Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021: 4001 - 4008

Research Article

IMPLEMENTING SECURED INFORMATION SYSTEM FOR EDUCATIONAL INSTITUTIONS USING SERVER-SIDE ENCRYPTION OF FILES AND DATA ON THE CLOUD

David Livingston J[1,] Kirubakaran E[2] and Richard S[3]

A Research Paper

Abstract—

Though cloud computing promotes less expensive and collaborative work environment among a group of employees, it involves risks in keeping the resources such as computing and data secured. Every organization classifies its data based on the sensitivity of data defined in its policy. Some classification schemes label data as Confidential, Internal Use Only, or Public Domain, where as others use labels such as Level 1, Level 2, and Level 3. Using cloud computing, especially in the public cloud model, the critical information of an organization is stored and maintained at various geographical locations in the cloud platform. The organization does not have any control over the data in the cloud. Though Cloud Service Providers (CSP) such as Amazon and Google provide their own mechanism for securing files and databases stored and maintained on the cloud, it is the sole responsibility of the users (Cloud Users) to secure their sensitive data uploaded and stored on the cloud storage. This privacy preserving of sensitive data can be achieved using cryptography that conceals information from others. Encryption allows data to be stored safely anywhere on the cloud. Depending on the sensitivity of the data, the owner of the data needs to encrypt the data in transmission and/or at rest as in a database. In this research, the authors have proposed a model of Server-side Encryption of files/data after migrating them on to the server.

Keywords- Cloud Computing; Cloud Service Providers; Cryptographic Algorithm; Privacy Protection

I. INTRODUCTION

Cloud computing may be viewed as a resource available as a service for an individual or an organization over the Internet. With cloud computing, customers need not own the infrastructure used in cloud computing infrastructure. Instead, they consume resources as a service by just paying for what they use. This leads to the benefit of forgoing capital expenditure involved in setting up the whole infrastructure for computing. Moreover, cloud computing promotes sharing of computing

power among multiple users. This results in improving the utilization rate of computing resources such as servers, which are not sitting dormant for lack of use in the cloud.

It has been reported that 61% of enterprises are currently using public clouds, 38% are using private clouds and 29% are using hybrid clouds. Large enterprises have slack resources, both financial and technical to afford deploying private clouds, whereas, Micro, Small and Medium Enterprises (MSMEs) tend to avail public clouds which are appropriate for them due to their limited financial and IT capabilities. In cloud computing, especially in the public cloud model, the critical information of an organization is stored on the storage at various geographical locations in the cloud platform. The organization does not have any control over the data in the cloud. To protect such data, traditional security mechanisms are used.

One of the most important tools for protecting data is cryptography. Cryptographic algorithms are made available to the public, cryptanalysts and computer engineers so that they get a chance to examine them for weaknesses. Despite the threat from cryptanalysts, cryptography has emerged as the safest way to transfer data across networks. There are three factors that determine the strength of encryption process of an encryption algorithm. They are: (i) strength of the algorithm, (ii) secrecy of the key and (iii) length of the key. In the previous paper written by the same author, the authors have come up with a client/server model for preserving the privacy of data on the cloud [1].

Encryption of plain text in a file/database can be done either at the client or on the server. The sensitive data must be encrypted at the client side using one of the symmetric cryptographic algorithms like AES (Advanced Encryption Standard) before moving them on to the cloud. For encrypting non-critical textual data, the authors have proposed a modified version of play-fair algorithm. Searchable encryption is also possible with the help of modified play-fair algorithm using the client/server model of data privacy [2]. In this paper, the authors have tried implementing the server-side encryption of cryptography on data after its migration to the remote server.

II. COMPARISION OF MAJOR CLOUD SERVICE PROVIDERS

Some of the Multi National Companies (MNCs) that provide cloud services in India are Amazon, Google and Microsoft. Among the three, Google is the one which provides its services in three different forms namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Though IaaS is provided by both Google and Amazon, Amazon took its lead by providing its services since 2006 in the cloud market. Amazon Web Services (AWS) is the cloud platform provided by **Amazon**. Today, AWS provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that empowers hundreds of businesses in 190 countries around the world. AWS provides Infrastructure-as-a-Service (IaaS) offerings in the cloud for organizations requiring computing power, storage, and other services. AWS offers a number of infrastructure-related services, which include: Elastic Compute Cloud (EC2), Simple Storage Service (S3), Simple Queue Service (SQS), CloudFront, and Simple DB. Moreover, Amazon provides a set of development tools for developers that include CodeStart, CodeCommit, CodeBuild, CodeDeploy, CodePipeline and Cloud9. Amazon's Cloud9 supports almost all programming languages such as C, C++, Java, PHP, Python, Node.js, Go and Ruby.

