



MACHINE LEARNING APPROACH FOR CRYPTOSYSTEM SUGGEST IN EDUCARE OVER CLOUDS



Ravish G K¹  and Dr. K Thippeswamy² 

¹Assistant Professor Department of Cse, Cpgs Vtu Mysuru, Belagavi, India

²Professor, Department of Cse, Cpgs Vtu Mysuru, Belagavi, India



ABSTRACT

In the current situation of the pandemic, global organizations are turning to online functionality to ensure survival and sustainability. The future, even though uncertain, holds great promise for the education system being online. Cloud services for education are the center of this research work as they require security and privacy. The sensitive information about the users and the institutions need to be protected from all interested third parties. However since the data delivery on any of the online educare systems is always time sensitive, the cryptosystems have to be fast. In previous works some of the algorithms were explored and statistical inference based decision was presented. In this work a machine learning system is designed to make that decision based on data type and time requirements.

Received 2 June 2021

Accepted 17 June 2021

Published 30 June 2021

Corresponding Author

Ravish G K, gkravish@gmail.com

DOI [10.29121/
granthaalayah.v9.i6.2021.4009](https://doi.org/10.29121/granthaalayah.v9.i6.2021.4009)

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Copyright: © 2021 The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.



Keywords: Machine Learning, Cryptography, Cloud Computing, Online Educare, Decision Support

1. INTRODUCTION

The pandemic has left many a industry in a conundrum so as to how to adapt to the radical change. Many industries has fast changed their basic operational mode to work from home. However, educare has been in the middle of this crisis and still finding ways to accommodate the traditional and modern pedagogy in the online mode of teaching. When data goes online on a streaming platform, its security becomes a prime challenge for the provider as well as the user. Many methods exist and each has its own pros and cons.

In this research paper, based on the studies conducted by the same authors [Ravish and Thippeswamy \(2020b\)](#) [Ravish and Thippeswamy \(2020a\)](#) and [Ravish and Thippeswamy \(2021\)](#), a machine learning system capable of suggesting a suitable cryptosystem for use in cloud based educare systems. This is so because Initially a set of systems were compared for their parameters for common sized files with mixed

content as shown in Table 1 from the work presented in [Ravish and Thippeswamy \(2021\)](#). On top of the results from [Ravish and Thippeswamy \(2021\)](#), a decision tree algorithm was applied and best suited cryptosystem was suggested by the algorithm. The method and results are presented in the next sections.

The list of methods or cryptosystems to protect data in clouds is a rather long one [Padhy et al. \(2011\)](#). However, since education platforms on cloud tend to require faster encryption with above average security whereas other data sharing systems require high security albeit the time consumption;

Table 1 Comparison of Cryptosystem parameters [Ravish and Thippeswamy \(2021\)](#)

Parameters	RSA	DH	DES	AES	3-DES	Bitwise Stream Cipher	SSL	OTP
File Size	1024	1024	1024	1024	1024	1024	1024	1024
Key size	128	64	56	256	192	1024	128	1024
E. Time	0.208	0.208	0.402	0.604	1.206	0.088	0.167	0.314
Complexity	0.8013	0.6728	0.7691	0.9301	0.928	0.6152	0.7193	1

For the data in [Table 1](#), a radar plot is shown below to help understand the various parameters and how they're affected by different algorithms.

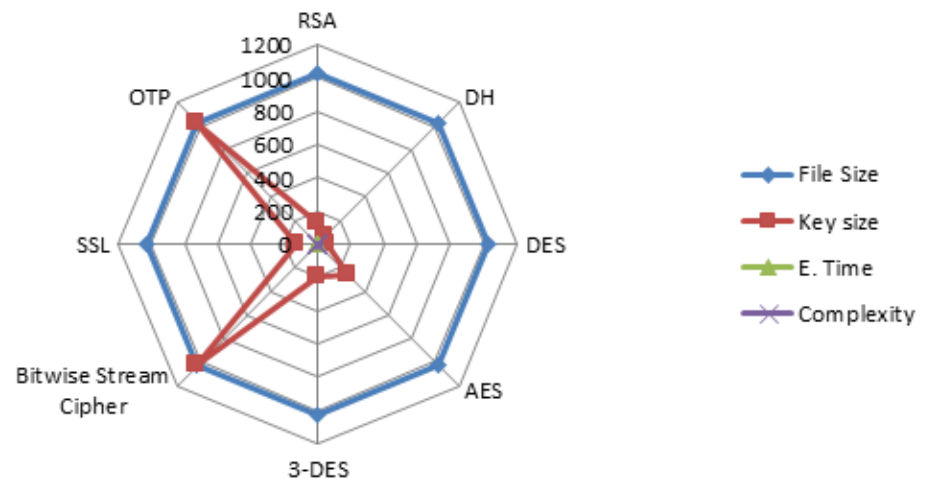


Figure 1 Graph showing the relation between data from [Table 1](#).

The correlation from the graph makes it evident that on any time bound system the best bets are on bit wise stream cipher and/or secure session layer.

