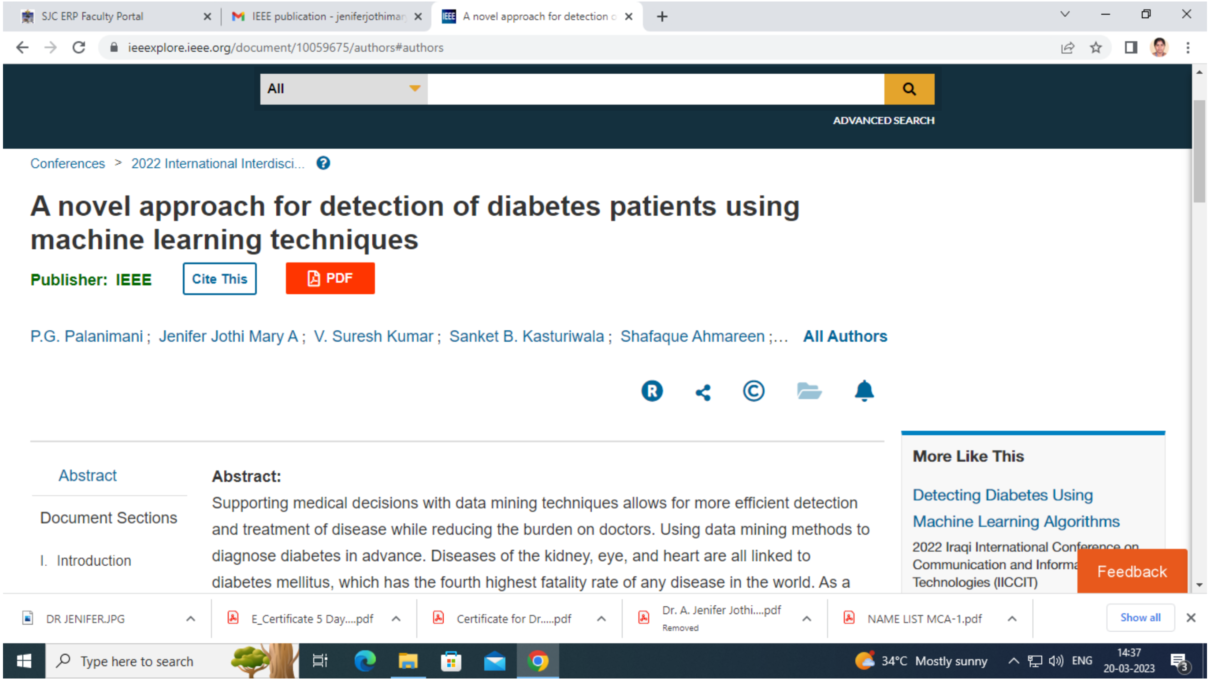

SJC ERP Faculty Portal
IEEE publication - jeniferjothimar
A novel approach for detection o
ieeexplore.ieee.org/document/10059675/authors#authors
All
ADVANCED SEARCH
Conferences > 2022 International Interdisci...
Cite This
PDF
All Authors
Feedback
DR JENIFER.JPG
E_Certificate 5 Day....pdf
Certificate for Dr.....pdf
Dr. A. Jenifer Jothi....pdf
Removed
NAME LIST MCA-1.pdf
Show all
Type here to search
34°C Mostly sunny
ENG
14:37
20-03-2023

A novel approach for detection of diabetes patients using machine learning techniques

Publisher: IEEE

P.G. Palanimani ; Jenifer Jothi Mary A ; V. Suresh Kumar ; Sanket B. Kasturiwala ; Shafaque Ahmareen ;...

Abstract

Document Sections

I. Introduction

Abstract:

Supporting medical decisions with data mining techniques allows for more efficient detection and treatment of disease while reducing the burden on doctors. Using data mining methods to diagnose diabetes in advance. Diseases of the kidney, eye, and heart are all linked to diabetes mellitus, which has the fourth highest fatality rate of any disease in the world. As a

More Like This

Detecting Diabetes Using Machine Learning Algorithms

2022 Iraqi International Conference on Communication and Informa Technologies (IICCIT)

AIP Conference Proceedings

Efficiency of online classes in Tamil Nādu during Covid-19 lockdown: A statistical analysis

Cite as: AIP Conference Proceedings **2418**, 030061 (2022); https://doi.org/10.1063/5.0081860
Published Online: 24 May 2022

A Jenifer Jothi Mary, Ch. Padmaja, B. Fathima Josepin Prasanna, et al.

View Online

Export Citation

AIP Conference Proceedings **2418**, 030061 (2022); https://doi.org/10.1063/5.0081860

AIP Publishing

Efficiency of Online Classes in Tamil Nādu During Covid-19 Lockdown: A Statistical Analysis

A Jenifer Jothi Mary[1, a)], Ch. Padmaja[2], Fathima Josepin Prasanna B[3], Jasmine B[4], S. Vijayprasath[3]

[1]St. Joseph's College (Autonomous), Affiliated to Bharathidasan University, Trichy, Tamil Nadu, India.
[2]Sumathi Reddy Institute of Technology for Women, Warangal, Telangana, India.
[3]Jayaraj Annapackiam College for Women (Autonomous), Periyakulam, Theni Dt., Tamil Nadu, India
[4]PSNA College of Engineering and Technology, Dindigul, India.
[a)] Corresponding author: ajenifer.jothi@gmail.com

***Abstract*.** The Corona Virus Disease (COVID – 19) pandemic, emanated in December 2019, in the city of Wuhan, China is deliberated as a significant challenge for all humanity. Later has rapidly spread throughout the world causing millions of lives. The Governments planned multiple strategies in controlling the outbreak, one of which measures was imposing lockdowns adequately. The inextricable situation has affected various walks of life of people, in particular the students of the educational institutions. Thus, the need of hour has come to broaden the horizons of hearing option for it. While digital learning, both educators and students face some inconveniences like network connectivity and conducive atmosphere for learning. The researchers conducted a case study to sort out the efficacy of the online classes during this pandemic situation and the challenges that digital learners face. Eventually, learner centric methods of teaching are discussed and valuation procedures are also presented in that research work.

Keywords— Efficiency of Online Classes, Digital Learning, Learner Centric Methods, Covid-19, Tamil Nadu, Lockdown.

INTRODUCTION

Originated in the mid of December 2019, novel Corona Virus has changed entire world. The deadly virus has spread in an accelerated speed through personal contact and in a few months scattered to more than 100 countries. Because of the severity of the deadly disease, World Health Organization (WHO) announced COVID-19 is a pandemic. Worldwide spread is caused by the high transmissibility of the virus. In order to control the virus spread, many countries announced lock down and the global economy was seriously disrupted by this outbreak. The impact of virus is not limited with health, but social, economic and environmental systems were also affected in a distinguished consideration [1]. It developed substantial challenges for the Education system globally. To reduce the spread of the disease, most Governments have temporarily closed the Educational Institutions including Schools, Colleges and Universities [2]. Though this closure is temporary, the consequences has forced many problems in learners' lives. The gap has affected their attentiveness in learning and due to the family situations students found jobs to balance the economic crisis. It threatened the right to education that resulted a fall in the literacy rate of many countries. To limit the disruption of education, UNESCO suggested all governments to use distance learning and online applications and platform to make the students to learn from the places where they are [3]. Virtual Classroom has changed many components of the education system. This paper attempts to analyze the components of online teaching and learning process in higher education system in Tamil Nadu, India and provides measures to improve the efficiency of online learning.

International Conference on Research in Sciences, Engineering & Technology
AIP Conf. Proc. 2418, 030061-1–030061-8; https://doi.org/10.1063/5.0081860
Published by AIP Publishing. 978-0-7354-4368-6/$30.00

COVID-19 AND INTERNATIONAL HIGHER EDUCATION

Crawford Joseph et al. discussed the responses of the Higher Educational Institutions to the pandemic situation globally [4]. They analyzed the action taken by Institutions across 20 countries and reported that the responses vary from no action to redesigning curriculum for fully online courses. Online Courses were conducted in several forms through real time lectures or recorded videos. The researchers came out with a finding that the recorded videos can be helpful as students can get it anytime anywhere.

Wei Bao presented a case study of Peking University, China and provided principles of high impact teaching practice to improve the efficiency of online learning in higher education [5]. The principles were listed as relevance, effective delivery of the information, sufficient support system, participation of the students and finally contingency plan preparation. These guidelines made the students to involve in online learning more effectively.

