have referred in this research paper. Authors are also thankful to Mr. Dhishan Dhammearatchi for his constant support and encouragement for conducting research work in Computer Networks Design and Implementation.

REFERENCES

[1] Omotunde, O. Awodele, S. Kuyoro and C. Ajaegbu, "Survey of Cloud Computing Issues at Implementation Level", Journal of Emerging Trends in Computing and Information Sciences, vol. 4, no.1, 2013 [Online]. Available: https://www.researchgate.net/publication/259481468_Survey_of_Cloud_Computing_Issues_at_Implementation_Level. [Accessed: 06-Jun-2016]

[2] M. Kazim and S. Zhu, "A survey on top security threats in cloud computing", (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 6, no. 3, pp. 109-113, 2015 [Online]. Available: http://thesai.org/Downloads/Volume6No3/Paper_16-A_survey_on_top_security_threats_in_cloud_computing.pdf. [Accessed: 08- Aug- 2016]

[3] M. Ahmed and M. Hossain, "CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD",International Journal of Network Security & Its Applications (IJNSA), vol. 6, no. 1, 2014 [Online]. Available: http://airccse.org/journal/nsa/6114nsa03.pdf. [Accessed: 07-Aug- 2016]

[4] 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 [Online]. Available: http://www.ijcsits.org/papers/Vol1no22011/13vol1no2.pdf. [Accessed: 05-Jul- 2016]

[5] P. Jain, "Security Issues and their Solution in Cloud Computing", International Journal of Computing & Business Research, 2012 [Online]. Available: http://www.researchmanuscripts.com/isociety2012/1.pdf. [Accessed: 06- Jun- 2016]

[6] J. Kaur and D. Garg, "SURVEY PAPER ON SECURITY IN CLOUD COMPUTING", International Journal In Applied Studies And Production Management, vol. 1, no. 3, pp. 28-32, 2015 [Online]. Available: http://www.ijaspm.org/feb-may%202015/volume%201%20issue%203%20august,%202015/SURVEY%20PAPER%20ON%20SECURITY%20IN%20CLOUD%20COMPUTING.pdf. [Accessed: 05- Jun- 2016]

[7] S. Kumar and R. Goudar, "Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey", International Journal of Future Computer and Communication, vol. 1, no. 4, pp. 356-360, 2012 [Online]. Available: http://www.ijfcc.org/papers/95-F0048.pdf. [Accessed: 04- Jul- 2016]

[8] M. Ahmed and M. Hossain, "CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD",International Journal of Network Security & Its Applications (IJNSA), vol. 6, no. 1, pp. 25-36, 2014 [Online]. Available:http://airccse.org/journal/nsa/6114nsa03.pdf. [Accessed: 07-Jul-2016]

[9] V. Ashktorab and S. Taghizadeh, "Security Threats and Countermeasures in Cloud Computing",International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 1, no. 2, pp. 234-245, 2012 [Online]. Available: http://ijaiem.org/volume1Issue2/IJAIEM-2012-11-3-076.pdf. [Accessed: 07- Jul- 2016]

[10] Asma, M. Chaurasia and H. Mokhtar, "Cloud Computing Security Issues", International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 1, no. 2, pp. 141-147,2012 [Online]. Available:http://www.ijaiem.org/volume1Issue2/IJAIEM-2012-10-22-038.pdf. [Accessed: 07- Aug- 2016]

[11] Atayero, O. Feyisetan, Journal of Emerging Trends in Computing and Information Sciences, vol. 2, no. 3, pp. 546-552, 2011 [Online]. Available: http://eprints.covenantuniversity.edu.ng/912/1/vol2no10_11.pdf. [Accessed: 15- Sep- 2016]

[12] D. Mukhopadhyay, G. Sonawane, S. Gupta, S. Bhavsar and V. Mittal, International Journal of Innovative Research in Computer and Communication Engineering, no. 2, pp. 3-6, 2015 [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1303/1303.7075.pdf. [Accessed: 02- Sep-2016]

[13] S. Sharma and A. Chugh, International Journal of Innovative Research in Computer and Communication Engineering, vol. 1, no.2, pp. 1-10, 2013 [Online]. Available: http://www.ijircce.com/upload/2013/april/11_V1204092_O.pdf. [Accessed: 13- Sep- 2016]

[14] S. Kumar and R. Goudar, International Journal of Future Computer and Communication, vol. 1, no. 4, 2012 [Online]. Available: http://www.ijfcc.org/papers/95-F0048.pdf. [Accessed:05- Aug- 2016]

AUTHORS

First Author – Ailapperuma D C R, Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka

Second Author – Kaushalya A H L D C, Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka

Third Author – Bandara H.M.P.M, Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka

First Author – Ranghadari M.I.T, Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka

Second Author – A.B.M.U.I.Bandara, Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka

Third Author – Mr. Dhammearatchi D, Faculty of Information Technology, Sri Lanka Institute of Information Technology, Colombo, Sri Lanka