International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Data Security in Cloud Computing with Elliptic Curve Cryptography

Abdulkadir Abdullahi Ibrahim[a]*, Dr. Wilson Cheruiyot[b], Dr. Michael W. Kimwele[c]

[a,b,c]*School of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology Kenya*

[a]*Email: fadlurabi@gmail.com,* [b]*Email: wilchery68@gmail.com,* [c]*Email: mkimwele@jkuat.ac.ke*

Abstract

Cloud Computing (CC) is one of the most important and hottest deal of attention, both in academia researches and among users, due to its ability for satisfying the computing needs by reducing commercial expenditure bandwidth with computing compounds while increasing scalability and flexibility for computing services, accessing it through an Internet connection from anywhere in the world its available Internet network..However it becomes particularly serious because the data is located in different places even in the entire globe and should be taken into account such as violation of the confidentiality and privacy of customers' data via unauthorized parties. So the only causes imperfection in the cloud computing is security impairment generally and especially data security. Despite about organizations and individual user adopting cloud computing, put their data in cloud due to the security issues challenges associated with it requires that organizations trust needs a technical tools protecting their data. Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. Hence, we proposed data security in cloud computing with elliptic curve cryptography a proficient data security model algorithm, as a secure tool to model a Secured platform for Data in cloud computing. The algorithm was simulated using Java Development Kit (JDK) to implement the curve operations to extract the data in the Cloud, encrypting, decrypting, signing and verifications the signature, followed by testing the acquired results the implemented classes and their design Although this topic represent a good sample of the work that is being done, there are many requirements to study this area due to the needs of cloud computing in the next generation both individuals and organization even governmental agencies Might parallel increase of cyber attackers and they improve their techniques so as a researcher suggest the importance of data in ECC to be studied.

Keywords: cloud computing; Data security; Hashing; Digital Signature; ECC algorithm.

---

* Corresponding author.

1. Introduction

Cloud Computing (CC) is one of the most important and hottest deal of attention, both in academia researches and among users, due to its ability for satisfying the computing needs of the users by reducing commercial expenditure bandwidth with computing compounds while increasing scalability and flexibility for computing services, accessing it through an Internet connection from anywhere in the world available Internet network. It was predicted as early as in 1969 by Leonard Kleinrock, one of the chief scientists of the original Advanced Research Projects Agency Network (ARPANET) project which preceded the Internet, who said: "As of now, computer networks are still in their infancy, but as they grow up and become sophisticated, we will probably see the spread of 'computer utilities' which, like present electric and telephone utilities, will service individual homes and offices across the country." This vision of computing utilities based on a service provisioning model anticipated the massive transformation of the entire computing industry in the 21st century whereby computing services will be readily available on demand, like other utility services available in today's society [1]. The National Institute of Standards and Technology (NIST) define cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [2]. The Cloud Computing model offers the promise of massive cost savings combined with increased IT agility. It is considered critical that government and industry begin adoption of this technology in response to difficult economic constraints. However, cloud computing technology challenges many traditional approaches to datacenter and enterprise application design and management. Cloud computing is currently being used; however, security, interoperability, and portability are cited as major barriers to broader adoption [3]. The following Figure shows the various cloud computing services with their examples.