Mansureh Kebritchi et al., conducted a study on the issues related to the online teaching-learning process in higher education system [6]. They found three major categories of findings such as issues related to learners, instructors and content. Eric Bettinger et al., presented the promises and pitfalls of online education. Due to this present pandemic situation, online learning has extended to world-wide educational institutions and may to prolong further [7]. However, as the students are least prepared to face the new method of learning process, they struggled in gaining knowledge with the online class.

Muhammad Adna et al., expressed the Students' perspectives on Online learning amid the COVID-19 pandemic [8]. In under-developed countries like Pakistan, the online learning in higher education institutions will not produce desired effect as expected. Access to Internet is limited because of network availability and monetary issues. Eddie M. Mulenga et al., articulated that the COVID-19 would be the Gateway for Digital Learning in Mathematics Education [9]. The authors analyzed the education system in CBU, Zambia and gave suggestions for practicing Digital Learning especially in Mathematics in during this Pandemic period. They scrutinized the results of the questionnaire given to the University students to assess various social media applications, used for online learning. Though Zambia is one of the countries that are historically not conversant to digital learning, COVID – 19 prompted the need for online learning. Adoption of digital technology in this closure period inspired the evolution of online learning in Zambia.

Wenjun Cao et al., conducted a survey to analyze the psychological effect on students owing to COVID 19 [10]. They had collected a sample from Changzhi medical college, China to analyze the impact. The student's anxiety levels were highly diverted due to some positive and negative factors. Economic effect and delayed academic activities were highly correlated with the anxiety symptoms in students. Julio Torales described the COVID-19 and its impact on global mental health [11]. The spread of COVID – 19 infection all over the world not only affected people's health but also produced psychological problems. Health measures were used to analyze the psychological factors related with fear, anxiety and isolation. Student's health was monitored and strategies were required to solve mental health issues.

NEED FOR DIGITAL LEARNING IN INDIA

Due to the spread of the pandemic disease worldwide, almost every country announced lockdown for the whole country or for the affected region. The first conformed case of Corona virus in India was identified in Kerala on January 30, 2020 [12]. The patient had a travel history from Wuhan, China and she was cured. But with the outbreak of the new cases, Indian Government declared lockdown in four phases starting from March 24. With the identification of new cases in Indian states, Tamil Nadu Government was in emergency to take preventative measure to control the spread of Coronavirus in the state [13]. On Monday, 16 March, 2020, Tamil Nadu government had announced the closure of all educational institutions, theatres, parks, museum and all other people gathering places. This order came into effect from March 17 and till it continued. Government of India had instructed the universities and colleges to start the online classes from the first week of August to the students [14]. This paper analyses the efficiency of the online classes and proposes some measures to improve it.

METHODOLOGY

Collection of Data

The data were collected from students of various colleges in Tamil Nadu. Structured questionnaire was designed to evaluate the responses and issues of students attending online classes. In order to make the data reliable and true, the questionnaire was designed anonymous. Finally, 18,376 completed forms were collected from responses.

Cleaning Data

Data cleansing plays a significant role in constructing a model. When the data are cleaned before processing, it will avoid some unwanted failures and erroneous results. Simple algorithm is enough to process the cleaned information. Figure 1 depicted the process of cleaning data used in this research [15].

Step 1. *Managing missing data:* The result of the analysis will not be correct if some data were missing. The missing data were replaced with the values from the past records. As this survey use computerized forms, very few entries were missed in the dataset. They were replaced by the previous dataset.

Step 2. *Removal of unwanted observation:* In this step, some duplicate entries and the values which were not needed for further processing were removed from the dataset [16]. As the name of the students, their mail id and the Institution's names are not essential for further processing, they were removed from the dataset.

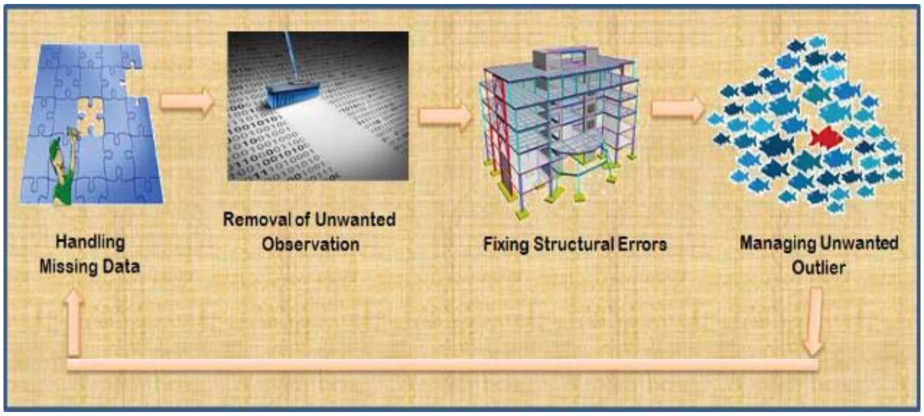


FIGURE 1. Data Cleaning Processes

Step 3. *Fixing structural errors:* Structural errors are typographical errors that arises while typing names and other details. Same attribute with different names and errors occurred while transferring the data. These data were handled using appropriate methods.

Step 4. *Managing unwanted outliers:* Among the 18,376 responses, few responses were found from School students. As this analysis considers only students from higher education, the details of school students were also removed. And the responses from other states were also ignored as the survey is limited to Tamil Nadu State. Totally 1,264 entries were removed and the remaining 17,112 responses were selected for final analysis.

Data Analysis

The collected data were analyzed with Chi – Square statistic and Cramer's V test. The analysis was conducted to identify the personal, emotional and social factors that influence the satisfactory level of the respondents while attending online class during this pandemic period. The correlation between the sample characteristics and efficiency level were explored by the nonparametric test Chi – square test. The Chi – Square test of independence determined the association between the categorical values. Spearman's correlation coefficient, c, was used to assess the dependency between the categorical values and Cramer's V values define the strength of association.

Cramer's V is used as post-test to find out strengths of association after significance was determined by chi-square test of independence. It possesses the value from 0 to 1, identifies the strength of dependency. Cramer's V value is calculated by the equation

$$\emptyset_c = \sqrt{X/(N*(k-1))} \tag{1}$$

Where, $\emptyset_c$ - Cramer's V

X - Pearson's Chi-squared statistic

N - Sample size

K - Min (number of rows or columns) i.e. lesser number of categories of any variable.

The value from 0 to 1 in Cramer's V reveals weak to strong association between the variables. The personal, social and economic factors of the respondents were recorded and considered for analysis. Among the respondents, 42% from Science Discipline, 36.5% from Arts, 15.4% belong to Engineering, 4.8% studying medical and the remaining are from various disciplines.

a. *Platform Used:* Though the Institutions prefer the convenient platform, the most widely used one is Google meet which is presented in Table 1.

TABLE 1. The Platforms Used by The Students to Attend the Online Class

Platform	Platforms used by the students to attend the online classes (In Percentage)
Google Meet	81.4
ZOOM	8.2
Cisco Webex	4.3
Microsoft Team	1.6
Others	4.5

b. *Device Selection:* Selection of device that is used for attending classes depends on the economic condition of the family. Only 71.3% use their own gadgets and the remaining 28.7% have borrowed from their family members, friends and relatives. So, they could not attend the whole class of a day.

c. Chi- square test for independence compares two variables that consists of categorical values to check the association between them. The factors such as duration of the class hours, break time between the sessions, accessibility of the device, data usage, network problems, health issues, interactivity and other distraction during the classes were analyzed using Pearson's Chi-Square test to assess the efficiency level of the digital learning. The p – value states whether the test results are significant or not. The p-value and Cramer's V values of the variables are listed in Table 2.

TABLE 2. Chi-Square Test Results and Cramer's V Values

	Satisfaction Level of Online Class		
	X-squared	p-value	Cramer's V Value
Duration	44.067	1.488e-05	0.1386594
Break time	5.4177	0.4915	0.05958408
Interactivity	628.66	2.2e-16	0.5237217
Accessibility of device	16.173	0.001045	0.1454952
Need for additional data	3.7223	0.2931	0.06980058

d. *Reasons for skipping Online Classes:* The advantage of digital learning is that any students can attend the classes from anywhere where they are residing. They need not to be physically present in the college campus. But the problematic truth is that they are not fully present throughout the class hours. Though coping with the new method of teaching learning process is not an easy task, there are many other factors that made the students leave or skip the online classes. The problems may be from their family, health problems, network problems or lack of their own interest. Figure.2 illustrates the reason for skipping the online classes by the students.

