

Enhancing Security in cloud based Educare Platforms

Ravish G K

*Research Scholar, VTU -RRC,
Belagavi, Karnataka, India*

Dr.K Thippeswamy

*Professor, Department of CS&E, VTU-RRC,
Belagavi, Karnataka, India*

Abstract: Education has taken a fore front in the services industry ever since the evolution of reforms (Education Commission of 1964–66) and amidst the pandemic, education has taken a vibrant turn towards being a completely online service. In many works, this change has been analyzed and logical conclusions are provided as to whether this would be a permanent shift or a temporary fix to the problem at hand. However, there are aspects of this system that need to be addressed such as speed of delivery, security, completeness of the user experience etc. In previous works, we had attempted to assess the above aspects. Post assessment, in this paper a comparison of the available security measures and a machine learning system to suggest the best suited method are presented.

Key words: *Cloud Computing, Educare, Security, Stream Cipher, Transfer Delay*

Introduction:

In the recent times, when the world is bracing itself for the second wave of the pandemic, educational services are facing a new challenge to adapt or expire. Most systems are shifting to the cloud based platforms where they have seen considerable success. However, in most related works, one can observe that the major challenges are not data delivery or the experience but the security and time delay incurred to the service by the security algorithm. Hence most systems utilize stream ciphers which consume very little time when compared to other algorithms. However, stream cipher security is questionable when it comes to extended usage as the repeated use of keys and the simplicity of the bitwise operations. In this paper a machine learning system is designed on a cloud simulation to compare and contrast some cryptosystems and to finally present to the user, a feasible cryptosystem for any given file type and size.

Review of Previous Work:

This research work encompasses the study of cloud computing, cloud platforms for education, network security, cloud security and their performance issues and features. The study done so far is presented below.

The authors of [1] describe an architecture for a cloud based classroom for online education in the period of the pandemic. The paper details the issues that may be faced by the implementation and also attempts to provide feasible solutions to the said issues.

In [2] a major issue of cloud computing systems is analyzed and presented in detail. Security for data and other resources on cloud is of prime importance and it requires major research to understand and develop solutions.

[3], [4], [5] and [6] present a basic idea of cloud computing and analyze the key challenges for the cloud computing research and industry. They also describe the threat to cloud based educare platforms from piracy and other forms of copyright infringement.

In [7] the authors examine the use of social learning platforms with the emergent pedagogy of the “flipped classroom”. They have considered “Edmodo” as a case study in the United Kingdom area for drawing their conclusions.

[8] presents a review on the cloud computing concepts as well as security issues of cloud computing and cloud infrastructure. It concludes that where a user needs to have cloud storage or cloud computing or both as a services, all the 3 cases have inherent issues of security and delay.

[9] This white paper surveying the transformation of classic IT operations with the advancement in cloud computing, concludes that the issues of security and delay are the major concerns if left unanswered can impede the growth of the industry.

[10] This white paper presents cloud computing as a highly innovative tool that can be extensively used by industry as well as individuals for various computational needs. It also presents a cloud based governance model that can ease the administrative load on governments.

[11] and [12] present the problems in cloud computing as well as the advantages where the need for face to face meetings is fading out and classes are progressing towards being completely online. They conclude that technology has become invasive to the point that existence without it has become unimaginable.

[13] and [14] discuss the concepts of remote work, telework and cloud enterprises as they are on the rise since the past decade. The two white papers raise the same question in their conclusion, as to how can the problem of security in cloud environment be solved keeping in consideration the timeliness of service.

In [15], [16] and [17] the authors describe how online learning has evolved during the pandemic in a large scale with multiple players in the industry contributing to the change. Multinational companies such as Google inc started their own courses to train the educational professionals to use online platforms for enhancing the reach of educate.

In [18] the authors have presented a comparison of various encryption systems for different types of data which are enhanced in this paper for cloud data delivery service.

The authors of [19] present the faculty perception on the online learning, the apprehension, acceptance and opposition in a holistic manner to enhance one’s understanding of the current state of online educate platforms.