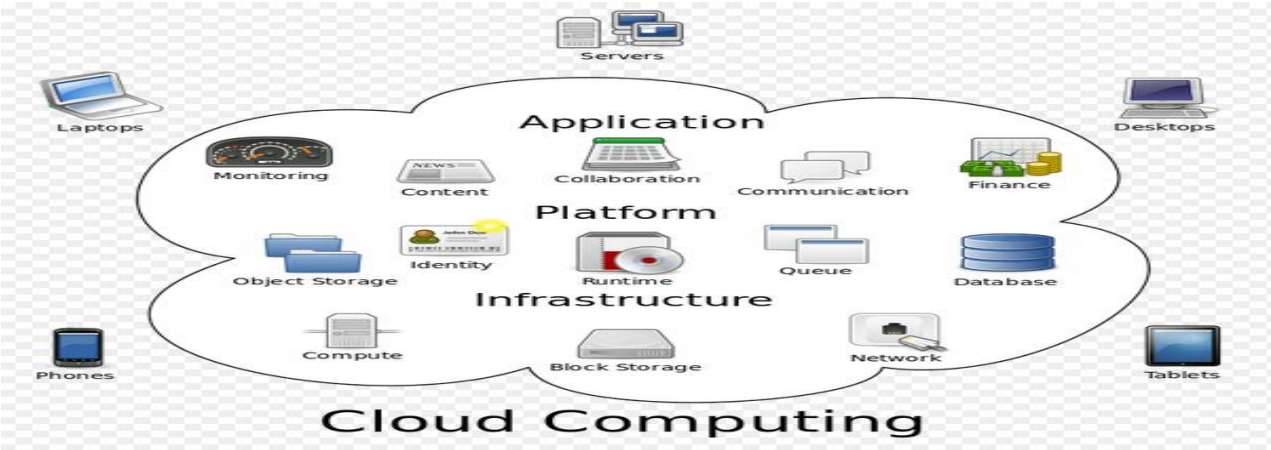

Figure 1: The various cloud computing services with their examples [4].

Cloud Providers offer services that can be grouped into **three** categories:

1. **Software as a Service (SaaS):** In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the

customers'' side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

2. Platform as a Service (Paas): Here, a layer of software, or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE, Ruby etc. Google's App Engine, Force.com, etc are some of the popular PaaS examples.

3. Infrastructure as a Service (Iaas): IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, GoGrid, 3 Tera, etc [5].

2.1 Cloud computing security services

The basic security services for information security include assurance of data Confidentiality, Integrity, and Availability (CIA). In Cloud computing, the issue of data security becomes more complicated because of the intrinsic cloud characteristics. Before potential cloud users are able to safely move their applications/data to the cloud, a suit of security services would be in place which we can identify as follows (not necessarily all needed in a specific application):

I. **Data Confidentiality assurance**: This service protects data from being disclosed to illegitimate parties. In Cloud Computing, data Confidentiality is a basic security service to be in place. Although different applications may have different requirements in terms of what kind of data need Confidentiality protection, this security service could be applicable to all the data objects discussed above.
II. **Data integrity protection**: This service protects data from malicious modification. When having outsourced their data to remote cloud servers, cloud users must have a way to check whether or not their data at rest or in transit are intact. Such a security service would be of the core value to cloud users. When auditing cloud services, it is also critical to guarantee that all the audit data are authentic since these data would be of legal concerns. This security service is also applicable to other data objects discussed above.
III. **Guarantee of data availability**: This service assures that data stored in the cloud are available on each user retrieval request. This service is particularly important for data at rest in cloud servers and related to the fulfillment of Services Level Agreement. For long-term data storage services, data availability assurance is of more importance because of the increasing possibility of data damage or loss over the time.
IV. **Secure data access**: This security service is to limit the disclosure of data content to authorized users. In practical applications, disclosing application data to unauthorized users may threat the cloud user's

business goal. In mission- critical applications, inappropriate disclosure of sensitive data can have juristic concerns. For better protection on sensitive data, cloud users may need fine grained data access control in the sense that different users may have access to different set of data. This security service is applicable to most of the data objects addressed.

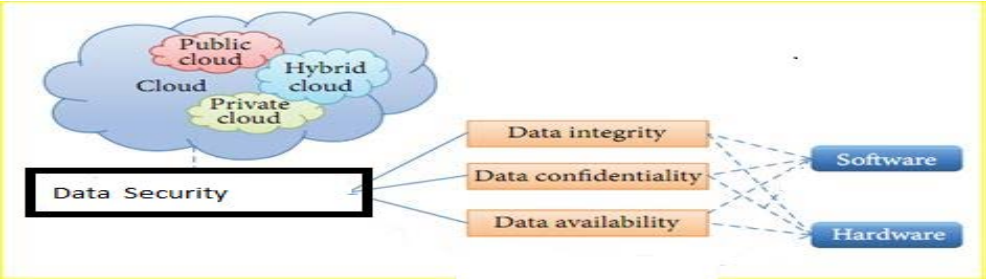

Figure 2.1: Organization of Data Security in Cloud Computing [6].