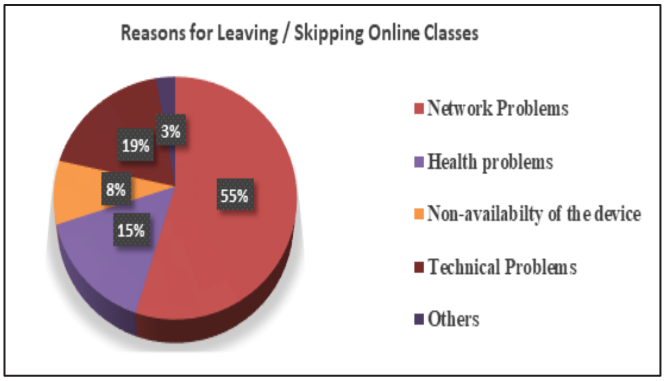


FIGURE 2. Reasons for skipping Online Classes

e. *Distractions during Classes:* The students are distracted by many aspects in online class mode, as their teachers are not monitoring them. Another key factor is incoming calls while attending classes (51.2%). Most of the students are using mobile phones to attend the classes and some of them are attending with their family member's mobile phones in which the incoming calls to the phone is a great disturbance for the students. A list of distraction that affect student's concentration is depicted in Figure.3.

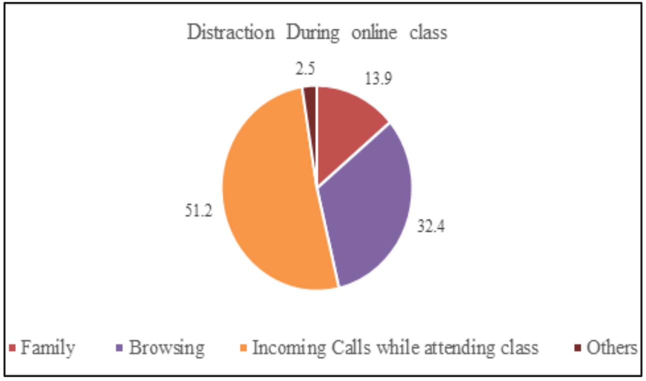


FIGURE 3. Distraction that affects student's concentration

f. *Health problems:* The only solution any country to provide education during this COVID – 19 situations are online learning. But long screen time and usage of electronic gadgets cause many problems to student's health. It creates eye dryness, irritation, back pain and especially mental stress. Figure 4 reveals that the major problem the student encounter is eye irritation with the highest percentage (63.5%). The students are also affected with other problems such as Headache, Mental stress and back pain. Surprisingly, 11.3% respondents reported that they didn't face any health issues.

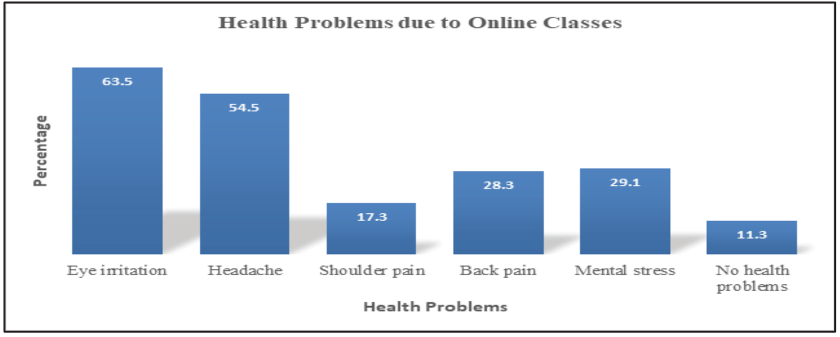


FIGURE 4. Health problems due to Online Classes

g. *Factors influencing the classroom teaching with Online Classes during the epidemic:* Table 3 presents the association between the factors that helps to analyze the efficiency of online classes with traditional classroom. For variables having two groups of values, Mann-whitney test is used [17]. Availability of the supporting material for the online learners had significant effect on the comparison between online and traditional classes. (p = 0.028). Kruskal Wallis test is applied to identify the relationship between the variables when there are more than two groups to compare [18]. All the factors the course chosen by the students, level of understanding and Interactivity of the session have significant effect on the effectiveness of virtual classrooms. (P<0.05). Among the variables, the course of the students and interactivity of the session had high impact with the smaller value for p.

TABLE 3. Univariate Analysis of College Students' Opinion on Comparison of Classroom Teaching with Online Classes

Variables	Total	Normal	Comparison of classroom teaching with Online Classes				Statistics	P
			Poor	Fair	Good	Excellent		
Course Type							−0.805[b]	
Arts	6414	4861	899	1480	3194	832		3.1e-7
Science	7827	5853	1098	1805	3898	1016		
Engineering	2647	1953	371	611	1318	343		
Medical	224	170	31	52	112	29		
Providing Supporting Material							0.292[a]	
Yes	16484	12492	2312	3802	8210	2139		0.02857
No	628	476	88	145	313	81		
Level of Understanding							30.550[b]	
Poor	1436	1088	201	331	715	186		0.0023
Fair	3185	2414	447	735	1586	413		
Good	10497	7955	1472	2421	5228	1362		
Excellent	1995	1512	280	460	994	259		
Interactivity of the Session							−7.262[b]	
Poor	1973	1495	277	455	983	256		2.2e-9
Fair	3118	2363	437	719	1553	405		
Good	9487	7189	1330	2188	4725	1231		
Excellent	2534	1920	355	585	1262	329		

[a]*Mann-Whitney test.* [b]*Kruskal-Wallis test.*

DISCUSSION

Data were collected from a sample of 17,112 students from various colleges in Tamil Nadu. Most of the respondents are from arts and science colleges. It is understood that most widely used platform for conducting online classes is Google meet. It was observed that network problems, health issues and interactivity during the class have the high impact on the satisfactory level of the online learning with values approximately greater than 0.5 indicating high dependency. But the duration for break time and the need for additional data specifies less significance in the understanding level in digital learning. So, interactivity during the online class plays a vital role in improving the efficiency of online teaching learning process.

Regarding the difficulties for attending classes, network problem is prevalent among others as it is 55 %. Both the faculties and students face this complication. As a good number of students are from rural, remote places and the internet connectivity is a major problem for them. There are some other problems that make the students to leave or skip the classes. Technical problems (19%), health problems that are caused by attending online classes (18 %) and non-availability of the device (8%) make the students to avoid the classes. Among the health problems, eye related diseases are very common as they are watching the screen continuously. Students are not attentive in their studies as their classes are interrupted by the incoming calls to their mobile, family disturbances and they spent time for surfing the internet.

CONCLUSION

This paper presents a statistical analysis on the efficiency of online education in Tamil Nadu during Covid -19. The researchers have collected data using google forms and the data were analyzed using Chi – square and Cramer's V tests. A univariate analysis of College Students' opinion on comparison of classroom teaching with Online Classes was also performed. Analysis of the results disclose that the efficiency of new way of teaching learning process can be improved. As the digital teaching learning process is entirely based on internet, connectivity or bandwidth issues play a major role in the efficiency of virtual classroom. Students are tired of long screening time affected with eye problems, head ache and mental stress. This research explores that the duration of class hours can be reduced or recorded videos can be sent to students and clarifications / discussion should be done to avoid these difficulties. Moreover, it pointed out that the online teaching learning process can be more effective while it is converted as learner centered and also suggested that new methods such as film show, online debate, case study and seminars will make learning more enjoyable and encourages developing new experience of learning.

