Secured Cloud Application Platform Using Elliptic Curve Cryptography

Alowolodu Olufunso Dayo, Alese Boniface Kayode, Adetunmbi Olusola Adebayo, *Member, IAENG*

Abstract— **Computing applications and data are growing so quickly that increasingly larger servers and disks are needed to process them fast enough within the required time period, which brought about the concept of Cloud Computing. Cloud Computing was introduced as a result of unfriendly environment created by Data Centers due to carbon emissions in addition to huge maintenance costs. Although, the major aim of the Cloud is for storage of data, attention has now shifted from that to the security of data in the Cloud. One of the ways by which data in the Cloud could be secured is cryptography. Elliptic Curve Cryptography which is a public key cryptographic scheme is employed in this work because of the smaller key size. This makes it suitable in a situation where resources like processing power, storage space, bandwidth and power consumption is limited.**

***Index Terms*—Cloud Computing, Elliptic Curve, Cryptograpky, Application.**

I. INTRODUCTION

Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications which allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access [6]. This is envisioned to achieve not only efficient processing and utilization of computing infrastructure, but also minimizes energy consumption and is being adopted today as the latest in the world of Computing technology. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth utilization. Cloud Computing utilizes massive scalable computing resources delivered as a service using Internet technologies.

However, despite the fact that the Cloud is offering a better solution to all and sundry in the sense of scalability, flexibility , availability and so on, people are still skeptical of relinquishing their data to either a second or third party depending on their choice of provider or how they want to go about their data storage. To put their mind at rest, a solution in the form of Elliptic Curve Cryptography (ECC) to model a secure Cloud application is hereby developed. Whichever data to be deployed, ECC which is one of the fastest, robust and smaller key required form of Cryptography can be used.

Manuscript received June 30, 2016; revised July 17, 2016.

This work was supported in part by Nigerian Government under Tetfund Research Grant.

O. D. Alowolodu is with Computer Science Department, Federal University of Technology, P.M.B. 704, Akure.; e-mail: odalowolodu@ futa.edu.ng

B. K. Alese is with Computer Science Department, Federal University of Technology, P.M.B. 704, Akure.; e-mail: bkalese@ futa.edu.ng

O. A. Adetunmbi is with Computer Science Department, Federal University of Technology, P.M.B. 704, Akure.; e-mail: oaadetunmbi@ futa.edu.ng

II. THE ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. '

For current cryptographic purposes, an Elliptic Curve is a plane curve which consists of the points satisfying the equation:

$$y^2 = x^3 + ax = b \dots\dots\dots\dots\dots eqn\ 1$$

along with a distinguished point at infinity.

The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated.) This set together with the group operation of the elliptic group theory form an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety. To make operations on Elliptic Curve accurate and more efficient, the curve is defined over two finite fields.

a. Prime field Fp and

b. Binary field $\mathbb{F}_2{}^m$

How it works depends on the cryptographic scheme it is applied to. As an example, it can be applied to the Diffie-Hellman key exchange, which is commonly known as the Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol.

A. The Justification For ECC

Elliptic Curve Cryptography being a family of Public Key Cryptography has some criteria that was put into consideration before it was selected as the method of choice.

According to [3], the three main criteria that must be considered are:

Functionality: Does the public-key family provide the

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

desired capabilities?

Security: What assurances are available that the protocols are secure?

Performance: For the desired level of security, the protocols meet the performance

d) Key Size: ECC offers the same amount of security with a shorter key than its non-ECC counterpart. For example, typical guidelines suggest 160-bit keys in ECDH provide the same level of security as 1024-bit keys in regular Diffie-Hellmann Algorithm.

The table below shows the differences in key sizes of RSA and ECC under the same security condition.

Table 1. Different key sizes of RSA and ECC

RSA Key Size (in bits)	ECC key size (in bits)
1024	160
2048	224
3072	256
7680	384
15360	512

[4]

B. RELATED WORKS

[8] Compared two Public Key Cryptographic algorithms and their variants in generating certificate that is exchanged in a network. It was discovered that Elliptic Curve based systems can give better security compared to RSA with less key size. This study compares the performance of ECC based signature schemes and RSA schemes using NS2 simulation. It was observed that ECC based certificate authority schemes gives better speed and security. In their conclusion, Elliptic Curve based schemes are the best for time and resource constrained wireless applications.