2. MATERIALS AND METHODS

The data for the research work is from Harsha S et al [Harsha et al. \(2015\)](#) [S et al. \(2016\)](#) and the additional experiments were carried on a cloud simulation “CloudSim” a free cloud simulation platform. The method is iterated below.

The system is simulated as an online educational platform with multiple users accessing varied contents via a registered portal [Wallace \(2014\)](#). In a multi-user multi-service environment security issues rack up quite quickly and into large volumes [Ahmed and Hossain \(j2014\)](#). The onus of protecting data as well as the user privacy is always on the service provider “[Securing The Cloud For The Enterprise” \(2015\)](#). Using the methods listed in [Ravish and Thippeswamy \(2020b\)](#) it was attempted to provide security and privacy to the data. The algorithm was designed to look into the type of data that needed to be encrypted and the time frame for the data delivery and make a decision based on the two in selecting a suitable cryptosystem.

The data usually contains text, images, formatted text, power point presentations, audio and video. This clearly places a rider on the type of cryptosystems one can choose from “[State Of Cloud Security](#)”, [CSA Global Enterprise Advisory Board \(2016\)](#) [Fu et al. \(2013\)](#). Also users with individual connection have different requirements from those with a Wi-Fi [Harsha et al. \(2018\)](#). Hence the decision tree based algorithm was slightly altered to suite the requirement of this experimentation. The algorithm runs from the enterprise server on each request independently and unique decisions are provided each time. The training and testing samples have a ratio 80:20.

3. RESULTS AND DISCUSSIONS

The experiment was run on 1000 files with varying number of users as given in [Ravish and Thippeswamy \(2020a\)](#). The conditions were varied for different requirements and speeds. The sample of data obtained from the results is shown below.

Table 2 Training and Testing results from Decision tree

Requests (X100)	Train_Acc	Train_Loss	Test_Acc	Test_Loss
1	0.006657	0.977297	0.824888	0.470182
2	0.008624	0.942908	0.828614	0.447142
3	0.009605	0.924438	0.832964	0.417871
4	0.0101	0.913609	0.838279	0.384107
5	0.010236	0.909096	0.83998	0.367999
6	0.011852	0.884438	0.84168	0.337444
7	0.012893	0.86844	0.842542	0.310876
8	0.013977	0.852588	0.845343	0.284352
9	0.015106	0.836883	0.84811	0.257872
10	0.016278	0.821323	0.850841	0.247243
11	0.017494	0.80591	0.853537	0.242603

Continued on next page

Table 2 continued

12	0.018754	0.790642	0.856199	0.238007
13	0.020058	0.775521	0.858825	0.233455
14	0.021405	0.760545	0.861417	0.228947
15	0.022796	0.745716	0.863973	0.224483

From the data presented in Table 2 , it can be seen clearly that as the number of requests increases, the accuracy improves and loss reduces drastically. The accuracy and loss plots are shown in Figure 2 .