REFERENCES

1. S.Jayachitra, A.Prasanth, "Multi-Feature Analysis for Automated Brain Stroke Classification Using Weighted Gaussian Naïve Baye's Classifier", *Journal of Circuits, Systems, and Computers*, 2021.
2. F Reimers, A Schleicher, J Saavedra, S Tuominen, "Supporting the continuation of teaching and learning during the COVID-19 Pandemic", *globaled.gse.harvard.edu.*
3. Jorge Larreamendy-Joerns and Gaea Leinhardt, "Going the Distance With Online Education" *Review of Educational Research Winter,* Vol. 76, Issue 4, 2006, pp. 567–605.
4. Joseph Crawford, "COVID-19: 20 countries' higher education intra-period digital pedagogy responses", *Journal of Applied Learning and Teaching,* Vol. 3, Issue 1, 2020, pp. 1-11.
5. Wei Bao, "COVID-19 and online teaching in higher education: A case study of Peking University", *Human Behavior and Emerging Technology,* Vol. 2, Issue 2, 2020, pp. 113-115, https://doi.org/10.1002/hbe2.191
6. Mansureh Kebritchi, Angie Lipschuetz, and Lilia Santiague, "Issues and Challenges for Teaching Successful Online Courses in Higher Education: A Literature Review ", *Journal of Educational Technology Systems,* Vol. 46, Issue 1, 2017, pp.4–29. DOI: 10.1177/0047239516661713
7. Eric Bettinger and Susanna Loeb, "Promises and pitfalls of online education Evidence", *Speaks Reports,* Vol. 2, Issue 15, 2017, pp. 1-4.
8. Muhammad Adnan and Kainat Anwar, "Online learning amid the COVID-19 pandemic: Students' perspectives", *Journal of Pedagogical Sociology and Psychology,* Vol. 2, Issue 1,2020, pp. 45 – 51.
9. Eddie M. Mulenga and José M. Marbán, "Is COVID-19 the Gateway for Digital Learning in Mathematics Education?", *Contemporary Educational Technology,* Vol. 12, Issue 2, pp. 1-11. https://doi.org/10.30935/cedtech/7949
10. Wenjun Cao, Ziwei Fang, Guoqiang Hou, Mei Han, Xinrong Xu, Jiaxin Dong and Jianzhong Zheng, "The psychological impact of the COVID-19 epidemic on college students in China", *Psychiatry Res*, 2020, 287: 112934. https://www.elsevier.com/locate/psychres.2020.112934
11. Julio Torales, "The outbreak of COVID-19 coronavirus and its impact on global mental health", *International Journal of Health Psychiatry,* Vol. 66, issue 4, pp. 317-320.
12. Raman Swathy Vaman, Mathew J. Valamparampil, A.V. Ramdas, A. T. Manoj, Basil Varghese, and Flory Joseph, "A confirmed case of COVID-19 among the first three from Kerala, India", *Indian Journal of Medical Research,* Vol. 151, Issue 5, 2020, pp. 493–494. doi: 10.4103/ijmr.IJMR_2205_20
13. Younis Ahmad Sheikh, "Higher Education in India: Challenges and Opportunities, Journal of Education and Practice", *Journal of Education and Practice,* Vol. 8, Issue 1, 2017, pp. 39-42.
14. Isabel Steinhardt and Christian Schneijderberg, "Mapping the quality assurance of teaching and learning in higher education: the emergence of a specialty?", *High Education,* Vol. 74, Issue 2, 2017, pp. 221–237. DOI 10.1007/s10734-016-00455
15. L. Arockiam A. Jenifer Jothi Mary, S. Santiago, "A
16. Methodological Framework to Identify the Students' Opinion using Aspect based Sentiment Analysis", *International Journal of Engineering and Technical,* Vol. 5, Issue 2, 2016, pp. 642-645.
17. Jenifer Jothi Mary A and Shantha Mary Joshitta, "Aspect Based Sentiment Analysis of Students' Opinion Using Big Data Analytics", *Our Heritage Journal,* Vol. 68, Issue 1, 2020, 8683 – 8693.

18. Mann-Whitney U Test, https://www.sciencedirect.com/topics/biochemistry-genetics-and-molecular-biology/mann-whitney-u-test
19. Kruskal Wallis Test, https://www.sciencedirect.com/topics/medicine-and-dentistry/kruskal-wallis-test

AIP Conference Proceedings

Security analysis of hybrid one time password generation algorithm for IoT data

Cite as: AIP Conference Proceedings **2418**, 030021 (2022); https://doi.org/10.1063/5.0081958
Published Online: 24 May 2022

R. Mary Joshitta Shantha, K. Mahender, A. Jothi Mary Jenifer, et al.

AIP Conference Proceedings **2418**, 030021 (2022); https://doi.org/10.1063/5.0081958 **2418**, 030021

Security Analysis of Hybrid One Time Password Generation Algorithm for IoT Data

Shantha Mary Joshitta R[1, a)], K. Mahender[2], Jenifer Jothi Mary A[3], A. Prasanth[4]

[1]Jayaraj Annapackiam College for Women (Autonomous), Periyakulam, Theni Dt., Tamil Nadu, India
[2]Sumathi Reddy Institute of Technology for Women, Warangal, Telangana, India.
[3]St. Joseph's College (Autonomous), Affiliated to Bharathidasan University, Trichy, Tamil Nadu, India
[4]PSNA College of Engineering and Technology, Dindigul, India

[a)] Corresponding author: rjoshitta@gmail.com

Abstract. The growing reality today is the application of Internet of Things (IoT) in day-to-day. Though there are lot of complexities around this environment such as security, energy consumption and heterogeneity, this giant network of connecting devices with internet is sky rocketing. The mounting increase in the sharing of information made this connected network of devices is mandatory in everyday life. This powerful IoT platform suffers a lot by the security breaches as more people uses it. Authentication of IoT users using One Time Password (OTP) is one kind of resolution to solve many security issues. The OTP has added an additional coating to the traditional username-password authentication system. So, this research proposes a hybrid One-time Password generation algorithm, AroSheb_Jo, for IoT data and presents a security analysis of that algorithm. Additionally, this paper presents a comparison of its lightweight characteristics and resistance against security attacks. Experimental and performance analysis of that algorithm is also elaborated in this paper.

Keywords— Security Analysis, Hybrid One Time Password Generation Algorithm, IoT data, Authentication.

INTRODUCTION

The advent of computers and internet opens new avenues for connecting everything and everyone at all times. Many times, insecure connectivity of these devices raises queries on the protection of the information collected and communicated by these devices which encourages the intruders and compromise the protection of the information. To overcome such issues, a higher-level security algorithm is much needed to avoid access by the unauthorized users. Though, there are several security algorithms available to authenticate the remote users based on traditional password, biometric, etc. with varied efficiencies, One Time Password (OTP) algorithm is another effectual mechanism to offer ample protection of authentication when the remote users login their system. However, it suffers from problems such as high computation cost, delayed OTP delivery, memory usage, secure computation of OTP and security attacks such as impersonation and eavesdropping attacks. So, there is a requirement for better authentication algorithm which considers the heterogeneity of the IoT devices and communication networks [1]. Thus, this research presents a new hybrid OTP generating algorithm, AroSheb_Jo for secure accessing of IoT medical data from the Central Medical Server. Moreover, performance and experimental analysis of that algorithm is also elaborated in this paper. The lightweight features of the algorithm also analysed based on the latency, throughput, parameters area and energy used to implement the algorithm and compared with two more lightweight algorithms.

International Conference on Research in Sciences, Engineering & Technology
AIP Conf. Proc. 2418, 030021-1–030021-10; https://doi.org/10.1063/5.0081958
Published by AIP Publishing. 978-0-7354-4368-6/$30.00

USER AUTHENTICATION TECHNIQUES

As the usage of digital gadgets in the IoT healthcare domain increases, the quantity of data accumulated and stored in the IoT cloud storage also keep on increasing. But unauthorized accessing of these IoT data or modification in these data should be controlled or prohibited [2, 25]. To safeguard the medical users' data, normally, cloud administrators use identification badges, passwords, authentication protocols and security measures. The commonly used authentication techniques are presented below.

Token Based Authentication

This authentication method is the widely used method mostly in smart cards, bank cards and key cards. Many ecommerce systems normally use this technique to improve the security. For example, Credit cards with a PIN number [1].

Biometric Based Authentication

The distinctive biological features of an individual are used for validating the user. Iris scan, fingerprints and facial recognition are few techniques but not yet broadly adopted. The key drawbacks of this approach are cost, slow processing and recurrent unreliability. However, these techniques offer the maximum order of authenticity.

Knowledge Based Authentication

It is the utmost used certification technique. It includes both text-based and picture-based mechanisms. The picture-based methods are subsequently divided into recall-based and recognition-based graphic oriented techniques [3]. In the former, a group of custom pictures are presented to the user and the user is verified by matching the pictures the user has already registered as password while registering [4]. In the latter, a user is expected to reproduce the password or pin that the user had selected during the registration. Widely used authentication measure of securing is data using passwords. There are two types of passwords namely, static passwords and dynamic passwords.

RELATED RESEARCH WORK

Ankita Patil et al., explained an OTP technique to handle the security of cloud user's data [5]. In this research, the encryption was performed by RSA algorithm with the OTP driven using MD5. The OTP was delivered to the user's mobile phone and the user shared the public data with authenticated cloud users only. Security was achieved by bi-directional cloud framework.