2.2 Data security in cc challenges

Cloud computing security is the major concern and has various challenges that need attention [8:24] . If proper security measures are not implemented to the data transmitted and operated on cloud, the data is at higher risk than when stored or operated in local repositories. Malicious user, who wants to gain access to transmitted data in cloud, can do that by tapping into the connection between user and remote location. He can also hack into users account and get access to sensitive information by creating another account (by using virtualized infrastructure that CC provides) in the same service provider with malicious intent Since cloud computing provides different services to chose from for diversified group of users (nave, expert, malicious etc.), possibility of having data at risk when working in cloud computing systems is a huge [8:3].

So the need for categories of data security challenges in cloud computing is very important, and there are some categorizations proposed by some authors in their discussions as mentioned below.

Security provided by cloud SP's might not be highly cost effective when implemented in small companies. But when two or more organizations share a common resource there is a risk of data misuse. In such situation it is required to secure data repositories, Not only the data repositories but also data should be secured in any stage such as storage, transit or process, Since this kind of sharing resources is prevalent in the CC scenario, protection of data is important and is the most important challenge among other CC challenges, In shared areas to keep data secure is challenging than protecting in a personal computer .Given below are three key areas in Data security that CC refers to:

1. Confidentiality: When enterprise data is stored outside organizational boundaries it needs to be protected from vulnerabilities. To protect data from vulnerabilities; employees must adopt security checks to ensure that their data stays protected from malicious attacks. Few tests are used to help organizations to assess and validate, to which extent data is protected from malicious user and they are as follows:

(a) Cross-site scripting [XSS]

(b) Access control weaknesses(c) OS and SQL injection flaws

(d) Cross-site request forgery [CSRF]

(e) Cookie manipulation

(f) Hidden field manipulation

(g) Insecure storage

(h) Insecure configuration

Example: With the help of Payment Card Industry Data Security Standard (PCI DSS) the data is not allowed to go outside the European Union .This can also enforce encryption on certain areas of data and by encrypting data in this way permission is given only to specific users to access specific areas of data.

2. **Integrity**: There is no common policy that exists for data exchange. To maintain security on client data, thin clients are used where only few resources are possible. Since only few resources are given access user are not suggested to store any personal data such as passwords. Since passwords are not stored on desktops, passwords cannot be stolen by anyone.

Integrity of data can be further assured by:

- Using some extra features which are like unpublished API's for securing a particular section of data.
- Using DHCP and FTP for long time has been rendered as insecure.

3. **Availability**: Availability is the most problematic issue, where several companies face downtime (i.e., denial of service attack) as a major issue. The availability of a service generally depends on contract signed between client and vendor

Some other points that need to be highlight when it comes to data security:

- Who has rights over data (i.e., does data still belong to company?)
- If there is any other company or organization being involved (i.e., is there involvement of any third party organization)
- Customers using CC applications need to check, if the data provided by cloud service providers is carried out in a lawful way or not.
- If data protection fails while data is being processed, it could result in administrative, criminal sanctions or civil type of issues (which depends on country controlling data). These issues may occur due to multi transfers of data log between federated cloud providers.
- Cryptographic algorithm should be maintained well and updated regularly, failing to do so could lead

in disclosing personal data

- Data is not completely protected when it is encrypted and stored. When searching for a piece of information again in CC servers care should be taken to retrieve information in a secured process. Traditional searches can disclose data to other companies/individuals

Not only this but also using complex ways to encrypt can also raise issues while retrieving data from storage [8:25-27].

