Client/Server Model of Data Privacy using Extended Playfair Cipher for SaaS Applications on the Cloud

David Livingston J, Kirubakaran E

Abstract: *Cloud Computing is a paradigm of distributed computing that delivers on-demand and utility-based services to its customers. It provides a set of shared computing resources such as networking, servers, storage, and applications in the form of services to an organization or an individual. The major benefits of cloud computing include on-demand self-service and cost-effectiveness. For the customer, there is no up-front cost for setting up and running the applications on the cloud. Despite the benefits provided by various cloud services, the outsourcing of data storage and computation raise many new security issues. One of such security issues that have to be addressed before uploading our sensitive data to the cloud is data privacy. With the cloud model, end-users lose control over the physical location of data, because data will be stored and processed elsewhere on the globe and not in the local computer. Hence, we need an algorithm for encrypting the data that can be stored and retrieved from a database managed by the public cloud.*

Keywords: *Distributed Computing, Cloud Computing, Data Privacy, Encryption, Public Cloud*

I. INTRODUCTION

Cloud Computing is a technology that provides IT infrastructure and services for computing, storage, networking, and application development and deployment. End-users can make use of the services provided by Cloud Providers for doing any kind of activities that can be done with the help of a desktop or laptop. Cloud computing makes use of the approaches, concepts and best practices that have already been established over the last few decades. It provides a set of shared computing resources such as networking, servers, storage, and applications in the form of services to an organization or an individual. It allows its user to get resources such as storage and computation elastically as much as they require. With the help of cloud computing, users can store and access their data as well as applications over the Internet instead of keeping them on the local computer's hard drive.

Different Cloud Providers provide cloud services at different abstraction levels namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Using SaaS, a cloud user can do day to day activities such as document creation, sending and receiving mails, and chatting over the Internet. As per the reports published by public cloud tracker, the top seven cloud vendors or Cloud Service Providers (CSPs) in India are Multi-National Companies (MNC) like Amazon, Microsoft, and Google [1].

India based vendors have a minimal share in the country's cloud market, mostly because it becomes difficult for these companies to compete with the operational scale of MNCs. Amazon is well known for IaaS (through EC2 - Elastic Compute Cloud) and PaaS, whereas Microsoft is delivering its services as a Platform (PaaS) for its developers. Google has a host of Software as a Service (SaaS) for its users which include a word processor, spreadsheet, presentation software, and drawing applications. It also has utilities like contacts, calendar for its customers to manage their contacts and events respectively. Its search engine, which is available at google.com is used by millions of people every day. Many of them are using non-search based apps such as Gmail and Google Drives for mailing and storage purposes respectively [2].

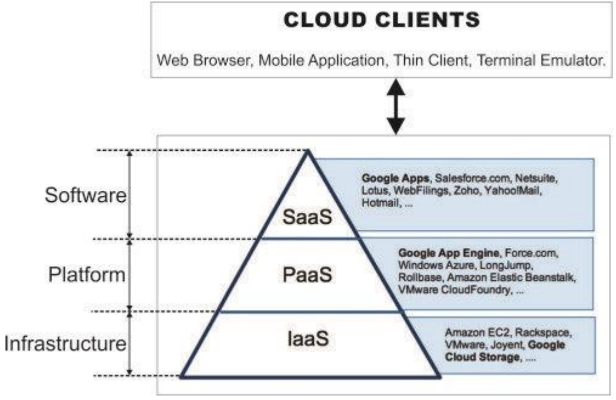
CLOUD CLIENTS
Web Browser, Mobile Application, Thin Client, Terminal Emulator.
Software
Platform
Infrastructure
SaaS
PaaS
IaaS
Google Apps, Salesforce.com, Netsuite, Lotus, WebFilings, Zoho, Yahoo!Mail, Hotmail, ...
Google App Engine, Force.com, Windows Azure, LongJump, Rollbase, Amazon Elastic Beanstalk, VMware CloudFoundry, ...
Amazon EC2, Rackspace, VMware, Joyent, Google Cloud Storage, ...