Figure-1: Some of the Popular Cloud Service Providers

Microsoft Azure is a PaaS offering from Microsoft for building, testing, deploying, and managing applications online through a global network of Microsoft-managed data centers [3]. Azure supports a range of application programming languages, including JavaScript, Python, .NET and Node.js [4]. Platform as a Service (PaaS) is provided by Google in the form of Google App Engine, which serves applications on Google's infrastructure. Google App Engine standard environment supports Java, Python, PHP, Go and Node.js [5].

With Google Docs, users can create and edit text documents right in the web browser without the need for word processor or spreadsheet software installed on the local computer. It allows multiple people work at the same time on the same document, and each person can see the changes made by others as soon as they save their work [6]. Google Calendar lets the user organize his/her schedule and share events with co-workers and students. With this Google App, it is easy to keep track of the daily schedule of its user. Google Contacts, the address book manager of Gmail lets the user keep track of all the contacts, which include the contact details of colleagues and students.

Google Blogger is a free publishing platform provided by Google. It is designed to be a tool for writers to upload their contents on their blogs using an easy to use editor online [7]. With the help of Blogger, authors can publish their articles on their personal web site called blog that can be accessed by many through browsing the net worldwide. With Google Classroom, educators can create classes, distribute assignments, send feedback, and manage the student activities in one place. Educators can set up classroom in minutes and can communicate with students and their guardians in one convenient place [8]. Though the cloud services such as SaaS, PaaS and IaaS are provided by one or more of the cloud providers, Google is good at providing SaaS offerings to an organization that makes use of collaborative work environment.

III. CLOUD SERVICES FOR EDUCATION

Today's students access the Internet constantly for exploring the world of information. By accessing web portals such as Twitter, Facebook, and Gmail, students are already using Cloud Computing technology in their day to day life. Cloud Computing is an excellent technology for Educational Institutions which operate under budget shortage for setting up their own Information Technology infrastructure that require capital investment on resources such as computers, storage and networking devices.

Now-a-days, major Cloud Provider like Google provides free services to students as well as staff community for managing their email, contact list, calendar, documents, and their own websites. Educational Institutions can take advantage of the cloud-based solutions offered by various Cloud

Service Providers in order to equip their own student/staff members to do their teaching/learning process more effectively. In this paper, an analysis is made between the major Cloud Service Providers namely Amazon, Google and Microsoft from the point of view of their services provided for managing teaching/learning process in Educational Sector.

Software as a Service (SaaS) is the most widely used cloud computing service in higher education. Email is the most popular SaaS application in the cloud. SaaS covers a wide variety of other applications for managing teaching/learning process that include Content Management System (also called as Learning Management System), Student Information System (SIS) and applications for Academic Research. Using PaaS cloud offering, educational institutions can take advantage of the existing platforms available on the cloud through one of the service providers, without having them installed on their own systems located in the campus. This eliminates the need for installing all the necessary hardware and system software (such as OS, Compilers, Interpreters etc.) required to setup various platforms of their choice on the campus. Just by providing Desktops or workstations with an internet connection, students can work on multiple platforms for developing and testing programs using various programming languages.

Using IaaS on Google or AWS helps educational institutions minimize the up-front costs involved in setting-up and running the hardware such as servers, storage, and networking devices. Resources such as CPU, storage, and networking bandwidth are dynamically allocated among multiples tenants in IaaS. This enables sharing of resources and costs among a pool of users of IaaS, and improves the efficiency of systems that are often underutilized. The below figure (Figure-2) compares the services of SaaS, PaaS and IaaS cloud offerings for educational institutions to manage the teaching/learning process:

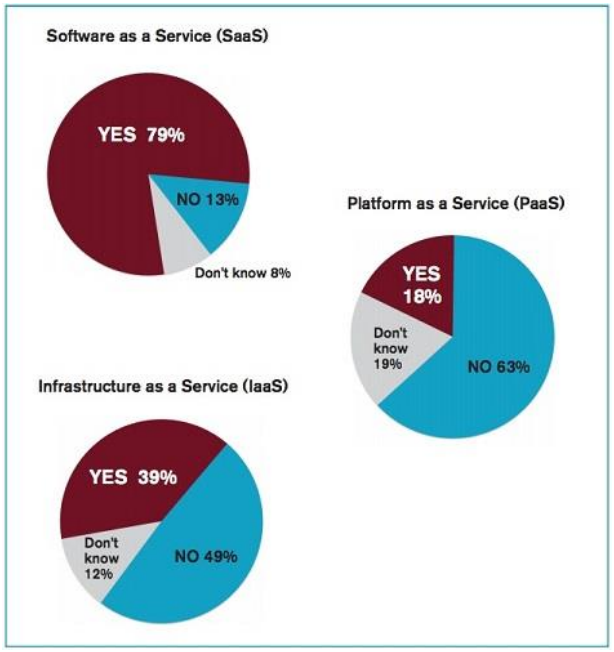

Figure-2: Use of Cloud Services in Education Institutions

Almost eight out of 10 (around 80 percent) respondents report that their institutions are using SaaS. Only four out of 10 respondents (around 40 percent) report that their institutions use Infrastructure as a Service (IaaS). Platform as a Service (PaaS) is the least widely used cloud service as it is meant for developers who can develop and deploy their own software (SaaS) over the Internet without downloads or installation [9].

IV. REVIEW OF EXISTING LITERATURE

In any research work, the researcher is expected to provide evidence of reading a certain amount of relevant literature in order to have some awareness of the current state of knowledge on the subject. The purpose of literature review is primarily to demonstrate the level of understanding of his/her research work. The major benefits of conducting a literature review area as follows:

i) It helps the researcher to defend his/her choice of problem undertaken for research

ii) It helps in determining what extent the research topic chosen is important and current.

iii) It helps to get to know the background information required to ensure better comprehension of the research work

The literature search process of the literature review involves querying scholarly literature databases such as IEEE Explore, Science Direct, EBSCO Host, Pro Quest, Wiley Online Library, ACM Digital library. The following are some of the findings of the author during the literature review process. **Arjun Kumar et al** (2012) in their conference paper proposed a model, in which the data stored on the cloud will be encrypted by using the elliptic curve cryptography approach. According to this model, secret key is used to encrypt user's data on the cloud. On user's request, data stored on the cloud will be sent in encrypted form to the user. After arrival of data at the client side, data will be decrypted and made available to the client in plain text [10]. **Gurpreet Singh et al** (2013) in their journal article surveyed the existing encryption techniques and found that the AES algorithm is most efficient in terms of speed, time, and throughput [11].

Fei Han et al (2016) in their survey paper on "Searchable Encryption" classified the searchable encryption algorithms based on the mode of their operation. They have identified the algorithms that can be used for implementing searchable encryption on cloud data. They concluded that the searchable symmetric encryption enables its users search securely on the encrypted data on the cloud. According to them, data can be uploaded in encrypted form along with the secret keys. Receivers can securely search on it with the help of private keys generated and shared by the owner of the data [12].

Surya Karunagaran et al (2017) have identified in their journal article the differences between SMEs and large enterprises in adopting the cloud technologies. They found out that any enterprises that employ between 50 and 250 people and having an annual turnover not exceeding 50 million are termed as SMEs. They have also analyzed the issues that must be dealt with while adopting the cloud from users' perspective. They concluded that though there are differences in cloud adoption between SMEs and large firms at present, they are likely to diminish over a period of time as the technology matures [13].

Nate Drake et al (2021) in their article published online at techradar.com identified some of the best cloud services providers who provide Database as a Service for storing and managing data in a database on the cloud. He recommended the service provided by Cloud Providers such as Oracle, who use always-on encryption to keep the information safe and secure from intruders [14]. **Georgios Amanatidis et al (2007)** in their journal article proposed several searchable encryption schemes that are easy to implement and are defined based on standard cryptographic primitives such as block ciphers, symmetric encryption schemes, and message authentication codes [15]. **Erez Shmueli et al (2014)** have suggested a new architecture for achieving high level of data security while offering enhanced performance and total transparency to the application layer. They outlined the implementation details of their new architecture using various DBMS, which include Open Source MySQL [16].