2.3 Data security lifecycle

One of the primary goals of information security is to protect the fundamental data that powers our systems and applications. As we transition to Cloud Computing, our traditional methods of securing data are challenged by cloud-based architectures. Elasticity, multi-tenancy, new physical and logical architectures, and abstracted controls require new data security strategies. With many cloud deployments we are also transferring data to external — or even public — environments, in ways that would have been unthinkable only a few years ago (Cloud Security Alliance, 2009). The Data Security Lifecycle is different from Information Lifecycle Management, reflecting the different needs of the security audience. The Data Security Lifecycle consists of six phases:

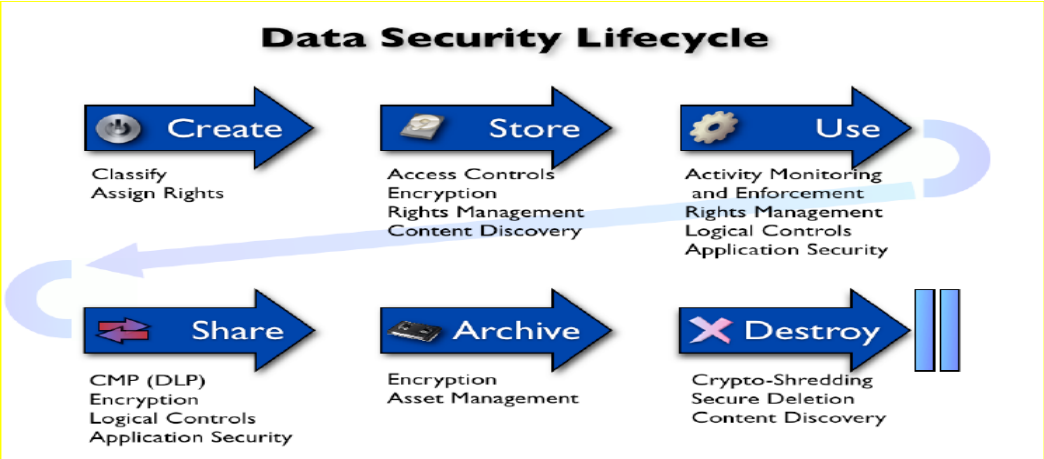

Figure 2.3: The data security lifecycle phases

2.4 Data Breaches

Since data from various users and organizations is stored in a cloud environment, if user with malicious intent enters the cloud environment, the entire cloud environment is prone to a high value target. A breach can occur due to accidental transmission issues (such breaches did happen in Amazon, Google CC's) or due to an insider attack. In any case of breach data is com- promised and is always a security risk which is also a top threat mentioned by CSA. There is a high requirement for breach notification process available in the cloud. It is because if breaches are not notified the cloud might not be able to notify serious attacks.

Table 2.1: Business breach report blog

	Threat	**Impact**	**Resulting in Pseudo Risk**
External Criminals Pose	Greatest (73%)	Least (30,000 compromised records)	67,500
Insiders Pose	Least (18%)	Greatest (375,000 compromised records)	67,500
Partners are middle	73.39%	73.39%	73,125

The business breach report blog gives information on the impact of breaches, as shown in table 2.1. We can see that the threat of external criminals is greatest by 73% but with least compromised records. On the other hand threat of insiders is least with 18% but the impact they cause is greatest [9].

2.4 Related Works

propose a Data security model that uses Elliptic curve cryptosystem for digital signature, to provide the safety and security assurance to the users data in Cloud Computing, In his work both digital signature scheme and public key cryptography are integrated to enhance the security level of Cloud. In his results showed The Strength of the algorithm due to the difficulty level used in computing discrete logs in a large prime modulus has increased the efficiency of the proposed model. Also Integration of Elliptic curve cryptosystems and digital signature has improved the security level provided to the user's data in the Cloud. ECC uses the smaller key sizes that involves less complexity but provides the same level of security as other public-key cryptosystems which uses larger key sizes involving greater complexity**.**

Proposes techniqsues to enhance users' privacy based on RSA algorithm. This proposal allowing users to authorize access to their remotely-stored data. But the largest bits may caused more problems with transferring data to the cloud computing, the use ECC techniques best privacy to the users of cloud computing **.**

Propose an effective and safe protocol by use ECC and Sobol sequence. This protocol provides integrity and confidentiality of data. Moreover, their system also supports dynamic data operations, which performed by the user on data stored in cloud while maintaining same security assurance.

2.5 Critique analysis for data security in cloud computing with ECC

As many companies move their data to the cloud the data undergoes many changes and there are many challenges to overcome. To be effective, cloud data security depends on more than simply applying appropriate data security procedures and countermeasures. Computer based security measures mostly capitalizes on user

authorization and authentication.