Ioannis Tzemos et al., presented a comparison of OTP approaches to minimize non-authenticated access in sensitive IoT data [6]. In the Existing N/R OTP schemes, the OTP was generated by the stream cipher with random digit and the IoT user validation based on encrypted OTP were compared. It was indicated that adding new security parameters to boost up attack resistance had an impact on the computational competence of the IoT healthcare system.

Longyan Gong et al., presented an OTP based authentication method using challenge / response algorithm. The random sub-passwords and their corresponding hashes were made open between server and user [7]. Modular algebraic procedures were executed on selected sub-passwords and independent OTPs were formed from it.

Priyanka Patel et al., explained an OTP based logging system to authenticate a cloud computing environment [8]. It combined Langrage's Interpolation-based OTP with MD5 hash algorithm. It offered high computational complexity and higher level of security. OTPs were generated using MD5 hash algorithm and AES encryption technique. Experimental analysis was also performed and discussed.

Shivraj V L et al., studied another certification scheme for IoT devices [9]. The authors projected an OTP scheme which used Lamport's OTP algorithm and lightweight ECC scheme to produce OTP. The working process of the scheme was assessed experimentally. It executed well with the existing OTP schemes without negotiating security. The authors suggested it as the precise contender for two-factor validation in IoT domain.

Sang-Ho Lee et al., presented an authentication scheme for the IoT ecosystem based on joint probability mechanism [10]. The user information was shared secretly among various IoT services. In the transmission and reception processes of information system in the IoT environment and random variables were allocated to critical information to improve the security. Information accessibility of users was interrelated through joint probability of the random variables. The performance of the scheme was calculated and improved the process time by 7.8%, security strength by 5.2% and lowered the server overhead by 3.5%.

Hou J. L. et al., proposed a communication architecture based on sensors for future IoT healthcare systems [11]. The architecture used a co-existence proof scheme for authenticating devices of IoT healthcare systems. For ensuring competence of the proposed protocol, a singular token was sent to contact manifold services and random nonce was adopted. The accuracy of the coexisting items was enhanced by the projected coexistence mechanism. The toughness of the two schemes was surefire with proper security analysis under the adversary model.

Fan W. et al., presented another validation scheme for Wireless Sensor Networks [12]. An arbitrary oracle model was hired to deliver the formal proof and use a scheme analysing tool to enlist the verification process. Many other authentication schemes for WSNs were also studied and compared. The common security attack such as insider, and gateway forgery were overcome by the proposed scheme and the experimental analysis proved the security parameters of the scheme for IoT environment.

METHODOLOGY OF THE HYBRID OTP GENERATION ALGORITHM

The proposed hybrid OTP generating algorithm is used to authenticate the remote users of the IoT environment while accessing the medical data from the Cloud Medical Server (CMS). A remote user can use a Smart phone, Tablet, Laptop and Desktop to access the data from the CMS. Here, the user tries to access the data from CMS by a device from anywhere at any time. This scenario is depicted in Figure. 1.

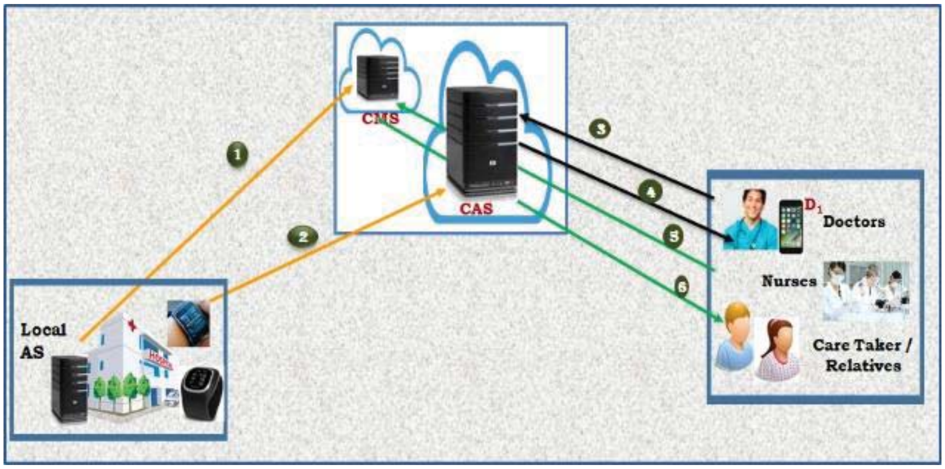


FIGURE 1. Methodology of Hybrid One Time Password Generation Algorithm [13]

A medical user, using the device (D1), would like to access data from CMS of another gateway. So, D1 sends a request to the Cloud Authentication Server (CAS) using its device identity (IMEI / EPC / IP / Mobile Number). The CAS generates the OTP using the proposed hybrid OTP generating algorithm by taking EPC / IMEI / IP/ Mobile Number of D1, the time stamp t in which the request is received by the CAS, a counter value c and the message m sent by the D1 as its inputs. It sends the OTP to the CMS and the user device for further authentication by the CMS before accessing the medical data. The user resubmits the OTP to the CMS for authenticating it for accessing the medical data securely.

THE HYBRID OTP GENERATION ALGORITHM

TABLE 1. The hybrid AroSheb_Jo OTP generation is represented below.

	Procedure AroSheb_Jo [13]
	Input: EPC / IMEI / IP/ Mobile Number of the device, the time stamp **t,** counter value **c** and the message **m** **Process:** OTP generation using hybrid algorithm **Output:** An OTP to authenticating user device
Step 1.	*Start*
Step 2.	*Medical device saves Authentication details in CAS*
Step 3.	*Medical device saves medical data in CMS*
Step 4.	*User request for data from CAS from a device*
Step 5.	*CAS generates OTP using SHA-256 and JAC_Jo [14] and sends it to the User device*
Step 6.	*User resubmits the OTP to CMS and request data*
Step 7.	*If OTP matches, it permits the user to access the data*
Step 8.	*Stop*

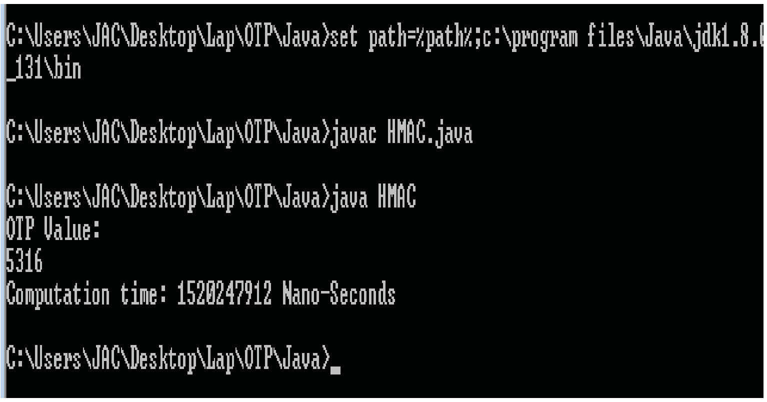
RESULTS AND ANALYSIS

The lightweight OTP generation Algorithm AroSheb_Jo is evaluated on the basis of perform time of the OTP generation operations. The time to compute the OTP using encryption and decryption operation is calculated using a JAVA 6 program. The developed program is deployed in a server, a desktop and an Android Galaxy Tab A whose configuration is specified in Table 1. The experimental setup has two different set of connections. One is Server to Client communication using modem / router on server side with manual configuration and the other is communication between Server to Tablet using Terminal IDE on the Android Tab. Variable OTP generation requests are made to verify the computation and communication time required to generate OTP at the server.

TABLE 2. Setup of Arosheb_Jo Algorithm

Environment	Server, Desktop, Android Galaxy Tab A
Server	Intel Core i7-1035G1 CPU@3.6 Ghz
Server Memory	8 GB RAM
Server OS	Windows 10 Ultimate, 64 bit
Android Galaxy Tab A	Android 6.0.1

Java program for the generation of OTP is implemented as shown in Figure. 2. The Java program calculates the execution time taken to generate the OTP in nano-seconds. The OTP is generated by applying a random function on the digest generated by the HMAC functions using SHA-256 and JAC_Jo encryption algorithm.



```
C:\Users\JAC\Desktop\Lap\OTP\Java>set path=%path%;c:\program files\Java\jdk1.8.0
_131\bin

C:\Users\JAC\Desktop\Lap\OTP\Java>javac HMAC.java

C:\Users\JAC\Desktop\Lap\OTP\Java>java HMAC
OTP Value:
5316
Computation time: 1520247912 Nano-Seconds

C:\Users\JAC\Desktop\Lap\OTP\Java>_
```

FIGURE 2. OTP generation with Computation Time

Time to compute the OTP of different sizes such as 32, 64,128 and so on is calculated for the L. Gong's Scheme, Shivraj's IBE ECC OTP generation algorithm and the proposed AroSheb_Jo. The analysis result is presented in Figure. 3.