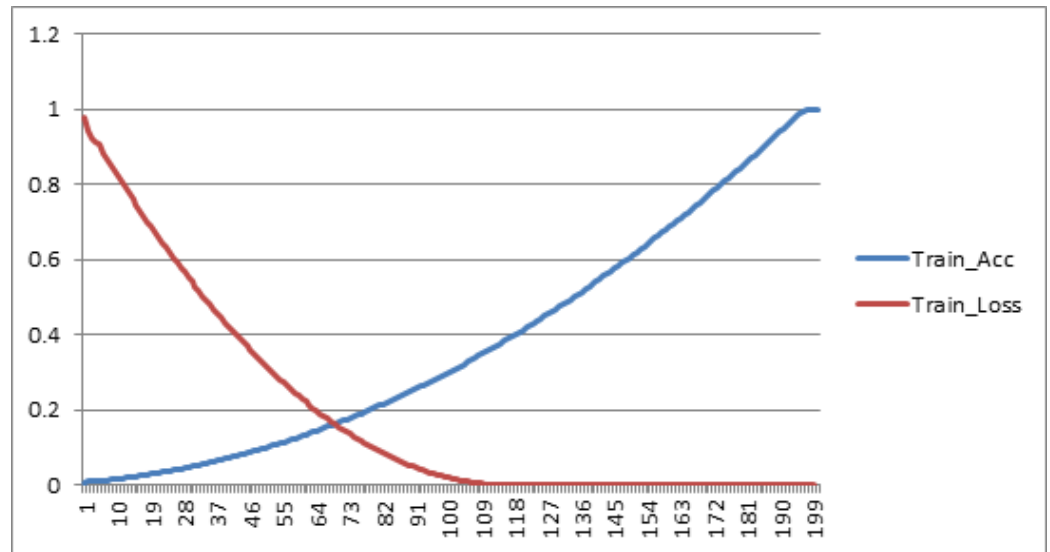


Figure 2 Training accuracy and loss

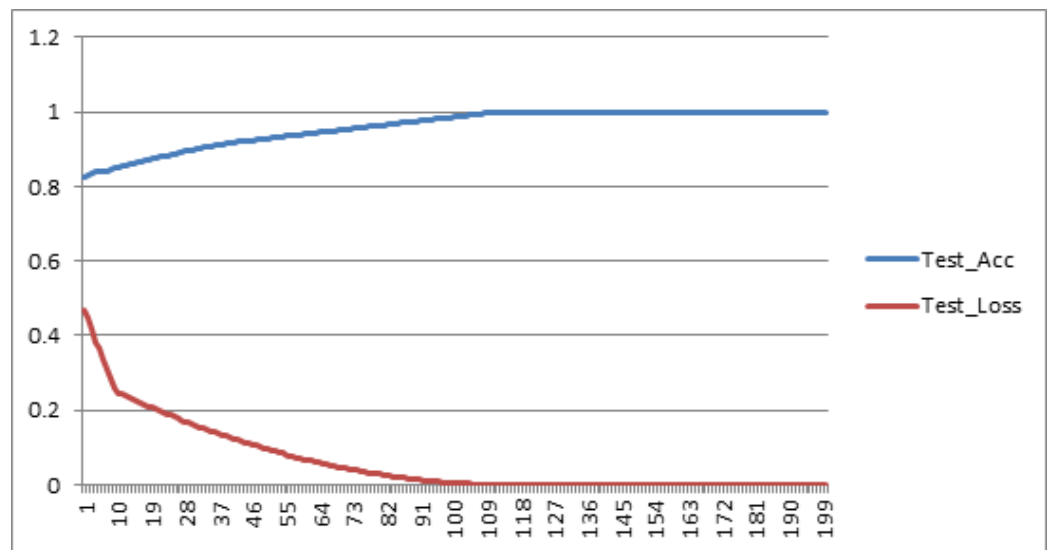


Figure 3 Test accuracy and loss

The graphs show that over large number of requests (say 100000), loss reaches 0 and remains as the decision made by the algorithm suites the data as well as the requirement perfectly.

4. CONCLUSIONS AND RECOMMENDATIONS

From the experimental data it can be interpreted that an altered decision tree [S et al. \(2016\)](#) can be utilized in place of a human choice with faster decisions and higher accuracy every time over large cloud based platforms for online education.

This work can further be continued and other decision making and decision support systems such as classification and regression algorithms can be experimented with to choose the best suited cryptosystems to cater to the ever increasing need for faster and secure data protection and privacy in cloud based online streaming platforms for educare, medicine, industry and any other business.

REFERENCES

- Ahmed, M., & Hossain, M. A. (2014). CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD. *International Journal Of Network Security & Its Applications (IJNSA)*, 6(1).
- Fu, H.-C., Xu, Y.-Y., Pao, H.-T., & Wang, J. (2013). Interactive Video Platform For E-Learning And Remote Services. *IJCSI International Journal Of Computer Science Issues*, 10(1).
- Harsha, S., Bhaskar, M. N., & Sheshaprakash. (2015). A 3-D Advancement To Pythocrypt For Any File Type. *Journal of Open Innovation: Technology, Market, and Complexity*. <https://doi.org/10.1186/s40852-015-0022-8>
- Harsha, S., Nazim, K., Vallabh, S. A., & Rao, V. (2018). Improving Wifi Security Against Evil Twin Attack Using A Light Weight Machine Learning Application. *In IJACT By Compusoft ISSN*, 2320-0790.
- Padhy, R. P., Patra, M. R., & Satapathy, S. C. (2011). Cloud Computing: Security Issues And Research Challenges. *IRACST - International Journal Of Computer Science And Information Technology & Security (IJCSITS)*, 1(2).
- Ravish, G. K., & Thippeswamy. (2020a). Analysis Of Time Delays Incurred For Security In Cloud Based Data Services For Educare Systems. *Journal of Xi'an University of Architecture & Technology*, 12(11), 365-368.
- Ravish, G. K., & Thippeswamy. (2020b). STEM Learning Environments On Clouds - A Data Security Perspective, *IJETER, WARSE.*, 8. [10.34218/IJARET.11.12.2020.091](https://doi.org/10.34218/IJARET.11.12.2020.091)
- Ravish, G. K., & Thippeswamy. (2021). Enhancing Security In Cloud Based Educare Platforms. *Journal of Xi'an University of Architecture & Technology*, 13(4), 219-224. Retrieved from <https://www.xajzkjdx.cn/gallery/22-april2021.pdf>
- S, H., Bhaskar, N., Sheshaprakash, M. N., & Rao, G. R. (2016). Auto Mutating Cryptosystem- An approach towards better security. *IOSR Journal of Computer Engineering*, 18(04), 42-46. Retrieved from <https://dx.doi.org/10.9790/0661-1804054246> [10.9790/0661-1804054246](https://doi.org/10.9790/0661-1804054246)
- Securing The Cloud For The Enterprise. (2015). *A Joint White Paper From Symantec And VMware*.
- "State Of Cloud Security", *CSA Global Enterprise Advisory Board*. (2016).

Wallace, A. (2014). Social Learning Platforms and the Flipped Classroom. *International Journal of Information and Education Technology*, 4(4), 293–296. Retrieved from <https://dx.doi.org/10.7763/ijiet.2014.v4.416> 10.7763/ijiet.2014.v4.416