Zonda Wu et al (2012) have devised a strategy for querying encrypted character strings stored in a database on the cloud. In this approach, they store index values along with the encrypted character strings in a database. During the query operation, the index values are queried first in order to filter out some of the tuples not related to the condition. The resultant tuples are decrypted at the client side and a refined query is executed for extracting the required data [17]. **Jianfeng Wang et al (2017)** in their journal article proposed a novel search scheme based on Invertible Bloom Filter (IBF) for outsourced database on the cloud. In this scheme, users can achieve verifiability of search result without the process of pre-counting. It also uses Multi Party Searchable Encryption (MPSE) algorithm for overcoming collision attack between the CSP and any malicious users [18].

Clemens Heidinger et al (2013) have proposed three novel data-transformation and query-execution schemes for query processing of data in a database. They introduced three data-transformation and query-execution schemes SSEARCH, SMULTI-SEARCH, and SAPPROX for speeding up the query processing of databases [19]. **Ji Hong Kim et al (2013)** in his Book Chapter published by Springer proposed a new database encryption algorithm using Bloom Filter with the bucket index method. They also demonstrated the superiority of the proposed algorithm through several experiments [20].

V. IMPLEMENTING DATA PRIVACY ON THE SERVER

In this research work, the primary concern is to upload the text files or excel worksheets securely onto the server machine which is maintained by a service provider on the internet or public cloud. By default, a User Interface (UI) is provided by the service provider of the public cloud or domain space, for uploading and managing the resources on the server. The UI provided for this purpose is known as Dashboard or Control Panel. In order to access the storage space available on the server through such UI, the user has to login first using valid credentials to prove him/her as a valid user. Then only he/she will be allowed to manage the resources on the server. Allowing everyone to access the Dashboard or Control Panel is not a good practice. Because, it gives the user complete access to all the resources uploaded and managed on the server that include databases. Hence, we need a tool such as *filegator* – a Open Source Software for file uploading and downloading from a particular folder on the server. With the help of OSS - *filegator*, users can login to the server for uploading and managing files in a particular folder on the server.

For Server-side encrypting of text files, encryption must take place as soon as the files are uploaded. Securing the content of a text file on the server can be done using Advanced Encryption Standard (AES). AES is a kind of symmetric encryption algorithm, which makes use of the same key for encryption as well as for decryption process. While encrypting the contents of a text file, encryption is applied line by line. The user has to provide the key at the time of encrypting the text file. After encryption, the encrypted file can be moved and kept in a subfolder named *Encrypted*. As soon as the encryption process is over, the original file having the plain text must be deleted from the server. Similarly, for securing the data on a database on a server, the data must be encrypted as soon as they are inserted or imported from an external source (.csv file).

Each and every file to be encrypted and kept on the server will use a unique key for its encryption/decryption process. There is a separate table created and maintained in MySQL database for managing the keys. The actual keys are encrypted and stored in a table (named *tbl2)* in the database on the server itself. A special key is used for encrypting the actual keys that are associated with each and every resource (be it a file or a table in the database) on the server. Hence, for encryption, we need two keys: one is the special key (key to encrypt the actual key) and the other one is the actual key itself.

The special key is used at the time of encryption as well as decryption. With the help of special key, we can decrypt and obtain the actual key used for decrypting the cipher text. Therefore, it is the duty of end user to keep the special key secret so that the privacy of data can be maintained successfully on the server.

CONCLUSION

By knowing the various services provided by the Cloud Service Providers (CSPs), educational institutions can make use of them for improving their teaching/learning process that involves both staff and students. In this paper, the authors have done an analysis of various services provided by three major players of Cloud Computing for managing Teaching/Learning process effectively in Educational sector. The authors have also identified the need for an Open Source Software such as *filegator* that can be used for easily uploading and managing the files on the cloud. They have suggested the need for a symmetric encryption algorithm like Advanced Encryption Standard (AES) for storing sensitive data on the cloud. For searchable encryption, they have proposed an Extended Play-fair symmetric-key algorithm that can be used for securing non-sensitive data on the cloud.