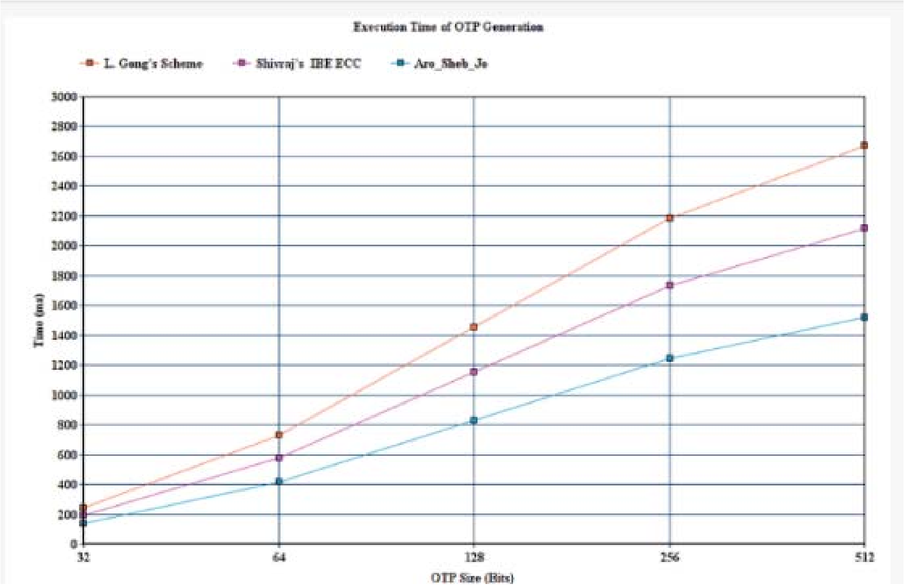


FIGURE 3. Execution Time of OTP Generation Operation

Even though, computing time of the OTP does not have much variance with lower bits, but it makes substantial variance in 512-bits. This change will rise if the message size is high [15]. The efficiency of the proposed algorithm was conducted in a system with 8GB RAM and 3.6 Ghz processor and the time taken for key generation, encryption and decryption is presented in Table 2. Comparison of the execution time of the AroSheb_Jo OTP generation algorithm with varying message sizes is depicted in Figure. 4. Though, there is not much difference in time taken for key generation and encryption operation, there is little variance in the decryption operation.

Performance evaluation of the proposed AroSheb_Jo OTP Algorithm in an Android Galaxy Tab and a Cloud Server with different size of the OTP is presented schemes in Figure. 5. From the Figure.5, it is proved that the proposed OTP algorithm takes less time to generate OTP than the other already existing OTP.

TABLE 3. Efficiency of Arosheb_Jo OTP Algorithm with Different Message Sizes

Message Size (Bits)	Time Taken for (ms)		
	Key Generation	Encryption	Decryption
1k	22.328	22.7812	23.706
2k	21.131	21.213	22.137
3k	20.019	19.674	20.097
4k	18.73	18.832	19.756
5k	19.217	19.012	19.036
6k	16.732	17.234	18.158
7k	17.081	16.67	17.594
8k	15.509	15.008	15.932
9k	14.38	13.93	13.973
10k	12.022	12.045	12.969

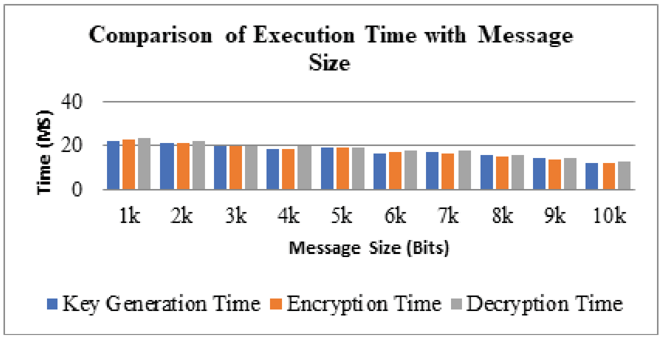


FIGURE 4. Comparison of Execution Time with Message Size

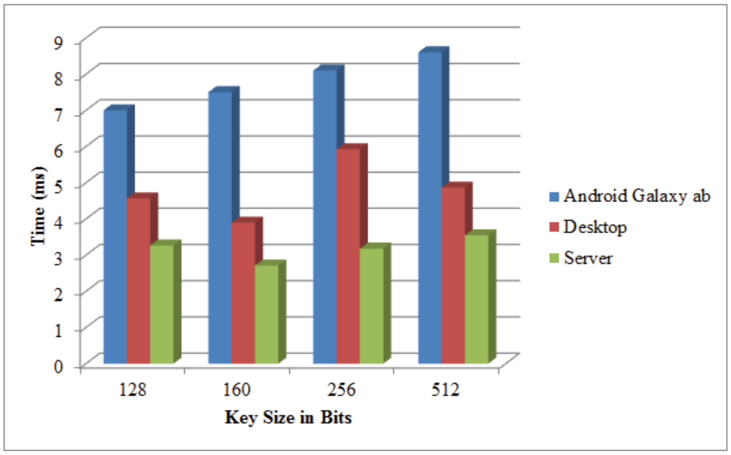


FIGURE 5. Performance of the AroSheb_Jo Algorithm on Different Devices

The computation time of the OTP for various sizes is taken into consideration and the computation time is calculated. It shows that the computational difficulty increases along with the size of the OTP. The higher OTP size needs more execution time than less OTP sizes. So, the proposed hybrid OTP algorithm, AroSheb_Jo performs well when it is deployed in Cloud Authentication Server rather than any energy constrained devices.

Performance of AroSheb_Jo OTP algorithm is evaluated with other hash based OTP generating algorithms L. Gong's Scheme [7] and Shivraj's IBE ECC OTP generation algorithm [9] and the results are presented in Table 3. Successive 1000 OTPs are produced and the time taken to generate the 1000th OTP is calculated. Though, the proposed algorithm, AroSheb_Jo is compared with different OTP algorithms, it provides better result and higher order security when hybridization is used.

TABLE 4. Performance of Arosheb_Jo with Other OTP Algorithms

Message Size (Bits)	Time Taken to generate OTP by difference OTP Algorithms (Sec.)		
	L. Gong's Scheme	**Shivraj's IBE ECC**	**AroSheb_Jo**
2k	2.09	1.87	1.52
4k	4.18	3.74	3.04
6k	8.36	7.48	6.08
8k	16.72	14.96	12.16
10k	33.44	29.92	24.32

The experimental results of the comparison of the time taken to generate OTP by different OTP Algorithms are presented in Figure. 6.

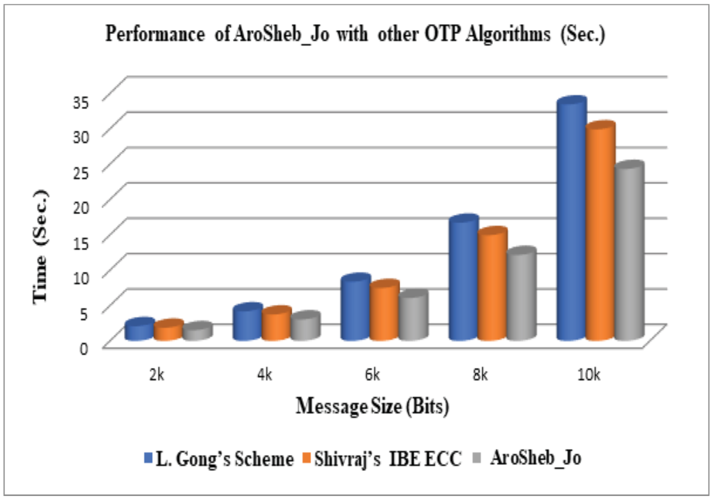


FIGURE 6. Comparison of AroSheb_Jo with other OTP Algorithms

As hybridization of JAC_Jo with SHA 256 is used in the proposed algorithm, the attacker may find difficult to guess the hash functions used, thus, provides less computational complexity. So, it is good to use the proposed AroSheb_Jo algorithm to authenticate resource constrained devices while accessing IoT data from healthcare environment.