Figure-1: Major Cloud Providers and their offerings

To deploy their applications, Cloud Providers must install Operating System (OS) images and applications software on IaaS. This is done with the help of PaaS that provides a platform on top of IaaS. Windows Azure is a PaaS offering from Microsoft for its developers who are familiar with Microsoft platform and development environments such as .NET and Visual Studio. It has a highly scalable, robust, and cost-effective environment for the deployment of applications and services that can be accessed by multiple users at a time [3].

The objective of this research includes the following:

Manuscript published on 30 August 2019.
***Correspondence Author(s)**

David Livingston J, Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, South India – 641 114.

Dr. Kirubakaran E, Professor, Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, South India – 641 114.

1. To find out the issues involved in securing the privacy of sensitive data of an organization on the cloud.
2. To identify the tools and techniques used for encrypting and decrypting the data that can be stored on the cloud.
3. To devise a new algorithm for encrypting the data that can be stored and retrieved efficiently from a database on the cloud.

II. A MAJOR SECURITY ISSUE IN ADOPTING THE CLOUD

A. Data Privacy

Professional services, security services, investment services as well as the insurance sector are among those adopting cloud computing in India. Using SaaS offerings in the cloud such as salesforce.com reduces the need for customized software development. SaaS will likely remain the dominant cloud service model for the foreseeable feature and the area where the most critical need for security practices and oversight will reside. One of the security issues that have to be handled while adopting the cloud is data privacy. Storing huge amount of critical information in centralized locations arises many concerns about data protection.

B. Findings from Existing Literature

Rania Fahim El-Gazzar (2016) has identified in her conference paper the risks involved in adopting Cloud Computing by Small and Medium Enterprises namely organizational risks, technical and non-technical risks, legal risks and performance risks. Among the various risks involved, the technical risks include data leakage, loss of data, downtime, data bottlenecks and cyber-attacks [4].

Frederico Durao et al (2014) have identified in their journal article the risks involved in data storage and protection on the cloud [5].

Gururaj Ramachandra et al (2017) have identified data breach as one of the threats that must be addressed before adopting the cloud for an enterprise [6].

Alessandro Agostino et al (2013) have identified that offering ubiquitous access to data in order to provide a responsive answer to customer requests is one of the major critical success factors of cloud computing adaptation. They concluded that SMEs can benefit from a more comprehensive understanding of one or more of the Critical Success Factors (CSF) for adopting the cloud-based solutions in an enterprise [8].

Nabil Giweli (2013) in his thesis submitted for the degree of Master of Science at University of Western Sydney discussed the benefits of using Data-Centric Security (DCS), an approach that aims to provide data owner full control over their data within the data itself on the cloud [9].

C. Cryptographic Approach of Data Privacy

In order to secure the data on the cloud, users ought to encrypt the data before moving it to the cloud. If the data to be migrated is encrypted using a trusted algorithm, then regardless of the service providers security and encryption policies, the data can only be accessed with the decryption keys available with the end-user. Security needs to move to the data-level so that enterprises can be sure that their data is protected wherever it goes.

- **Amar Ghorbel et al** (2017) have discussed the issues involved in maintaining the privacy of sensitive data such as financial, health-related and personal data. They identified cryptography as the most appropriate solution for data privacy. They also addressed the limitation of encrypted data when some computations are performed on it. They proposed an approach called a hybrid approach for enforcing better data privacy [10].
- **Mazhar Ali et al** (2015) have identified data privacy and integrity as a major security issue in cloud data storage. The main cause of security issues in data privacy is the lack of user control on data stored in the cloud. The authors concluded that a mechanism is needed to ensure privacy during computation on encrypted data. They proposed a framework that ensures privacy while performing computation over the encrypted data [11].
- **P. Ravi Kumar et al** (2018) in their conference paper identified different methods and procedures that can be used to improve data security and privacy. They also agree that storing the encryption keys should not be done along with the encrypted data [13].

D. AWS Security Best Practices

The **AWS white paper** (Aug 2016) on AWS Security Best Practices published by Amazon Web Services (AWS) suggests various ways of securing the data, operating systems and applications on the AWS cloud [7].