We outline several critical security and privacy challenges, point out their importance, and motivate need for further investigation of security solutions.

Privacy addresses the confidentiality of data for specific entities, and it carries legal and liability concerns, and should be viewed not only as a technical challenge but also as a legal and ethical concern. Protecting privacy in any computing system is a technical challenge, and in a cloud setting this challenge is complicated by the distributed nature of clouds and the possible lack of user awareness over where data are stored and who has or can have access. From the security and privacy point of view the following two features of cloud computing appears as the top important ones: data service outsourcing, and computation outsourcing. The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as critical data and processes. The researches proposed in data security in cloud computing sufficiently technique was not proved that ECC is less key size and less cost and high ratio according with RSA , ECC create faster, smaller, and more proficient than the other cryptography techniques when it applied in data for cloud computing . And there is less confidentiality from the organizations to adopt cloud computing to put their data. This gap and poor of the research area needs more technique to enhance and approve cryptogtography techniques [10].

3.1 Proposed algorithm for data security in cloud computing with ecc

Both clouds agree to some publicly-known data item.

a. The elliptic curve equation

I. values of a and b
II. prime, P

b. The elliptic group computed from the elliptic curve equation
c. A base point, B, taken from the elliptic group

Key generation:

I. A selects an integer dA. this is A's private key.
II. A then generates a public key PA=dA*B
III. B similarly selects a private key dB and computes a public key PB= dB *B
IV. A generates the security key K= dA *PB. B generates the secrete key K= dB *PA.

Signature Generation:

For signing a message m by sender of cloud A, using A's private key dA

1. Calculate e=HASH (m), where HASH is a cryptographic hash function, such as SHA-1
2. Select a random integer k from [1, n − 1]

3. Calculate r = x1 (mod n), where (x1, y1) = k * B. If r = 0, go to step 2
4. Calculate s = k − 1(e + dAr)(mod n). If s = 0, go to step 2
5. The signature is the pair (r, s)
6. Send signature (r, s) to B cloud.

Encryption algorithm: Suppose

A wants to send to **B** an encrypted message.

I. A takes plaintext message M, and encodes it onto a point, PM, from the elliptic group.
II. A chooses another random integer, k from the interval [1, p-1]
III. The cipher text is a pair of points : PC = [(kB), (PM + kPB)]
IV. Send cipher text PC to cloud B.

Decryption algorithm: Cloud

B will take the following steps to decrypt cipher text PC

a. B computes the product of the first point from PC and his private key, dB dB * (kB)
b. B then takes this product and subtracts it from the second point from PC (PM + kPB) – [dB(kB)] = PM + k(dBB) – dB(kB) = PM
c. B cloud then decodes PM to get the message, M.

Signature Verification:

For B to authenticate as signature, B must have as public key PA

1. Verify that r and s are integers in [1, n − 1]. If not, the signature is invalid
2. Calculate e = HASH (m), where HASH is the same function used in the signature generation
3. Calculate w = s −1 (mod n)
4. Calculate u1 = ew (mod n) and u2 = rw (mod n)
5. Calculate (x1, y1) = u1B + u2PA

The signature is valid if x1 = r(mod n), invalid otherwise.

4.1 Introduction to the mathematical background

ECC Basically, it is “an approach to public-key cryptography based on the mathematics of elliptic curves” (Wikipedia). The good thing about Elliptic Curve Cryptography (or ECC), is that it can be faster than RSA and uses smaller keys, but still provides the same level of security. What makes ECC better? To quote Scott Vanstone (co-founder of Certicom, a company specializing in wireless security), “ECC is based on something called the elliptic curve discrete log problem, and it’s a much harder problem than factoring integers. Because it’s much harder, we can get away with fewer bits, so what we like to say is that ECC provides the most security

per bit of any public key scheme [11] .

Below is a table from Certicom comparing the security level of various key sizes in ECC and RSA?

NIST guidelines for public key sizes for AES

ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15 360	1 : 30	256

Supplied by NIST to ANSI X9-F1

Table4.1: The security level of various key sizes in ECC and RSA.