Methods and Materials:

The experimentation required various files of incremental size to be transferred on the cloud framework that was developed for the purpose of analysis. The algorithms chosen for the experiment and the resulting parameters are presented in Table 1. The same is plotted as a bar chart in Figure 1. On incrementing the file size, the time taken increased in a logarithmic manner whereas the algorithm’s complexity remained the same. This led to the data presented in Table 2. The table is overlapped with a heat map to highlight the extreme times taken by some of the most secure systems. When this data is plotted interesting patterns emerged. The same is presented in conclusion.

Table 1. Algorithms and their parameters for security

Algorithms	RSA	DH	DES	AES	3-DES	Bitwise Stream Cipher	SSL	OTP
Parameters								
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
WSTC(Pen-paper)	0.8013	0.6728	0.7691	0.9301	0.928	0.6152	0.7193	1

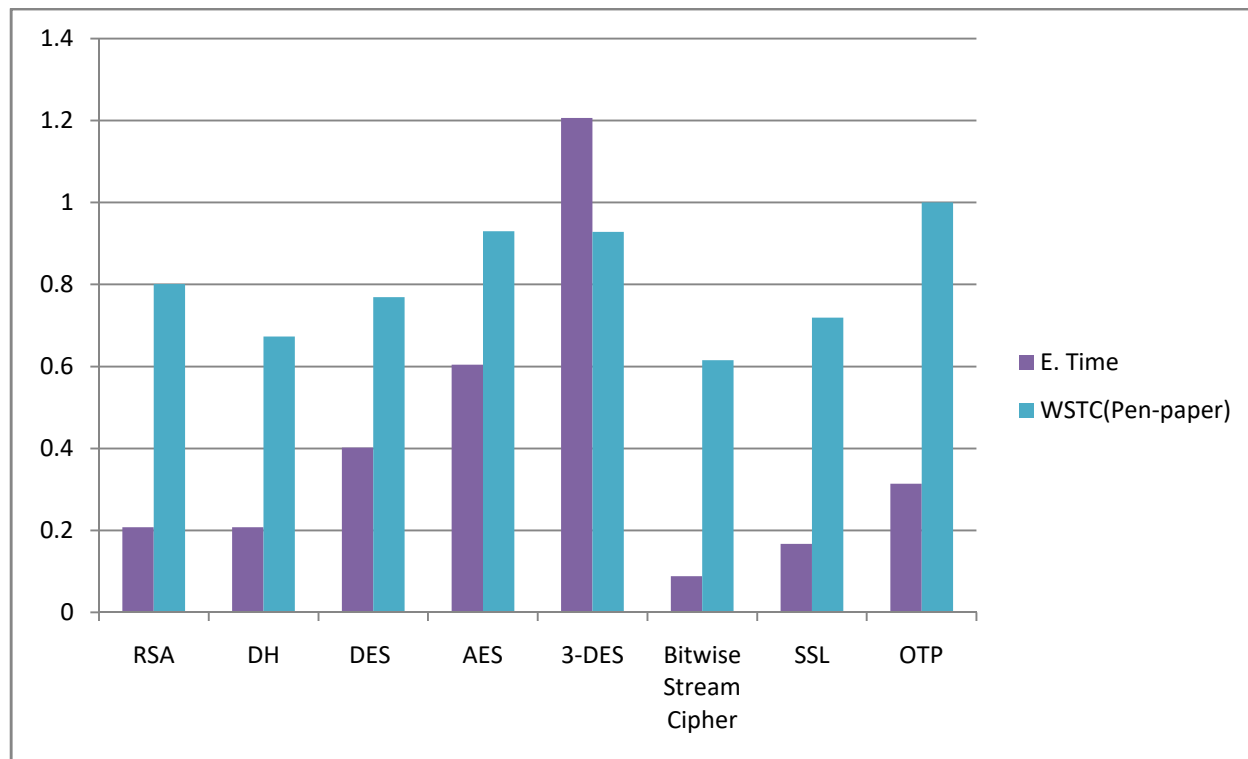


Figure 1. Bar graph showing the security vs delay

Table 2. Heat map of the incremental size of files and their encryption

File size (KB)	RSA	DH	DES	AES	3-DES	Bitwise Stream Cipher	SSL	OTP
1	0.208	0.208	0.402	0.604	1.206	0.088	0.167	0.314
2	0.217	0.217	0.650	1.190	3.101	0.026	0.143	0.440