[2] worked on the use of ECC as an efficient approach for encryption and decryption of a data sequence. The work illustrated the procedure of encryption and decryption of messages by first transforming the message into an affine point on the curve (EC) over the prime finite field $GF(P)$. The affine point is known as $Pm(x, y)$ which lies on the curve (EC). The implementation was done using text messages. A comparison was performed between the encrypted message using different key sizes to calculate the time taken for encryption and decryption. The work further went on to ascertain the fact that the strength of ECC lies in the infeasibility of solving the ECDLP. It also stated that the application areas of ECC in constrained environments because of the smaller key sizes required which can lead to faster execution timing for the schemes. This is discovered to be beneficial to systems where real time performances are critical factors. Although, the work stated that not all curves are used for cryptographic operations and for implementing cryptosystems. To choose the appropriate elliptic curve is a difficult task.

[1] proposed ECC for Cloud Computing applications. In this work, it was opined that several attempts had been made at providing a secured environment for activities in the Cloud, but Elliptic Curve Cryptography (ECC) can provide solutions for a secured Cloud environment with improved performance in computing power and battery resource usage. This will make it attractive for mobile applications.

Also, [7] implemented Elliptic Curve on a low Digital Signal Processor, it was ascertained that ECC is more effective in hand held devices and even suggested the possibility of implementing it on smart cards. This is because ECC was compared with RSA and discovered that due to the varying key sizes, and that ECC utilizes smaller key sizes than RSA.

[5] argued and proved that the attraction of ECC compared to RSA is that it offers equal security for a smaller key-size thereby reducing the processing overhead. The work was proposed over a finite field. It was proved using two entities Alice and Bob.

The random number used in the encryption of each message point is different from encryption of different message point. That is why the same characters in the message space are encrypted to different characters in the cipher space. The difference between characters of the plaintext is not the same as the difference between characters of the cipher-text. Due to this, the linear cryptanalysis is highly difficult. Also each character of the message is coded to the point on the elliptic curve using the code table which is agreed upon by the two communicating parties and each message point is encrypted to a pair of points on the elliptic curve. Hence the method of encryption proposed provides sufficient security against crypt-analysis at relatively low computational overhead.

III. SYSTEM ARCHITECTURE

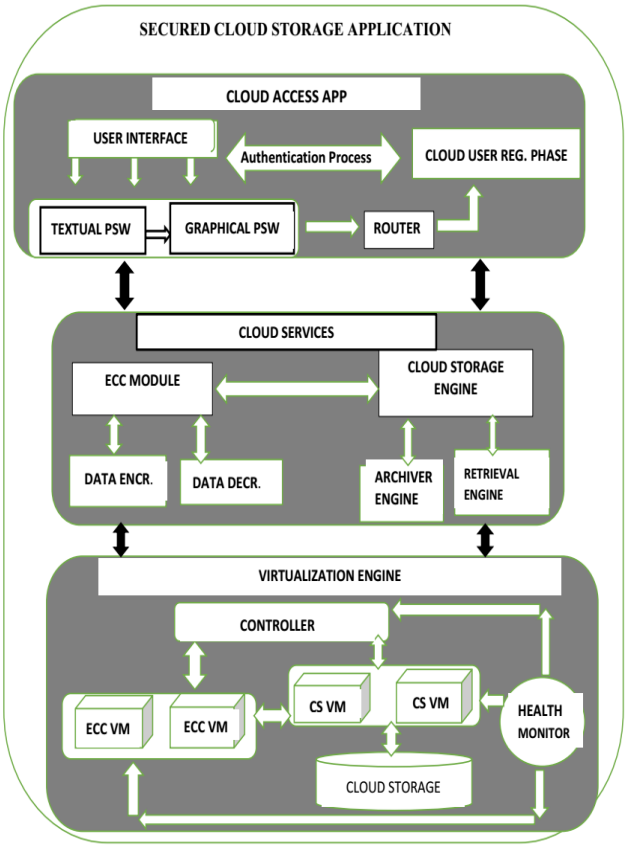

Figure 1. The Overall System Architecture.