Every cryptosystem is based on a hard mathematical problem that is "computationally infeasible to solve" (Certicom). ECC relies on the difficulty of solving the discrete logarithm problem for the group of an elliptic curve over some finite field (such as integers modulo a prime number, or a Galois field of size a power of two).Where RSA would use modular multiplication, ECC makes use of the addition operation of elliptic curves; and ECC's multiple addition is the equivalent of RSA's modular exponentiation. But first let's discuss elliptic curves. An elliptic curve over real numbers is a set of points (x, y) which satisfy an elliptic curve equation y2 = x3 + ax + b; where a, b, x, and y are real numbers (Certicom). The elliptic curve changes with various choices of a and b. "An elliptic curve group over real numbers consists of the points on the corresponding elliptic curve, together with a special point O called the point at infinity" (Certicom). So how do we perform the addition operation on the points of an elliptic curve? You have two points, P and Q on an elliptic curve, and P + Q = R. To determine R a line is drawn through points P and Q, and the line will intersect the elliptic curve at a third point, which is –R. The point –R is then reflected in the x-axis to point R. For example:

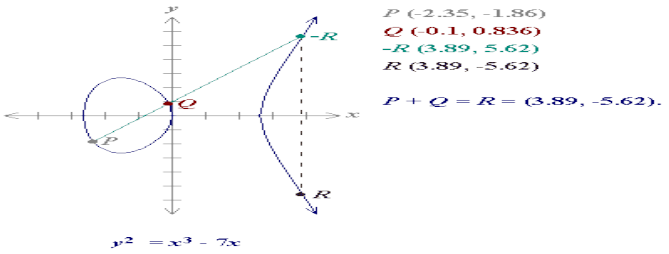

Figure 4.1: (Certicom)

4.2 Implementation of Elliptic Curve Cryptography

The design of the system proposed in this study illustrates the functions which were used in the system. It is started with the operation field, and this is followed by the elliptic curve operation to calculate the points over the curve. The highest level in the present system was designed to generate and verify data in cloud computing. The elliptic curve operations involve multiplication, squaring, addition and inversion in the underlying field. Meanwhile, the inversion operation is the most expensive operation in the field. The elliptic curve cryptosystem implementation in the present study uses the polynomial base fields. I used

Java Development Kit (JDK) to implement the curve operations to extract the data in the Cloud, encrypting, decrypting, signing and verifications the signature, followed by testing the acquired results the implemented classes and their design I discussed below a design of the present prototype system attempted to achieve a high level of security using signature generated to produce the domain parameters of the elliptic curve, or to produce private keys.

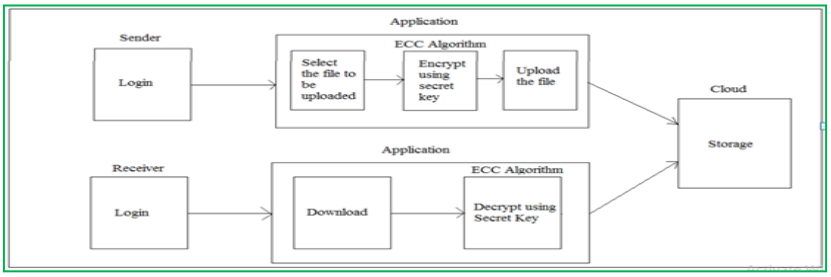

Figure 4.2: Implementation of ECC data in Cloud computing (simulation of The System proposed)

4.3 User Interface Development

After coding the classes, reasonably it has to be integrated to an appropriate interface so that users can perform and react to the actions of the system. Users' requests are sent as messages to a particular function or class for processing, and the results are shown on the interface. In addition, it is designed to prevent the user from entering invalid inputs which may corrupt the results. For instance, the user cannot change the fields of the domain parameters on the interface. Similarly, the user cannot sign the message without producing the digest for the message. The interface is assembled of the text fields, buttons, text area and radio buttons. The text area is actually the message 'm' where the user can enter his message. **Figure 4.3** shows or prototype system user interface [12].