3	0.326	0.326	0.975	1.785	4.651	0.039	0.214	0.660
4	0.434	0.434	1.300	2.380	6.201	0.052	0.285	0.881
5	0.543	0.543	1.625	2.975	7.751	0.065	0.356	1.101
10	1.086	1.086	3.250	5.950	15.503	0.131	0.713	2.201
20	2.172	2.172	6.499	11.901	31.005	0.262	1.426	4.403
30	3.258	3.258	9.749	17.851	46.508	0.392	2.138	6.604

40	4.345	4.345	12.998	23.801	62.011	0.523	2.851	8.805
50	5.431	5.431	16.248	29.752	77.514	0.654	3.564	11.006
100	10.861	10.861	32.496	59.503	155.027	1.308	7.128	22.013
200	21.723	21.723	64.991	119.007	310.055	2.615	14.256	44.026
300	32.584	32.584	97.487	178.510	465.082	3.923	21.385	66.039
400	43.446	43.446	129.982	238.014	620.109	5.231	28.513	88.052
500	54.307	54.307	162.478	297.517	775.137	6.539	35.641	110.065
1000	108.614	108.614	324.955	595.035	1550.274	13.077	71.282	220.130
2000	217.228	217.228	649.910	1190.070	3100.547	26.154	142.563	440.259
3000	325.842	325.842	974.865	1785.104	4650.821	39.231	213.845	660.389
4000	434.457	434.457	1299.820	2380.139	6201.094	52.308	285.127	880.518
5000	543.071	543.071	1624.776	2975.174	7751.368	65.385	356.408	1100.648
10000	1086.141	1086.141	3249.551	5950.348	15502.736	130.770	712.817	2201.296

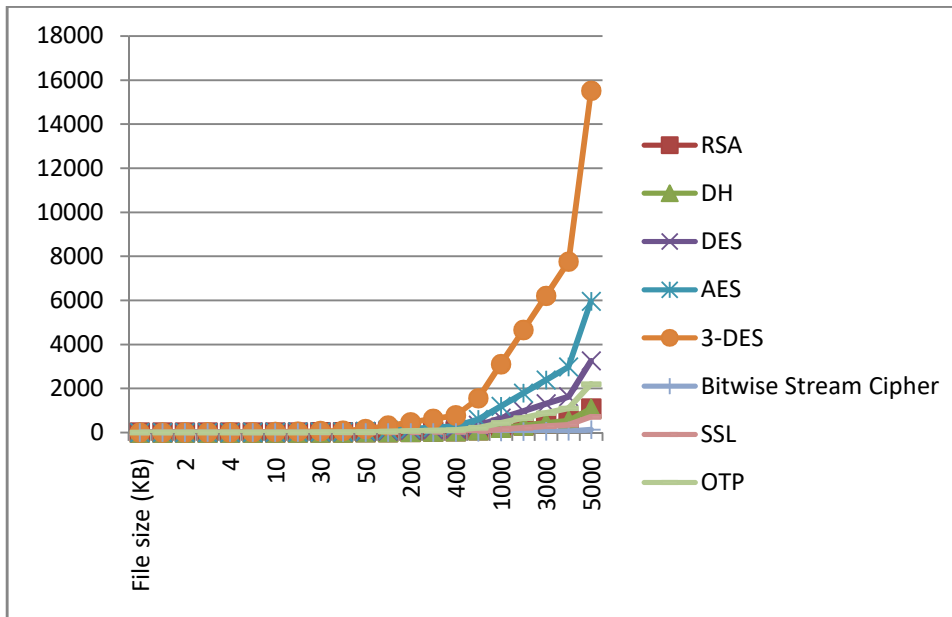


Figure 2. Graph of the encryption times

Results and Discussions:

From the graph in Figure 1 it can be seen that 3-DES (DES running 3 times on a data) consumes the highest time and One Time Pad (OTP) provides the best security. However, given the nature of the fluctuation of data and requirements, neither of them are optimal for a cloud. Hence using the incremental data size the same system is simulated to obtain the heat map in Table 2. From the data in Table 2, Figure 2 is plotted to reveal that Secure Session Layer, RSA and DH algorithms work best with a bivariate optimization over varied file sizes and security requirements.

Conclusion:

To conclude the experimentation has yielded successful results, where the algorithm has been able to suggest best suited cryptosystem over both time and security for a wide range of file types and sizes. With the implementation of this, cloud based educare platforms can further grow and be the next big change in the IT enabled services world.

References:

- [1]. Faritha Banu J etal, IoT based Cloud Integrated Smart Classroom for smart and a sustainable Campus, *Procedia Computer Science*, Volume 172, 2020, Pages 77-81
- [2]. Nurul Hidayah Ab Rahman etal, A survey of information security incident handling in the cloud, *Computers & Security*, Volume 49, March 2015, Pages 45-69
- [3]. Hoang T. Dinh, A survey of mobile cloud computing: architecture, applications, and approaches, *Wireless Communications and Mobile Computing*, 11 October 2011, <https://doi.org/10.1002/wcm.1203>
- [4]. <https://www.statista.com/statistics/688200/book-piracy-education/>
- [5]. <http://tdan.com/data-piracy-the-threat-from-within/5283>
- [6]. Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges", *IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS)* Vol. 1, No. 2, December 2011
- [7]. Albin Wallace, "Social Learning Platforms and the Flipped Classroom", *International Journal of Information and Education Technology*, Vol. 4, No. 4, August 2014
- [8]. Monjur Ahmed and Mohammad Ashraf Hossain, "CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD", *International Journal of Network Security & Its Applications (IJNSA)*, Vol.6, No.1, January 2014
- [9]. "Securing the Cloud for the Enterprise", A Joint White Paper from Symantec and VMware. White paper 2015
- [10]. "State of Cloud Security", CSA Global Enterprise Advisory Board, 2016
- [11]. Hsin-Chia Fu, Yeong-Yuh Xu, Hsiao-Tien Pao, Jiabin Wang, "Interactive Video Platform for E-learning and Remote services", *IJCSI International Journal of Computer Science Issues*, Vol. 10, Issue 1, No 1, January 2013
- [12]. Imane Moussaoui, Hafida Essaoudi, Mohamed El Ouazizi, Abdelaziz Hallaoui, Aziza El Ouazizi, Abdelouahed Essahlaoui, " Control Access to a Resource in an E-Learning Platform", *IOSR Journal of Research & Method in Education*, Volume 7, Issue 3 Ver. I (May. - June. 2017), PP 55-61.
- [13]. Jay L. Brand, "Learning to Support a Remote Workforce", HAWORTH 2011.
- [14]. CSO, "Security in the Cloud", White paper 2012
- [15]. Shivangi Dhawan, "Online Learning: A Panacea in the Time of COVID-19 Crisis", *Journal of Educational Technology Systems*, June 2020, <https://doi.org/10.1177/0047239520934018>
- [16]. <https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/>
- [17]. Petar Kolar "Experiences with Online Education During the COVID-19 Pandemic–Stricken Semester" *International Symposium on Electronics in Marine Engineering*, IEEEExplore.
- [18]. Harsha S, N Bhaskar, M N Sheshaprakash, "A 3-d Advancement to Pythocrypt for any file type", *Springer JOOI*, 2015

- [19]. Rome B. Moralista et al, "Faculty perception toward online education in a state college in the Philippines during the coronavirus disease 19 (COVID-19) pandemic" *Universal Journal of Educational Research*, DOI:10.13189/ujer.2020.081044