RESEARCH ARTICLE OPEN ACCESS

Analysis of the Technique for the Improvement of the Data Confidentiality in the Cloud Computing Environment

Dr.K.Sai Manoj
CEO, Innogeecks Technologies and Amrita Sai Institute of Science and Technology/Reviewer
Vijayawada, AP
India

ABSTRACT

Many Developers have been reviewed with some proposed solutions but these solutions have fallen short of addressing account misused and malicious insider threats. In addition, the online survey conducted highlighted that insider breaches are among the main form of vulnerability to cloud data. These challenges within the cloud storage informed the basis for the design of a scheme for improving data confidentiality in the cloud computing environment. The data confidentiality is achieved by implementing authentication login which triggers a six digit code to be sent to a client mobile or e-mail for further authentication, thus, enabling situational awareness of data breaches in real-time. This approach will enhance reliability and trust of cloud services enabling users to maximize on potential benefits offered by the cloud environment.

Keywords:- Cloud Computing

I. PROBLEM STATEMENT

In the Case of hacking into individual e-mail accounts and organization servers have being rising with the growth of online lifestyle. According to [1] it is observe that cloud computing is rife with history of leaks, both accidental and deliberate that has led to the recognition of the privacy risks of cloud deployment. Therefore, whether it is insiders or outsiders breaching data confidentiality in the cloud, such attacks occurs using stolen account credentials of a client. Thus, this challenge of stolen account credentials and lack of situational awareness on the client or system administrator side, when client account is accessed, informs this research. This dissertation therefore, is aimed at designing a scheme whereby when an account is hacked, the first successful authentication triggers a six digit code to be sent to client mobile or email account for the second round authentication before accessing cloud data. Since the hacker does not have client mobile or e-mail credentials, access will be denied, thus, enhancing confidentiality. The proposed system will ensure better situational awareness as well as hardening it, hence, making it costly to obtain client data. In addition, it would detect insider breaches in real-time, therefore, becoming a better deterrence against the growing vector threats.

This research paper therefore, is aimed at conceptual oriented analysis on a scheme whereby when an account is hacked, the first successful authentication triggers a six digit code to be sent to client mobile or email account for the second round authentication before accessing cloud data. Since the hacker does not have client mobile or e-mail credentials, access will be denied, thus, enhancing confidentiality. The proposed system will ensure better situational awareness as well as hardening it, hence, making it costly to obtain client data. In addition, it would detect insider breaches in real-time, therefore, becoming a better deterrence against the growing vector threats.

Security threats:

According to [2] cloud security refers to the protection of running applications, stored data and processing of transactions within the cloud, adding that the growth of attacks are in exponential factors. Thus, this calls for continuous awareness on how and when to secure systems against threats. As per [3] defines continuous monitoring as an ongoing awareness of information security, vulnerabilities and threats to enable risk based decision making. Similarly, [2] observes that there have been more malware attacks in the last 18 to 24 months than in the last 18 years. While cloud services promises so many things, for instance agility, scalability and efficiency, its security elements in the Cloud is not being fully met. From the authors above, there is a growing need to secure the ever increasing numbers of endpoint devices used by users because of an ever rising online lifestyle. Thus, these security risks and concerns need to be addressed if users are to benefit from the cloud promise of low-cost computing.

II. CLOUD SECURITY ALGORITHMS

According to [4] Cloud Computing is a technology where the clients can use high end services in form of applications that reside on different servers in addition to data that can be accessed globally. Accessing of services over open architectures of the internet has it's drawbacks, if proper security is not implemented to enable secure access. Therefore, the need for cryptography comes in handy. As [4] observes that encryption/decryption is the science of securely transmitting and retrieving data using an insecure channel. The authors went on to propose non breakability of Elliptic curve cryptography for data encryption and Diffie Hellman key exchange mechanism [5] for connection establishment. The authors' proposed an architecture that uses a combination of digital signature algorithm of Diffie Hellman and Advanced Encryption Standard (AES) encryption that would guarantee confidentiality. Despite the authors proposing Diffie Hellman and AES encryption, it's implementation and comparison with different algorithms were not carried out hence their proposal fell short. This section, therefore, will look at various algorithms and how their implementations in the cloud will enhance security and also their drawbacks.