SECURITY ANALYSIS OF AROSHEB_JO

The mathematical proof for the freshness and un-correlation of the OTPs generated by the proposed hybrid OTP algorithm are presented in this section. Freshness characteristic of OTP expresses that the generated OTP is new and fresh. The OTP once generated and used will no longer be available for any other authentication purpose. The un-correlation of OTPs states that the generated consecutive OTPs are not associated with each other. It is hard to find a correlation relationship between two or many OTPs generated.

Freshness of The OTPs

To prove the freshness of OTP, the correlations between OTPs generated by the hybrid OTP generating algorithm are tested using the scheme suggested by L. Gong et al., [7]., computed almost random OTPs from the tens of random sub-passwords generated by their proposed scheme. The same literature is used to verify the freshness of the OTP. Let the OTP generated out of the one-way hash function be OTP$^{s}_{n}$ which is equal to$\{C_n^1, C_n^2, C_n^3, \ldots.., C_n^l\}$. It is made up of digits (10) and characters (26). In practice, the length L of an OTP is 4 to 6 digits. i.e. L ∈ [4,6]. Based on the length, OTP is randomly chosen from all n characters.

Now, suppose OTP$^{o}_{t}$=$(C_t^1, C_t^2, \ldots., C_t^l, \ldots., C_t^L)$is the OTP produced at tth time, where t = 1, 2, . . . , T and also, C_t^l∈ {0,1,2 ....., 9, a,b, ..., z}. Therefore, the number of possible characters is 36. The probability distribution function for all P$^{o}_{t}$ is P(C$_b$, C$_a$). [7].Assume that, C$^{l}_{t}$ = C$_a$ and C$^{l}_{t+1}$ = C$_b$ for all T OTPs. The probability of occurrence of an OTP can be calculated by P(C$^{l}_{t+1}$ = C$_b$, C$^{l}_{t}$ = C$_a$). The probability distribution function in accordance to Bayes theorem can be given as depicted in equ (1)

$$P(C_b, C_a) = \frac{P(C_{t+1}^l = C_b, C_t^l = C_a)}{\sum_{C_a^i C_b^l} P(C_{t+1}^l = C_b, C_t^l = C_a)} \qquad (1)$$

Now the length L = 4 and T = 10^{6} can be checked for the above equation. If the OTP generation is completely random, then, for infinite OTPs, according to [7], the probability of getting a character consecutively is given by,

$$P(C_b, C_a) = \frac{1}{1296} \qquad (2)$$

Now the length L = 6 and T = 10^{6} can be checked for the above equation. If the OTP generation is completely random, then, for infinite OTPs, the probability of getting a character consecutively is given by,

$$\begin{matrix} P(C_b,\ C_a) \\ 1 \end{matrix} \qquad (3)$$

But in the proposed OTP algorithm, the counter will be reset after every 1000 hits. So, there is no chance of getting two consecutive OTPs. Thus, the freshness of OTP is proved.

Un-Correlation of The OTPs

In mathematical calculations, a set of characters say,$\{0,1,2, \ldots, 9, a, b, c, \ldots, z\}$is charted to a set of values$\{\frac{1}{36}, \frac{2}{36}, \ldots, \frac{36}{36}\}$. If the correlation function $C(\Delta t)$ for everyt^{th} OTP, P_t^0generated by the server is defined by,

$$C(\Delta t) = \langle C_t^l C_{t+\Delta t}^l \rangle - \langle (C_t^l)^2 \rangle \qquad (4)$$

Where, the braces denotes the average over for all possible t. $C(\Delta t)$ is trivial and approaches zero for allΔt.Therefore, the OTPs are uncorrelated [21].

Moreover, in the proposed OTP algorithm, the size of the OTP is 4 or 6 which is randomly generated with very less computation time. It is not generated using truncation as done in literature [7]. So, the chances of incurring collision between OTPs are avoided.

Uniqueness of The OTPs

The interpolating polynomial $I(a)$ in (1) can be written as follows.

$$I(a) = \frac{\varphi(a){a_0}^c}{(a-a_0)\varphi'(a_0)} + \frac{\varphi(a){a_1}^c}{(a-a_1)\varphi'(a_1)} + \ldots + \frac{\varphi(a){a_n}^c}{(a-a_n)\varphi'(a_n)}$$

(5)

Where, $\varphi(a) = (a - a_0)(a - a_1)(a - a_2)\ldots(a - a_n)$ and $\varphi'(a) = \frac{d}{dx}[(a - a_0)(a - a_1)(a - a_2) \ldots..(a - a_n)]$. $\therefore I(a) = \varphi(a)[\frac{{a_0}^c}{(a-a_0)\varphi'(a_0)} + \frac{{a_1}^c}{(a-a_1)\varphi'(a_1)} + \ldots + \frac{{a_n}^c}{(a-a_n)\varphi'(a_n)}]$

(6)

As $c$varies over the set of natural numbers $\{1,2,3, \ldots\}$, different polynomials for fixed values $a_0, a_1, a_2, \ldots, a_n$ are derived.

If we denote the polynomial corresponding to a particular$c$, by $I(a)_{/_c}$then for any two values of c, say l and $m$where $l \neq m, I(a)_{/_l}$ is not equal to $I(a)_{/_m}$. For,

$$I(a)_{/l} = \varphi(a)[\frac{{a_0}^l}{(a-a_0)\varphi'(a_0)} + \frac{{a_1}^l}{(a-a_1)\varphi'(a_1)} + \ldots + \frac{{a_n}^l}{(a-a_n)\varphi'(a_n)}]$$

(7)

and

$$I(a)_{/m} = \varphi(a)[\frac{a_0{}^m}{(a-a_0)\varphi'(a_0)} + \frac{a_1{}^m}{(a-a_1)\varphi'(a_1)} + \ldots + \frac{a_n{}^m}{(a-a_n)\varphi'(a_n)}]$$

(8)

The polynomials in (7) and (8) are equal if and only if $\frac{a_k{}^l}{(a-a_k)\varphi'(a_k)} = \frac{a_k{}^m}{(a-a_k)\varphi'(a_k)}$ for all $k = 0,1,2,\ldots n$. That is, if and only if $a_k{}^l = a_k{}^m$ for all $k = 0,1,2,\ldots n$. This is impossible, because $l \neq m$.

Thus, the uniqueness of OTP is proved.

CONCLUSION

This paper presents the security analysis of AroSheb_Jo, a hybrid OTP algorithm for authentication of data in IoT environment. The analysis reveal that the hybrid OTP algorithm is protected against various attacks. Additionally, performance evaluations between the hybrid OTP algorithm and related two more algorithms disclose that the OTP algorithm outpaces the previous algorithms with regard to execution time, security features and communication overhead. Due to these attributes, the proposed hybrid One Time Password algorithm offers a realistic solution for real-world use in IoT environment.

REFERENCES

1. Dr. K. Mohan Kumar and G. Bala Murugan, “Comparative Study on One Time Password Algorithms”, *International Journal of Computer Science and Mobile Computing*, Vol. 7, No. 8, pp. 37-52, 2018.
2. A.Prasanth, S.Jayachitra, “A Novel Multi-Objective Optimization Strategy for Enhancing Quality of Service in IoT enabled WSN Applications”, *Peer-to-Peer Networking and Applications*, Vol.13,pp.1905–1920, 2020.
3. Jeyanthi N and Sourav Kundu,” Backup key generation model for one-time password security protocol” *IOP Conf. Series: Materials Science and Engineering,* Vol. 263, 2017.
4. A.Prasanth, S.Pavalarajan “Particle Swarm Optimization Algorithm Based Zone Head Selection in Wireless Sensor Networks”, *International Journal of Scientific & Technology Research*, Vol.8, pp.1594-1597, 2019.
5. Ankita Patil, Kiran Zambare, Preeti Yadav, Pankaj Wasulkar and Nisha Kimmatkar, “Secure File Access Using MD5 for One Time Password Generation on Cloud”, *International Journal of Emerging Trend in Engineering and Basic Sciences*, Vol. 2, No. 1, ISSN: 2349–6967, pp. 345-348, 2015.
6. Ioannis Tzemos, Apostolos P. Fournaris and Nicolas Sklavos, “Security and Efficiency Analysis of One Time Password Techniques”, *In the proc. of the Pan-Hellenic Conference on Informatics,* pp. 1-5, 2016. DOI: 10.1145/3003733.3003791.
7. Longyan Gong, Jingxin Pan, Beibei Liu and Shengmei Zhao, “A novel One Time Password mutual authentication scheme on sharing renewed finite random sub-passwords”, *Journal of Computer and System Sciences,* Vol. 79, No. 1, pp. 122–130, 2013. DOI: 10.1016/j.jcss.2012.06.002.
8. Priyanka Patel and Nirmal D, “Access Control for Cloud Computing Through Secure OTP Logging as Services”, *International Journal of Computer Applications*, Vol. 141, No. 14, pp. 1-5, 2016, ISSN: 0975 – 8887.
9. Shivraj V L, Rajan M A, Meena Singh and Balamuralidhar P, “One Time Password Authentication Scheme based on Elliptic Curves for Internet of Things (IoT)”, *In the proc. of the 5th IEEE National Symposium on Information Technology: Towards New Smart World*, ISBN: 978-1-4799-7626-3, pp. 1-6, 2015. DOI: 10.1109/NSITNSW.2015.7176384.
10. Sang-Ho Lee and Yoon-Su Jeong, “Information Authentication Selection Scheme of IoT Devices using Conditional Probability”, *Indian Journal of Science and Technology,* Vol. 9, No. 24, pp. 1-7, 2016. DOI: 10.17485/ijst/2016/v9i24/95991.
11. Hou Jia-Li and Kuo-Hui Yeh, “Novel Authentication Schemes for IoT Based Healthcare Systems”, *International Journal of Distributed Sensor Networks,* Vol. 2015, Article ID e183659, pp. 1-15, 2015. DOI: 10.1155/2015/183659.