REFERENCES

[1] David Livingston J, Kirubakaran E, "Client/Server Model of Data Privacy using Extended Playfair Cipher for SaaS Applications on the Cloud", International Journal of Innovative Technology and Exploring Engineering, August 2019, DOI:10.35940/IJITEE.j9274.088101, https://www.ijitee.org/wp-content/uploads/papers/v8i10/J92740881019.pdf

[2] David Livingston J., Kirubakaran E. (2021) Implementation of Extended Play-Fair Algorithm for Client-Side Encryption of Cloud Data. In: Peter J., Fernandes S., Alavi A. (eds) Intelligence in Big Data Technologies—Beyond the Hype. Advances in Intelligent Systems and Computing, vol 1167. Springer, Singapore. https://doi.org/10.1007/978-981-15-5285-4_48

[3] https://en.wikipedia.org/wiki/Microsoft_Azure

[4] https://searchcloudcomputing.techtarget.com/definition/Windows-Azure

[5] https://cloud.google.com/appengine/kb/

[6] https://gsuite.google.com/learning-center/products/docs/get-started/#!/

[7] https://www.investopedia.com/terms/g/google-blogger.asp

[8] https://edu.google.com/k-12-solutions/classroom/?modal_active=none

[9] https://eschoolmedia.com/wp-content/uploads/2016/06/vion0622.pdf

[10] Arjun Kumar, Byung Gook Lee, HoonJae Lee, "Secure Storage and Access of Data in Cloud Computing", Conference Paper, October 2012, DOI:10.1109/ICTC.2012.6386854

[11] Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", 2013, International Journal of Computer Applications, Volume 67– No.19, April 2013

[12] Fei Han, Jing Qin, Jiankun Hu, "Secure Searches in the Cloud: A Survey", 2016, Journal of Future Generation Computer Systems, Available online at: http://dx.doi.org/10.1016/j.future.2016.01.007

[13] Surya Karunagaran, Saji K Mathew, Franz Lehner, "Differential Cloud Adoption: A Comparative Case Study of large Enterprises and SMEs in Germany", 2017, Springer Journal of Information System Front, Published online: 13 August 2017, DOI: 10.1007/s10796-017-9781-z

[14] Nate Drake, Brain Turner, "Best Cloud Databases of 2021", Published online, March, 2021 at https://www.techradar.com/news/best-cloud-database

[15] Georgios Amanatidis, Alexandra Boldyreva, and Adam O'Neill, "Provably-Secure Schemes for Basic Query Support in Outsourced Databases", 2007, Data and Applications Security 2007, LNCS 4602, pp. 14–30, 2007, DOI: 10.1007/978-3-540-73538-0_2

[16] Erez Shmueli, Ronen Vaisenberg, Ehud Gudes, Yuval Elovici, "Implementing a Database Encryption Solution, Design and Implementation Issues", 2014, Journal of Computers & Security, Available online at: http://dx.doi.org/10.1016/j.cose.2014.03.011

[17] Zonda Wu, GuanDong Xu, Zong Yu, Xun Yi, EnHong Chen, YanChun Zhang, "Executing SQL Queries over Encrypted Character Strings in the Database-as-a-Service Model", 2012, Journal of Knowledge-Based Systems, Published by Elsevier B.V., Available online at: http://dx.doi.org/10.1016/j.knosys.2012.05.009

[18] Jianfeng Wang, Xiaofeng Chen, Jin Li, Jiaolian Zhao, Jian Shen, "Towards Achieving Flexible and Verifiable Search for Outsourced Database in Cloud Computing", 2017, Journal of Future Generation Computer Systems, Available online at: http://dx.doi.org/10.1016/j.future.2016.05.002

[19] Clemens Heidinger, Klemens B¨ohm, Erik Buchmann, Martin Spoo, "Efficient and Secure Exact-match Queries in Outsourced Databases", 2013, Published online: 28 November 2013, Springer Science and Business Media Network 2013, Available online at: https://link.springer.com/article/10.1007/s11280-013-0270-0

[20] Ji Hong Kim, Tony Sahama and Sung Yong Kim, "A Performance Test of Query Operation on Encrypted Database", 2013, Chapter 89, Future Information Communication Technology and Applications, DOI: 10.1007/978-94-007-6516-0_89