Web-Cloud-based Security Services based-on Elliptic Curves Cryptosystem

Victor Onomza Waziri
Cyber Security Science Department, School of ICT, Federal University of Technology, Minna Nigeria

John K. Alhassan
Cyber Security Science Department, School of ICT, Federal University of Technology, Minna Nigeria

Hakimi Danladi
Department of Mathematics/Statistics, School of Physical Sciences, Federal University of Technology, Minna, Nigeria

Faiza Babakano Jada
Information Media Technology Department, School of ICT, Federal University of Technology, Minna Nigeria

ABSTRACT
This paper dwells theoretically on the application of Elliptic Curves Cryptography (ECC) for the web and Cloud and Cloud Computing environments. ECC is still in its embryonic utility formation unlike the RSA that has gained much ground in its application on the web security as it offers extensive applications to the various aspects of authentications, e-commerce and mobile phones; but it consumes a lot of power that may not be useful to Smartphones in the context of Mobile cloud computing. Notwithstanding, there is some remarkable deployment of ECC for web security currently on-going This paper establishes the position and role of ECC in the web computing environment. A general introduction to the web and security threats emerging from the use of the web is discussed. Different types of security protocols on the web (IPSec, SSL/TLS and SSH) are discussed. The paper expounds how ECC is deployed on the SSL/TLS protocol-the dominant security protocol on the web- to contain the adversaries. Moreover, we made an effort to discover why people may make the choice of ECC over other cryptographic systems like RSA and discrete logarithm cryptographic systems. Finally, with the hype in mobile Cloud Computing, the paper discusses the security implementations how ECC is applied on Digital Signature

Keywords
Public-key cryptography, Elliptic Curve Cryptography (ECC), Web security, Secure Socket Layer (SSL), Cloud computing

1. INTRODUCTION
There is a great need for web security in nowadays web services due to the constant insecurity being experienced on the Internet. Individuals, organizations, governments, schools and businesses all have one or more things to do on the Internet and therefore web services is becoming ubiquitous. Most information that passes through the web is more sensitive and confidential than others. For instance, businesses and financial institutions that are established on the web need to guarantee the security of their customers' information.

Web security infrastructures including IPSec on the Network layer and SSL/TLS on the transport layer of the TCP/IP protocol suit are deployed to contain the adversaries that exist on the web with malicious intends that may involve eavesdropping of packets flow on the network, changing and stealing sensitive messages contents and impersonating people and objects in form of identity theft. Different types of cryptographic systems are used for web securities that include symmetric and public-key cryptosystem schemes. Data

Encryption Standard (DES), RC4 and Advanced Data Encryption Standard (AES) are example of the former; while RSA, Discrete Logarithm (DL), Merkle-Damgard algorithm and Elliptic curves are examples of the latter (RSA relies the hardness of integer factorization problem, El Gamal (DL) is based on hardness of discrete logarithm problems with Digital Signature Algorithm(DSA) being one of its variants and elliptic curves cryptography is based on the hardness of elliptic curves discrete logarithm problem). Symmetric-key schemes can also use a message authentication code (MAC) algorithm such as Hash Message Authentication Code (HMAC) to achieve data integrity and data origin authentication.

Public-key cryptographic systems provide functionalities like key generation, encryption and digital signature schemes. Of the three cryptographic schemes, elliptic curve cryptography (ECC) is the newest while Quantum Cryptography (QC) is still in its embryonic developmental stage. It is anticipated that when QC is fully developed, it shall improve the scalability of computational processes more then the existing cryptosystems and this would improve web efficiencies and services with attendant web security enhancement services. ECC is based on mathematics of elliptic curves and uses the location of points on an elliptic curve to encrypt and decrypt information. Elliptic curves can achieve desired level of security with smaller number of encryption key – a value that must be fed into the encryption algorithm to decode an encrypted message.

The rest of the paper structures are as follow: Section 2 reviews some related works, section 3 establishes some comprehensive basic web services structure and adversaries outlook, section 4 gives a skeletal brief of elliptic curves cryptography algorithms and its implementations in ITL, section 5 proffers the preference of ECC to other cryptosystems, Section 6 interconnects the ECC implementation to the Cloud computing environment, section 7 makes an envisioned further research recommendations while section 8 concludes the write up.

2. RELATED WORKS
Cryptography is concerned with the development and analysis of mathematical techniques that enables secure communications in the presence of malicious adversaries [2]. Unlike the classical cryptosystems (private or secret key) in which some were based on perfectly secure information

assumptions (as proved by Claude Shannon in 1949), modern cryptosystems are established on the assumption of asymptotic security [15]. Before the midst of the 1970's, the symmetric cryptosystem was the only type of cryptography that was in use. However, due to the short comings of the symmetric key cryptography in such area like key distribution problems (finding a secure and authenticated channel for the shared secret key), inability to provide elegant digital signature scheme that provides non-repudiation services, and key management problem (where an entity on a network may have to maintain different keying materials for each of the other entities on the network), public-key cryptography was invented [2]. While symmetric key encryption has a common secret key shared between the sender and the receiver, public-key infrastructure is based on some mathematical computational hardness algorithm for the derivation of a private key that would involve passage over unsecure network; the second key is the public key use for encryption and is therefore known by the public. The message is decrypted using both the public key and the private key. The first public-key encryption was the RSA proposed by Rivest Shamir and Adleman in 1977. The first discrete logarithm (DL) system which was a key agreement protocol was proposed by Diffie and Hellman in 1976. In 1984, ElGamal described DL public-key encryption and signature schemes. Elliptic curve cryptography which is the most recent was introduced in 1985.