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

The system architecture as depicted figure 1 is a three-layered architecture. The first layer consists of the user-interface where authentication and authorization take place. A username, a textual password followed by a graphical password are the needed user's inputs for access to the system. The graphical password employs the use of image positioning system which may be a user preset picture. In an attempt to mitigate password phishing, the image positioning is dynamically shuffled with every user login attempt. If the user is not a registered user, the system will route to the logon page where the new user will register.

The second layer is the Cloud service layer. Operations which take place in this layer include: encryption; decryption; archiving; and retrieval of data. However, user may decide not to encrypt data and just directly access the Cloud storage engine.

The third layer is the virtualization engine which portrays the virtualization characteristics of the Cloud. The Cloud Controller is responsible for directing all elements of the systems. If encryption takes place, the ECC virtual machines are activated for data encryption and decryption. Otherwise, the Cloud virtual machines are activated directly. Directly attached to the Cloud Controller is the health monitor. This majorly monitors the virtual machines and sends signal to the Cloud Controller when any one malfunctions. The controller responds by scheduling any available virtual machine(s) for the waiting jobs.

A. Secured Cloud Storage Application (SCSA)

The Secured Cloud Storage Application houses encrypted data or files. The design has an authentication page to prevent unauthorized access to stored data. Notwithstanding, the prospects of an unauthorised access to information by an intruder is dimmed due to file encryption. An access control list highlights the multi tenancy characteristics of the Cloud. This is achieved with the virtualization technology. A set of operations including Create, Delete, Update, Retrieve or Download can be used to manage resources. Storage can be delivered on demand based on request for a given quality of service. There is no need to purchase storage or in some cases provision it before storing data. It is a pay-as-you-go service.

B. Access to the Cloud.

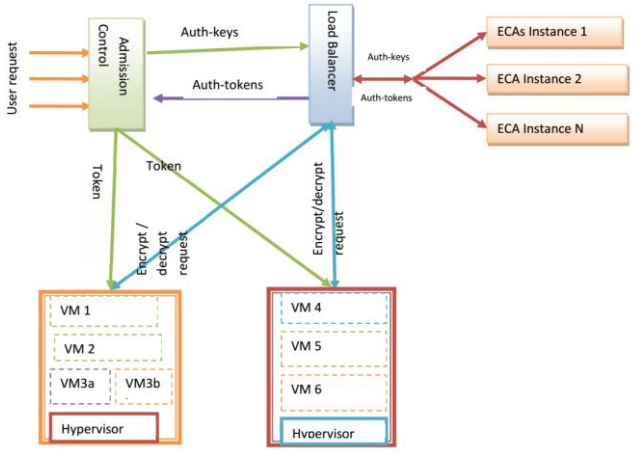

Figure 2. Flow of information in the Secured Cloud.

Datacenters are typically made up of thousands of servers. As instances of users' requests are being sent from various locations into the Cloud, two major concepts are applicable:

a) A set of dedicated virtual machines are provided solely for the ECC service which will automatically eliminate any potential performance interference which each application deployed in the hypervisors (VM1, VM2) may encounter.

b) Taking the advantage of resource elasticity inherent in the Cloud environments. Increase in load as there are more applications and in turn users can be handled by increasing the number of Elliptic Curve Admission (ECAs) instances to the Cloud by the controllers to avoid deadlocks.

(i) Admission Control — accepts requests from application users, performs authentication and generating authentication keys through the ECDH algorithm. This is forwarded to the load balancer of the ECAs services, it receives auth-tokens in return and then connect users to the respective application service running in either of the two nodes in the Data Centers.

(ii) Load Balancer — The load balancer distributes uniformly authentication requests from application users among the replicas of the ECAS instances. It also prevents deadlocks and avoids unnecessary queues.