The **AWS white paper** (Dec 2016) on AWS Storage Services published by Amazon Web Services (AWS) gives an overview of storage services offered by them. In that paper, a list of features available in various AWS Cloud Storage Services such as AWS S3 (Simple Storage Service) is given. The three ways in which data security is provided by the AWS cloud also discussed in this paper. They are Service-side encryption, Client-side encryption and using SSL. The data at rest can be encrypted using server-side encryption, in which AWS user requests Amazon S3 to encrypt the data before it's written to disks in data centers and decrypt it when it is downloaded. By using client-side encryption, the data is encrypted by AWS user on the client-side and then uploaded to Amazon S3. The third method is to protect the data in transit by using Secure Sockets Layer (SSL) or client-side encryption [12].

III. PROPOSED METHOD OF DATA PRIVACY

Generally, Cloud Providers tend to take care of security issues in cloud computing. For instance, Amazon provides a set of tools for managing the security of resources maintained on the cloud. Here is a list of Amazon Web Services (AWS) tools for managing security:

1. Identity and Access Management (IAM)
2. Cloud Tail
3. Cloud Watch
4. Trusted Advisor
5. Directory Services

Though security services are provided by the Cloud Service Providers (CSP) themselves, cloud computing best practices suggest that cloud consumers should employ some mechanism for protecting their resources in each layer of the cloud or avail the services provided by third-party security service provider. One such mechanism for data protection on the cloud is Encryption.

Different encryption mechanisms are available for securing the data on the cloud. After encryption of data, the encryption keys generated should be stored secretly behind firewalls so that private data can be kept securely on the cloud.

Gaurav Sharma et al (2012) in their journal article studied and observed various encryption algorithms and the use of keys in implementing the encryption of data. They observed that by increasing the length of the key, the algorithm will produce ciphertext which is more secured. But, longer keys may consume more power and dissipate more heat. They also identified that an efficient encryption algorithm should have a fast response and less complexity [14]. In this research, a novel method of encryption is introduced in order to have both properties of encryption – confusion, and diffusion. In this approach, a modified version of Play-fair Cipher will be used to encrypt the data before it is uploaded or outsourced on the cloud. This method of encryption is going to be implemented in two modules:

Module 1: Client-side encryption, which will be implemented at the client-side with the help of client-side scripts written and executed on a browser.

Module 2: Server-side storage and retrieval, is going to happen at the backend – a MySQL Database – that will hold the encrypted data in a server machine on the cloud.

At the back-end, the database will be designed and named in such a way that an intruder can't understand anything even if he breaks open the security at the file level. Columns that will hold the data of type Character String (either fixed-length or variable-length) are to be encrypted using this approach. By encrypting the textual data stored in a database, most of the sensitive information will be secured from unauthorized users or intruders. At the front-end (on a browser), data privacy is achieved with the help of encryption mechanism that will encrypt the data as soon as it is entered. The client will send the encrypted data to the back-end for storage or processing. It is the duty of the client-side script to encrypt the data using a mechanism implemented in a script that will run on the browser. During a search operation, the client will send the data to be searched for in an encrypted format so that data will not be maliciously accessed by an intruder. The server that runs on the cloud will receive the request and then do the search operation with the help of a query. Then the result will be sent back to the client in an encrypted format. It is again the duty of the client to get the plain text from the ciphertext received from the server.

IV. CONCLUSION

Cloud Computing is a kind of distributed computing that provides its customers on-demand, utility-based computing devices. It gives the ability to its customers to store and access data and programs over the Internet instead of having them on the local computer's hard drive. Cloud provides the capability for pooled resources to be made available and accessible to anyone or anything authorized to utilize them over the Internet. Cloud computing infrastructure is provided in India by three major Service Provides namely Google, Microsoft and Amazon in the form of Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

The widespread use of mobile devices in accessing the cloud gives more easy access to attackers in a cloud environment. This increases the vulnerabilities and threats to the cloud computing environment. Moreover, storing large amounts of data that is oriented around user privacy, identity and application-specific preferences in centralized locations raise many concerns about data protection. In this research, literature has been reviewed for identifying the issues involved in securing the privacy of sensitive data of an organization on the cloud. And then, a novel method of encryption has been proposed for encrypting the data that can be stored and accessed from a database on the cloud.