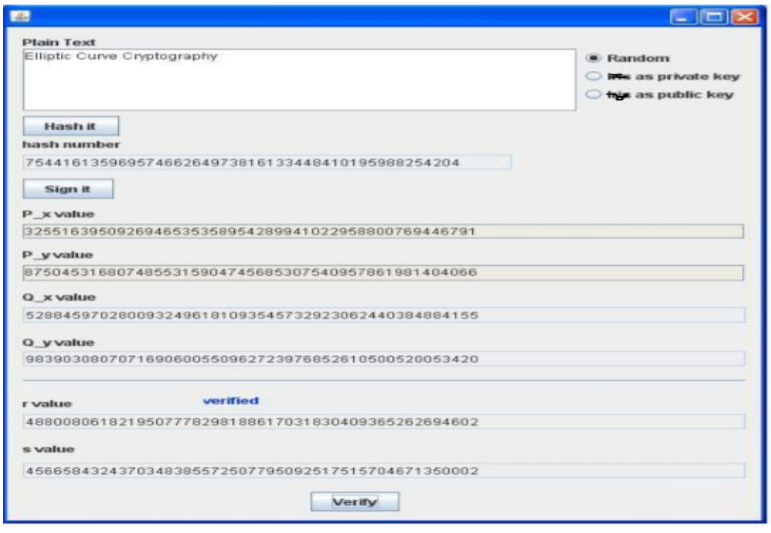

Figure 4.3: Simulation of the signature algorithm prototype system.

6. Conclusion

This paper mainly focuses on showing the Data Security in Cloud Computing with Elliptic Curve Cryptography (ECC). we were able to demonstrate Encryption, Decryption, and Digital Signature (ECDSA) with Elliptic curve cryptography using the polynomial representation over the binary field implemented security of the data in cloud computing its requires a thorough understanding of the application and the algorithms which are used in generating Public and Private keys. Cyber attackers As much as gigabytes of data deliberate actions to alter, disrupt, deceive, degrade, or destroy in the cloud computing, computer systems or networks or the information and/or programs resident in or transiting these systems or networks. ECC is slowly becoming accepted as the next generation default for information security, partially because mobile devices require smaller key sizes and ECC offers more security per bit of key length. There are a few known attacks on ECC, but most of the attacks require a specific type of Elliptic Curve and do not work for a general Elliptic Curve. Care are must be taken to ensure that the parameters chosen for an Elliptic Curve to be used in a cryptosystem do not form an insecure curve. Typically, however use a set of standard parameters that have been inspected thoroughly by companies whose mission is to develop security standards in the cloud computing.

In this paper, we have only had a glimpse into the massive body of mathematical and computational research that has been done and is being done on Elliptic Curves. Although I believe this topic represent a good sample of the work that is being done, there are many requirements to study this area due to the needs of cloud computing in the next generation both individuals and organization even governmental agencies may parallel increase of cyber attackers and they improve their techniques so as a researcher suggest the importance of data in ECC to be studied.

7. Recommendations

Cryptography is a body of mathematics with a very rich history. Securing information has been a real concern for centuries and this need for security has recently become even more essential with the introduction of the internet. The Public Key encryption process is a counter-intuitive scheme. It a strange system in which one cannot even decode one's own cipher text, but rather the cipher texts are furnished in such a way that only the person they were created for can decode them. It also relies on the Presumption that certain problems are computationally difficult to solve, unless one has some Extra information, for its security. For most encryption schemes we do not actually have a proof that a breaking the system is hard. Public Key encryption is useful because it allows parties that have never met to share small amounts of confidential information. Many times that small amount of information is a private key which can be used in a more efficient symmetric cipher [13].

So as researchers we recommended use of elliptic curve cryptography because it is faster with small keys of bits than the other and have the following the following specification in the cloud computing:

- the importance of strong data security in the Cloud Computing

- the appropriate strategies that may help use an effective and strongest data security in cloud computing to across cryptanalysis challenges in cloud computing technology
- verifying some application areas require cryptographic algorithms and protocols that can offer a higher confidence and assurance level of security that must protect organizations assets
- The data security of encryption primitive or technique can be reduced to an assumption on the difficulty of the mathematical problems by using, which are vitally importance to simplifying the complex system and designing proactive and adaptive system in a dynamic and complex environment towards data security.