(iii) ECA Service — this is a set of VMs running instances of the ECC application which is a self contained service that can receive authenticated requests and return authentication tokens as requested through the load balancer to the admission control in form of handshake.

(iv) Physical Machines: hosts a number of VMs running different types of application services. Some of the services are self-contained (e.g. VM1, VM2, etc.), while others may be composed of more than 1 VMs (as in VM3a & VM3b).

IV. RESULTS

When a file or document is to be sent to the Cloud, the document is first compressed using the Compression algorithm to make sure there is no alteration of the file even in transit and to compact it in such a way that the space to be occupied in the Cloud is very small. After passing through the compression algorithm, the ECC is now used to encrypt the file or document irrespective of the format. Figure 3 shows the screenshot of the homepage of the encryption and decryption app before the message is taken to the Cloud.

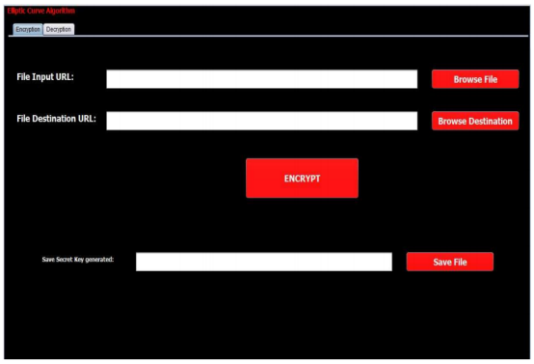

Figure 3. Encryption Home page.

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

After the destination path had been chosen for the encrypted file, a serialized, randomly generated secret key is saved for decryption of the data. This is done to prevent possible eavesdropping attack. The system then notifies user with a message on successful encryption as shown in figure 4.

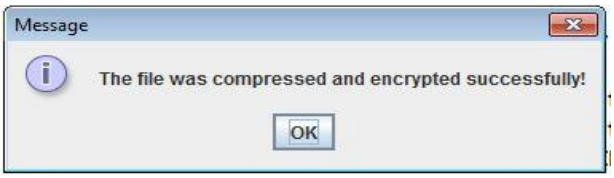

Figure 4 File compression and encryption success notification.

Next is the Cloud Storage.

Figure 5. The Welcome Page of SCSA

From this page, available tasks are presented as option buttons. These includes: app download; file management; and user account/profile management.

In the administrator's view of the storage system. The files are zipped automatically by the system for security and compactness and only visible to the storage provider.

The system is designed in a way that individual Cloud Client has access to their page. Any other Client that shares the same Cloud Provider cannot access the page of another Client. From here, screen, data or message stored irrespective of the size is compressed to optimize storage. The page also provides a view of the storage system with features for editing files. However, only filenames can be edited by the user on site. Any necessary modification to the files by the user or owner will require local decompression and decryption after a download. Thereafter, the system performs the reversal by encrypting, compressing and uploading to the Cloud. This forms part of the security system.

A. Comparative Analysis of ECC against RSA Relative to Cloud Services.

The comparative analysis was done using RSA against ECC. RSA is being used because it is an example of Public key Cryptography that is commonly used for any web service application. The metrics used in this comparative analysis is time of encryption and file size.

The key sizes definitely show their effect on these two algorithms. More so, the work of [9] ascertained that ECC have higher key strength than RSA. This can be deciphered from the key size ratio that is depicted in Table 1. The key and signature generation is still faster in ECC. Then the key size difference also goes a long way in giving much strength to ECC

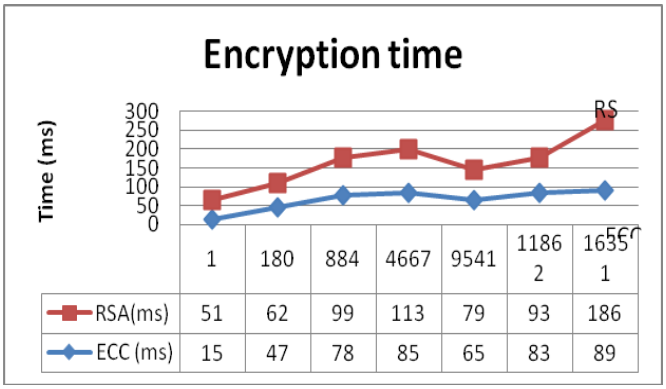

Figure 6. The Graph of RSA/ECC Encryption Time on Windows 7.