Implementing a *public-key infrastructure* (PKI) for distributing and managing public keys can be a formidable challenge in practice. Data security is a tradeoff between transmission speed and processing time, some servers employ both symmetric and asymmetric key encryption at the same time to get the best of both worlds. For instance windows 2000 use both symmetric and asymmetric key cryptography simultaneously.

3. THE WEB AND ITS ADVERVARY

The World Wide Web (WWW) and the Internet are terms that are usually used interchangeably. However, there exists some subtle difference between the two schemes. The Internet is a computer network that consists of a worldwide network of computer networks that interconnected through the application of the Transmission Control Protocol/Internet Protocol (TCP/IP) network protocols that facilitates data transmission and exchange of packets. The web is one of the services that run on the Internet. Surveys have shown that more than 80 % of Internet traffic is for the Web Services. TCP/IP is a stand that enables different types of computers and networks on the Internet to communicate. TCP defines how data are transferred across the Internet to their destinations through communications devices called routers. IP defines how data are divided into chunks, called packets, for transmission; it also determines the path each packet takes between computers. Due to the decentralized nature of its growth, the Web has been widely believed to lack structure and organization as a whole [1].

During data exchange on the Internet and on the web precisely, some security compromise may take place. These security challenges include Confidentiality, Integrity and Availability (CIA) which are the principal components for Information Security watch words.

Data Confidentiality: There is the need to prevent eavesdropping of messages or data that is passing from one point to another. The data may be sensitive and confidential, thus, making it a prey to the adversaries. Data may be safeguarded through encryption policies or by authorization permits. Any intrusions of data without express permission override the confidentiality of the principle of confidentiality of the data.

Data Integrity: Data could be seen as a mean of maintaining and assuring the accuracy and consistent over the entire life cycle of transmission between the client and the receiver. This means that data should not be modified in an unauthorized or undetected fashion. Integrity is violated when a message is modified in transit by an adversary. Information security systems typically provide message integrity in addition to data confidentiality.

Data Availability: For any information system to serve measurable purpose, the information must be available when it is needed. This connotes that the computing systems used to store and process the information, the security controls used must be protected, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

Data Origin Authentication: There is need to prevent impersonating people or objects on the web. For instance if A sends message to B, it is important for B to verify that the message has really originated from A.

Data Autherization: Data should be accessible only to whom it is intended to. Thus mechanisms should be developed that would forestall the data and should be accessible to only those that are in mutual agreement of acceptance

Data Non-repudiation: It is important to attribute the origin of a message to some entity on the web in order to prevent an entity from denying previous commitments or action. When *B* receives a message allegedly from *A*, not only is *B* convinced that the message originated with *A*, but *B* can convince a neutral third party of this; thus *A* cannot deny having sent the message to *B*.

Data Denial of Service: An attack can be in the form of preventing or inhibiting the normal use or management of communication facilities. For example an entity may suppress all messages directed to a particular destination like security audit service.

According to [5] the aforementioned attacks can be classified into passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect the system resources. Passive attacks include eavesdropping or monitoring of transmissions in order to obtain information that is being transmitted. Passive attacks are difficult to detect because they do not change the data. Encryption can help prevent such attacks. An active attack attempts to alter system resources or affect their operation. Example of such attacks include message modification, denial of service, impersonating and entity and non-repudiation

3.1 Current Security Protocols on the Web

Hypertext Transfer Protocol (HTTP) is the foundation protocol of the World Wide Web used by any client/server application involving hypertext. The protocol transfers any accessible information on the web with enough efficiency to

allow for hypertext jumps. The most typical use of HTTP is between a Web browser and a Web server. TCP is the protocol that HTTP uses because of its reliability. However, it can also use unreliable protocols such as User Datagram Protocol (UDP). HTTP is a stateless protocol (each transaction is treated independently) and is flexible, this means that when a client issues a request to a server, it may include prioritized lists of formats that it can handle, and the server replies with the appropriate format.

The web uses the TCP/IP protocol depicted in Fig 1. Internet Protocol Security (IPsec), SSL/TLS and Secure Shell (SSH) are different types of security protocols that is used on the web. IPsec are a set of protocols developed by IETF (In this paper TLS and SSL will be used interchangeably) to support secure exchange of packets at the IP layer. It is rather an extension to the TCP/IP protocol suit; figure 1. IPSec is most widely used to implement Virtual Private Network (VPNs). Transport being less secure, encrypts only the data portion (payload) of the IP packets without the header while the Tunnel mode encryption encrypts both the header and the payload. IPSec-compliant device decrypts each packet on the receiving end. It is the lowest layer protocol of all the other security protocols

SSH is a UNIX-based security protocol and interface that provides a secure connection to a remote computer. SSH connects a server and a client running SSH server and SSH client programs respectively. SSH operates on the transport layer of the TCP/IP protocol suit. SSH uses RSA-public key cryptography for both connection and authentication and passwords are encrypted. The cryptographic system we have can be deployed in SSH as well as in TLS/SSL.