III. CLOUD DATA SECURITY MODELS

As per [6] (2016) defines data security to mean self-assurance and reliability preservation of data processed by a company. The author discussed with industrial experts that by 12 accessing cloud services and information through the internet, the importance of safety measures increase because data is at greater security risk. From the above statements, the authors allege that organization data is at risk because of it being accessed through the internet. As per [3] observes that cloud computing is offered in three services and four deployment models. The three main service models include: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), although others have come up with Security as a Service, Storage as a Service, Business Process as a Service (BPaaS) among others. On the other hand, the four deployment models have so far been identified: private, public, community and hybrid.

IV. CONCLUSIONS

This research paper was aimed at developing a scheme for improving data confidentiality in the cloud computing environment by addressing a threat to client account attributed to stolen user credentials. The unauthorized access to client cloud account using stolen user credentials either by malicious insiders or outsiders as discussed in this dissertation has been a major challenge to organization. In trying to address this threat of using stolen user credentials, several cloud security models, architectures and algorithms were reviewed to establish the best way of securing data confidentiality in cloud storage.

REFERENCES

[1] Feldman, A. J. (2012). Privacy and integrity in the untrusted cloud. Mountain view, California, USA.

[2] Britt, P. (n.d). Cloud Security vs. Security in the Cloud: What's the difference? Similar Sounding Cloud Security has a very different Meaning. Accessed on 16.09.2015.

[3] Grance, T. & Mell, P. (2011). National Institute of Standards and Technology: The NIST Definition of Cloud Computing. NIST Special Publication 800-145.

[4] Tirthani, N. & Ganesan, R. (n.d). Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography

[5] INVESTIGATIONS ON THE CLOUD DATA STORAGE SECURITY BASED USING DIFFIE HELLMAN ALGORITHM Dr.K.Sai Manoj appreciated article in International Journal of Computer Engineering and Applications, Volume XIII, Issue VI,

JUNE. 19, www.ijcea.com ISSN 2321-3469

[6] Zoltan, B. & Milan, T. (2016). Modeling of Data Security in Cloud Computing

[7] Satish, Karuturi S R V, and M Swamy Das. "Quantum Leap in Cluster Efficiency by Analyzing Cost-Benefits in Cloud Computing." In Computer Science and Engineering by Auroras Scientific Technological & Research Academy Hyderabad, vol. 17, no. 2, pp. 58-71. Accessed 2018.

DECLARATIONS

Availability of data and material:

Not applicable.

Competing interests

Not applicable.

Funding:

No funding was applicable.

Authors' contributions:

The other of the paper do all the work, the environment for research work is done by my best of my knowledge and supporting my family members.

Acknowledgements:

First of all, I am thankful to Honourable Amrita Sai Management for giving me this opportunity and to complete my work. It gives me an immense pleasure and pride to express my deep sense of gratitude to the Innogeecks technologies for their technical support in all the aspects.

AUTHORS' INFORMATION

Dr K Sai Manoj, Founder and Executive Director of Innogeecks Global Services Pvt Ltd, Founder and CEO of Innogeecks Technologies and Founder of 3 start-ups based on IOT and Cloud Computing, is an Enthusiastic learner, Excellent Financial Advisor, Innovative and Visionary Leader, Insightful team builder and strategic planner, who has 10+ years of experience in Financial Services, Equity Research and IT- ITeS services to his credit. He has worked in Reputed Companies like WIPRO Technologies, Fidelity Inverstments.etc.,

He is Proud of achieving many laurels in the field of Computers and Research. He is a Certified Ethical hacker, Certified Computer hacking forensics Investigator, Certified Security Analyst, Charted Engineer from IEI (India), Certified Blockchain Expert, Microsoft Certified Technology Specialist, AWS Certified Solutions Architect-Associate, Google Analytics Individual Qualification, IBM Block chain Certification, Certified EC Council Instructor and so on.

He has a proven record of having 10+ certifications from the most sought after software giants such as Microsoft, IBM, Google, Face book, EC Council & Amazon besides this he has acted as a reviewer for the Journal of Super Computing (Springer) , Journal of Big Data (Springer) and Journal of the Institution of Engineers (India) – Series B (Springer). And also with his solid financial advice 21 start-ups of Kochi, Bangalore and Vijayawada have tread the success track.

Talking about his research excellence, it is exciting to know that he has filed 3 patents and 4 more are in pipeline and has Published more than 25 research papers in reputed journals like Thomas Reuters, IEEE, Scopus etc., and shows keenness in researching on Cyber Security, Cloud Computing, Big Data / Hadoop, Block chain and Data Analytics.