Figure 9 proofs the afore-mentioned theory that ECC encryption is faster. This is due to the smaller key size of ECC as compared to RSA. This makes the algorithm more suitable for constrained devices or environments. The time to break this encryption depends on the solution to the discrete logarithm problem.

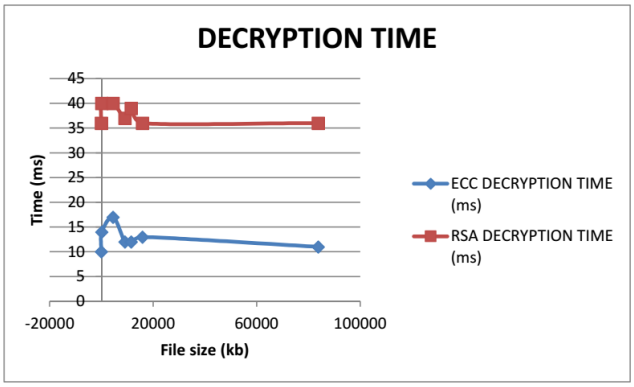

Figure 7. The decryption time graph.

This also follows the same trend as all the other ones. But the strength of ECC lies in the absence of a sub-exponential time algorithm for the ECDLP which means that significantly smaller parameters can be used in ECC than with RSA. The advantages that can be gained from smaller parameters include speed and smaller keys or certificates. These advantages are especially important in environments where at least one of the following resources is limited: Processing power; Storage space; Bandwidth and Power Consumption.

B. Processing Time

When these two algorithms were run on Windows 7, the ECC key size that was used was 160r1 as against the RSA 1024. From figure 8, it can be seen that the processing time of ECC is faster than that of RSA.

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

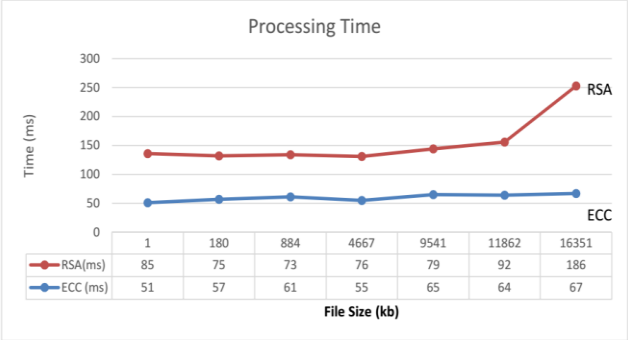

Figure 8. The graph of the processing time

It can also be inferred that the processing time of ECC is faster than that of RSA. This also shows that the processing power required to operate ECC is far less than that of RSA.

C. Server Handling Request Time

The effect of the algorithms could also be determined from the time taken for each request to be handled in the Cloud Server. According to Nick Sullivan's blog [10], While RSA could be kept secured by increasing the key length which comes with a cost of slower cryptographic performance, implying more cost of computational power and time for the client, ECC offer a better tradeoff: high security with short, fast keys.

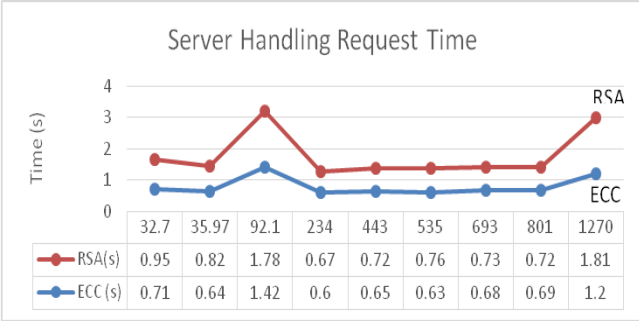

Figure 9. The Graph of the server handling request time.