12. Fan Wu, Lili Xu, Saru Kumari and Xiong Li, “A privacy-preserving and provable user authentication scheme for Wireless Sensor Networks based on Internet of Things security”, *Journal of Ambient Intelligence and Humanized Computing,* Vol. 8, No. 1, pp. 101–116, 2016. DOI: 10.1007/s12652-016-0345-8.
13. Shantha Mary Joshitta R and Arockiam L, “Secure Two-Tier User Authentication Mechanism for IoT Enabled Smart Healthcare System”, *International Journal of Recent Science Research*, Vol. 8, No. 7, pp. 18259-18263. DOI: http://dx.doi.org/10.24327/ijrsr.2017.0807.0478
14. R Shantha Mary Joshitta, L Arockiam, “A Novel Block Cipher for enhancing data security in healthcare Internet of Things”, *Journal of Physics,* Vol. 1142, 2018. https://doi.org/10.1088/1742-6596/1142/1/012002
15. R. Shantha Mary Joshitta, L Arockiam and P. D. Sheba Kezia Malarchelvi, “Security Analysis of SAT_Jo Lightweight Block Cipher for Data Security in Healthcare IoT”, *Proceedings of the 3rd International Conference on Cloud and Big Data Computing,* pp. 111–116, 2019. https://doi.org/10.1145/3358505.3358527
16. Deepti Sehrawat and Nasib Singh Gill, “Lightweight Block Ciphers for IoT based applications: A Review”, *International Journal of Applied Engineering Research,* ISSN 0973-4562, Vol. 13, Number 5, pp. 2258-2270, 2018.
17. ULur Coruh and OLuz Bayat, “Hybrid Secure Authentication and Key Exchange Scheme for M2M Home Networks”, *Hindawi Security and Communication Networks*, Vol. 2018, Article ID 6563089, pp. 1-25. https://doi.org/10.1155/2018/6563089
18. Sherin Peter and Raju K. Gopal, “Secure Authentication Schemes in IoT Environments”, *International Journal of Advanced Research,* Vol. 4, No. 8, pp. 10-22, 2016. ISSN: 2320-5407.
19. MA, Siqi, Feng, Runhan, LI, Juanru, LIU, Yang, Nepal, Surya, Bertino, Elisa, Deng, Robert H., MA, Zhuo and Jha, Sanjay, “An empirical study of SMS one-time password authentication in Android apps”, *Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC 2019),* pp. 339-354.
20. Jaeho Lee, Ang Chen and Dan S Wallach, “Total Recall: Persistence of Passwords in Android”, *In Proceedings of The Network and Distributed System Security Symposium (NDSS),* 2019.
21. Ming Fan et. al, “Android malware familial classification and representative sample selection via frequent subgraph analysis”, *IEEE Transactions on Information Forensics and Security,* Vol. 13, No. 8, pp.1890–1905, 2018.
22. I. Velásquez, A Caro and A Rodríguez, “Authentication schemes and methods: A systematic literature review”, *Int. Journal of Information and Software Tech.,* Vol. 94, 2018, pp. 30–37.
23. P Laka and W Mazurczyk, “User perspective and security of a new mobile authentication method”, *Journal of Telecommunication Systems,* Vol. 69, No. 3, 2018, pp. 365–379.
24. A.Prasanth, S.Pavalarajan, “Zone-Based Sink Mobility in Wireless Sensor Networks”, *Sensor Review*, Vol.39, pp.874–880, 2019.
25. A.Prasanth, “Certain Investigations on Energy-Efficient Fault Detection and Recovery Management in Underwater Wireless Sensor Networks”, *Journal of Circuits, Systems, and Computers*, Vol. 30, 2020

PRESIDENCY UNIVERSITY

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

Private University Estd. In Karnataka State by Act No. 41 of 2013
Established Under Section 2(f) of UGC Act, 1956
Approved by AICTE, New Delhi.

PRESIDENCY GROUP
OVER
40
YEARS
OF ACADEMIC
WISDOM

SCHOOL OF ENGINEERING

DEPARTMENT OF MATHEMATICS

CERTIFICATE OF PARTICIPATION

This is to certify that Prof./Dr./Mr./Ms./ **Dr. A. Jenifer Jothi Mary, Assistant Professor in CS** from **St. Joseph's College (Autonomous), Trichy** has participated in the **"Five Days Online Faculty Development Programme"** on **"Scientific Application Packages for State-of-the-Art Technical Computing"** organized by Department of Mathematics, School of Engineering, Presidency University, Bengaluru - 560 064, Karnataka State, India from 14 March 2022 to 18 March 2022.

S. Mat

Dr S Maruthamanikandan
HOD, Dept. of Mathematics

Dr Abdul Sharief
Dean, SOE

Dr Shrishail B Anadinni
Associate Dean, SOE

Sairam INSTITUTIONS

DEPARTMENT OF
COMPUTER SCIENCE &
ENGINEERING

CERTIFICATE OF PARTICIPATION

Sri
SAI RAM
ENGINEERING COLLEGE
An Autonomous Institution
West Tambaram, Chennai - 44
www.sairam.edu.in

This is to certify that

Mr/Ms. **Dr. A. Jenifer Jothi Mary**

of **St. Joseph's College (Autonomous), Tiruchirappalli.**

has participated in the ISTE and CSI Sponsored Five Days Virtual Faculty development Program (FDP) on **“Insights and Open Challenges in Computing Technologies”** held from 11.07.2022 to 15.07.2022.

Dr.K.Latha Co-ordinator	**Ms.A.Sheela** Co-ordinator	**Ms.S.Hemavathi** Co-ordinator	**Dr.B.Latha** Convenor & HOD/CSE	**Dr.K.Porkumaran** Principal Sri Sairam Engineering College	**Sai Prakash LeoMuthu** Chairman & CEO Sairam Institution

Sairam RAISE Sairam EOMS ARIIA TOP 25 RANKING INSTITUTION nirf 109 RANK INSTITUTION'S INNOVATION COUNCIL SUSTAINABLE DEVELOPMENT GOALS

The Institution of Electronics and Telecommunication Engineers

Hyderabad Centre

CERTIFICATE

OF PARTICIPATION

This is to certify that

Dr. A. Jenifer Jothi Mary

has participated in the **IETE Knowledge Sharing Session (KSS) – 74 : Webinar - 106** on **“RESEARCH METHODOLOGY”** September, 2022.

Asangamker

Sri Ashwani Kumar Sangamker
Honorary Secretary

www.ietehyd.org

Er. Nuli Namassivaya
Chairman

Internal Quality Assurance Cell

ST. JOSEPH'S COLLEGE (AUTONOMOUS)

College with Potential for Excellence by UGC
Accredited at A^{++} Grade (Cycle IV) by NAAC
Tiruchirappalli - 620 002

Certificate of Appreciation

This is to certify that

Dr. A. Jenifer Jothi Mary

Assistant Professor of Computer Science

has contributed as Resource Person for the One Day Workshop on **ICT Tools** for the Non-Teaching Staff of the college on 20.02.2023.

Dr A. ROSE VENIS
Dean - IQAC

Rev. Dr M. AROCKIASAMY XAVIER SJ
Principal