REFERENCES

1. Open Source For You, May 2018 issue.
2. David Crookes, Cloud Computing, Tata McGraw-Hill Edition, 2012
3. Dominic Betts, Scott Densmore, Ryan Dunn, Manashi Narumoto, Eugenio Pace, Matias Woloski, Developing Applications for the Cloud on the Microsoft Windows Azuer Platform, Microsoft Press, 1st Edition, 2011
4. Rania Fahim El-Gazzar, "A Literature Review on Cloud Computing Adoption Issues in Enterprises", 2016, HAL Id: hal-01381189, https://hal.inria.fr/hal-01381189
5. Frederico Durao, Jose Fernando S. Carvalho, Anderson Fonseka, Vinicius Cardoso Garcia, "A Systematic Review on Cloud Computing", Journal of Supercomputing, 2014, Published online: 31 January 2014, DOI: 10.1007/s11227-014-1089-x
6. Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, "A Comprehensive Survey on Security in Cloud Computing", Conference Paper, Procedia Computer Science 110 (2017) 465–472, DOI: 10.1016/j.procs.2017.06.124
7. AWS Security Best Practices, AWS Whitepaper, Published in August 2016.
8. Alessandro Agostino, Klaus Solberg Soilen, Bart Gerritsen, "Cloud Solution in Business Intelligence for SMEs – Vendor and Customer Perspectives", 2013, Journal of Intelligence Studies in Business, https://ojs.hh.se/index.php/JISIB/article/view/72/76
9. Nabil Giweli, "A Thesis on Enhancing Cloud Computing Security and Privacy", 2013, School of Computing, Engineering and Mathematics, University of Western Sydney
10. Amar Ghorbel, Mahmoud Ghorbel, Mohamed Jmaiel, "Privacy in Cloud Computing Environments: a Survey and Research Challenges", Journal of Supercomputing, 2017, Published online: 23 January 2017, DOI 10.1007/s11227-016-1953-y
11. Mazhar Ali, Samee U. Khan, Athanasios V. Vasilakos, "Security in Cloud Computing: Opportunity and Challenges", Journal of Information Sciences, 2015, Pp. 357-383, http://dx.doi.org./10.1016/j.ins.2015.01.025
12. Overview of AWS Storage Service, AWS Whitepaper, Published in December 2016.
13. P. Ravi Kumar, P. Herbert Rajb, P. Jelcianac, "Exploring Data Security Issues and Solutions in Cloud Computing", Procedia Computer Science 125 (2018) 691–697, DOI: 10.1016/j.procs.2017.12.089
14. Gaurav Sharma, Ajay Kakkar, "Cryptography Algorithms and approaches used for data security", 2012, International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012, ISSN 2229-5518

AUTHORS PROFILE

David Livingston J, a software professional turned academician, has been into teaching COMPUTER SCIENCE since 2003. He worked as an Assistant Professor in various Engineering Colleges affiliated to Anna University for 10 years. He also worked as HOD in the Department of Computer Engineering in SRI Polytechnic College, Coimbatore. He has expertise in the field of Client/Server programming, Web programming, and Cloud computing. Currently, he is pursuing his research in the field of Cloud Computing and Information Security at Karunya Institute of Technology and Science, Coimbatore.

Dr. E. Kirubakaran obtained B.E (Hons.) degree in Mechanical Engineering, M.E. in Computer Science and Ph.D. in Computer from Regional Engineering College, Tiruchirappalli. He also obtained his M.B.A. degree from IGNOU. He has more than 30 years of Industrial experience at Bharat Heavy Electricals Ltd. (BHEL) Tiruchirappalli. He worked as an Additional General Manager at BHEL. Moreover, he held various positions such as Secretary, Vice-Chairman, and Chairman in the Computer Society of India, Tiruchirappalli. He is a Member of the Syndicate of Bharathidasan University, Member in the Academic Council Anna University, Trichy and Academic Council Anna University, Chennai. Currently, He is working as a Professor at Karunya Institute of Technology, Coimbatore.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)