C. Analysis Based on Time Complexity.

Time Complexity of an algorithm according to [9] measures the amount of time taken for an algorithm to run as a function of the length of the string representing the input. This is usually denoted by the Big Order Notation (Θ) because the coefficients and the lower order terms are always excluded. To calculate the runtime complexity of the algorithms used in this research work, snippets of the codes where the major operation is carried out are used.

Summary of the run time complexity is shown in Table 2.

Table 2. Run Time Complexity

Algorithm	Encryption	Decryption	Observations
ECC	$\Theta(n^2)$	$\Theta(\log(n))$	Faster
RSA	$\Theta(n)$	$\Theta(n)$	Slower

From this, the theory that ECC is faster and much more suitable for resource constrained environments is further established as the run time of algorithmic complexity of ECC is faster than RSA.

V. CONCLUSION

Internet has become the fastest growing aspect of technology. And as its usage increases, so will malicious activities increase. In other to cope with this trend, stronger cryptographic algorithms that are more difficult to break are needed to make the internet which is the technology behind the Cloud safe. Although, several attempts had been made at providing secured environment for activities in the Cloud, Elliptic Curve Cryptography (ECC) provides solutions for a secured Cloud environment with improved performance in computing power and energy. This makes it attractive for mobile applications. ECC has been proven to provide a robust and secured model for the development and deployment of secured application in the Cloud both from the Client side and the Server side.

REFERENCES

[1]. Alowolodu O.D, Alese B.K, Adetunmbi A.O, Adewale O.S, Ogundele O.S (2013), Elliptic Curve Cryptography for securing Cloud Computing Applications. International Journal of Computing Applications (IJCA), USA, (0975-8887) Volume 66-No23.

[2]. Ankita Sim and Nisheeth Saxena (2013), Elliptic Curve Cryptography: An efficient approach for Encryption and Decryption of a Data Sequence. International Journal of Science and Research (IJSSR), India Online ISSN: 2319-7064. Vol 2 Issue 5.

[3]. Darrel Hankerson, Alfred Menezes, Vanstone (2004). "Guide to Elliptic Curve Cryptography". Springer-Verlag New York, INC., 175 fifth avenue, New York 10010, USA.

[4]. Kerry Matetsky (2015). RSA vs ECC Comparison for Embedded Systems, A White paper of Atmel-8951A-CryptoAuth-RSA-ECC-Comparison-Embedded-Systems-whitepaper.

[5]. Kumar S.D, Suneetha CH and ChandrasekhAR A (2012). Encryption of Data using ECC over Finite Fields. International Journal of Distributed and Parallel Systems (IJDPS) Vol 3, No. 1

[6]. McKinsey and Company (2009)." Clearing the Air on Cloud Computing" . A white paper. Source:http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/McKinsey_Cloud%2

[7]. Muhammad Yasir Malik (2010). Efficient Implementation of Elliptic Curve Cryptography Using Low-power Digital Signal Processor. ISBN 978-89-5519-146-2 ICACT 2010 News.cnet.com. http://news.cnet.com/8301-1009_3-10150569-83.html.

[8]. Shivkumar S. and Umamaheswari G. (2014), Certificate Authority Schemes Using ECC, RSA and their Variants –Simulation Using NS2. American Journal of Applied Sciences, Vol 11, Issue 2 (171-179).

[9]. Swadeep Singh, Anupriya Garg Anshulsachdeva (2013), Comparison of Cryptographic Algorithms: ECC and RSA, International Journal of Computer Science and Engineering (IJCSE) Special Issue on Recent Advances in Engineering and Technology (NCRAET).
[10]. Thomas H Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein (2009), Introduction to Algorithms (3rd Edition). Published by the Massachusetts Institute of Technology, USA.
[11]. Nick Sullivan (2015). Bringing Elliptic Curve Cryptography into the main Stream, Blog of Nick, www.slideshare.net

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)