References

[1] L. Kleinrock, "A Vision for the Internet", ST Journal of Research, 2(1):4-5, Nov, 2005.

[2] Mell, Peter, and Timothy Grance, "The NIST definition of cloud computing (draft)," NIST special publication vol.800, 2011.pp 145.

[3] P. Siani. "Privacy, security and trust in cloud computing." Privacy and Security for Cloud Computing. Springer London, 2013. pp3-42.

[4] H.Jian, Z. . "Analysis and Application of Consumer Features with Cloud Computing and Data Mining Technology." In Intelligent Computation Technology and Automation, 7th International Conference ICICTA, Oct 2014 ,pp. 84-87.

[5] B. Rajiv R and M.Nitin."CLOUD COMPUTING A CRM SERVICE BASED ON SEPARATEENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM." computing, vol.1, pp. 11.

[6] D.Sajal K and K. Krishna and Z.Nan . Handbook on securing cyber-physical critical infrastructure. Elsevier, 2012.PP.392-394.

[7] Y.Huiming, et al. "Cloud computing and security challenges." Proceedings of the 50th Annual Southeast Regional Conference. ACM, 2012. pp. 298-302.

[8] S .Bulusu and K. Sudia . "A Study on Cloud Computing Security Challenges." M.Sc. thesis, Blekinge Institute of Technology, Sweden, 2012.

[9] S.Subashini, and K.Veeraruna. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications, Vol.34.pp. 1-11, Jan. 2011.

[10] K.Parsi, and S.Singaraju. "Data security in cloud computing using RSA algorithm." .IJRCCT,vol. 1. pp143-146,apr.2012.

[11] V.Rajasekaran and M. Suganya. "An Analysis of SPI Security Issues for Cloud

Computing." Biometrics and Bioinformatics ,vol5,pp 425, dec.2013.

[12] G.Sagayee, and M. Anandha . "Biometric encryption using enhanced finger print image and elliptic curve." International Journal of Electronic Security and Digital Forensics, vol.2 5. pp. 110-123, feb.2013.

[13] A. Yasser." Implementation of Elliptic Curve Cryptography using biometric features to enhance security services". Diss. University of Malaya, 2009.

Firs author

ABDULKADIR ABDULLAHI IBRAHIM received his Bachelor's degree (Mathematics and computer science) from International University of Africa, Sudan, in 2009. He is going his Master's degree (Computer Systems) from Jomo Kenyatta University of Agriculture and Technology, Kenya. He is currently a Lecturer of Mathematics and Computer Science courses at University Of Somalia and Simad University, (Mogadishu, Somalia) His research interests include Information Systems, data security, Cloud Computing, mobile computing, Human computer interaction, and Information Systems Security, Cryptography and Computer ethics.

Second author

Wilson Cheruiyot received his Bachelor's degree (Mathematics and computer science) from Jomo Kenyatta University of Agriculture and Technology, Kenya, in 1994. He received his Master's degree and PhD (Computer Application Technology) both from Central South University, China, in 2002 and 2012 respectively. He is also a Microsoft Certified Professional (MCP) and a Microsoft Certified Database Administrator (MCDBA). He has previously worked with the Teachers Service Commission of Kenya and with the Kenya National Audit Office (KENAO). He is currently a professor of Computer Science at the Computing Department, Jomo Kenyatta University of agriculture and Technology .His research interests include Artificial Intelligent (Agents Applications in Automation and Data Mining, Evolutionary Computing, AI in Multimedia Applications) , Information Systems, E-Commerce, mobile computing, Human computer interaction, optimization Information Systems Security, and Computer ethics.

Third author

Dr. Mikel W. Kimwele is a lecturer in the department of computing, Jomo Kenyatta university of Agriculture and Technology. He holds BSc Mathematics and Computer Science from JKUAT. Received masters in information technology from university of Sunderland UK, and Doctorate in Information Technology from JKUAT. His research interests include Information Systems management, E-Commerce, mobile computing, Human computer interaction, Information Systems Security, and Computer ethics.