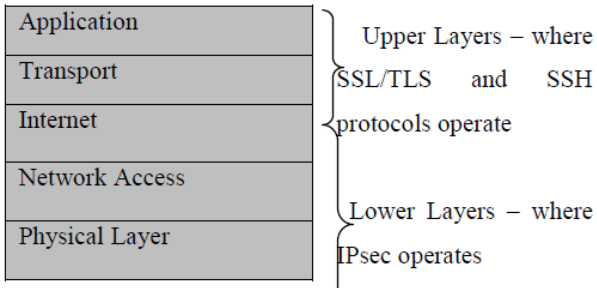

Figure1: TCP/IP Model

3.2 Transport Layer Security/ Secure Socket Layer (TLS/SSL) Protocols

The most common security protocols employed in the TCP/IP suit is the Secure Socket Layer and its successor the Transport Layer Security (TLS) which is the Internet standard defined as RFC 2246 [5]. The design of Transport Layer Security allows different algorithms to work either alone or side by side. However, the specification does recommend particular combinations of these algorithms called cipher-suits. For example a cipher-suite such as RSA-RC4-MD5 would indicate that RSA will be used for key exchange mechanism, RC4 for bulk-encryption and MD5 for hashing [8]. SSL provides secure communications over the The SSL Record Protocol provides basic security services to various higher layer protocols. HTTP is the most common application layer protocol that operates on SSL (HTTP running over SSL is termed HTTPS). The protocol is application independent – conceptually, any application that runs over TCP can also run over SSL [4]. Three higher layer protocols are defined as part of SSL: the Handshake protocol, the Change Cipher Spec Protocol, and the Alert Protocol. The Handshake protocol allows server and clients to authenticate each other and to negotiate an encryption and MAC (Message Authentication Code) algorithm and cryptographic keys to be used to protect data sent in an SSL Record. The Record Layer Protocol derives symmetric keys from the master key which are then used for bulk encryption and authentication of source data. The Change Cipher Spec Protocol contains a single message of one byte with value 1. The purpose of the message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection. The alert protocol is used to convey SSL-related alert to the peer. Elliptic Curves Cryptography-based SSL handshake is illustrated in Fig 3 above.

instant messaging, and email. The protocol relies on TCP and can be incorporated in the underlying protocol suit to be used by all applications or it can be implemented in specific packages. For instance, Microsoft Explorer and Netscape browsers come equipped with SSL, and most web servers have implemented the protocol. The SSL protocol operates above the Transport Layer but below the Application Layer protocols.

Two important concepts in SSL include the SSL session which is a peer-to-peer relationship that is transient and the SSL connection which is an association between a client and a server. Sessions define a set of cryptographic security parameters and are created by the Handshake protocol. SSL is two layers of protocol as shown in the Figure 2 below.

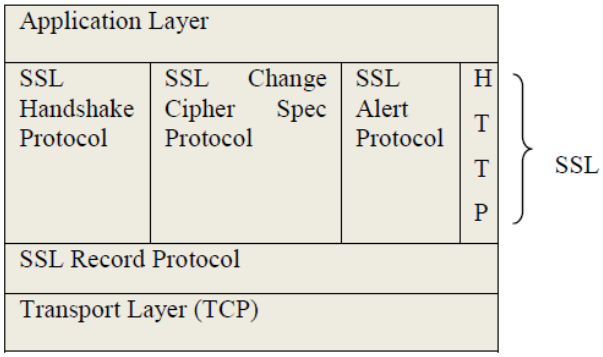

Fig 2: SSL Protocol Stack

The SSL Record Protocol provides basic security services to various higher layer protocols. HTTP is the most common application layer protocol that operates on SSL (HTTP running over SSL is termed HTTPS). The protocol is application independent –conceptually, any application that runs over TCP can also run over SSL [4]. Three higher layer protocols are defined as part of SSL: the Handshake protocol, the Change Cipher Spec Protocol, and the Alert Protocol. The Handshake protocol allows server and clients to authenticate each other and to negotiate an encryption and MAC (Message Authentication Code) algorithm and cryptographic keys to be used to protect data sent in an SSL Record. The Record Layer Protocol derives symmetric keys from the master key which are then used for bulk encryption and authentication of source data. The Change Cipher Spec Protocol contains a single message of one byte with value 1. The purpose of the message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection. The alert protocol is used to convey SSL-related alert to the peer. Elliptic Curves Cryptography-based SSL handshake is illustrated in Fig 3 above.

Client and Server negotiate a cipher suite through *ClientHello* and *ServerHello* messages. *ServerCertificate* message contains the server's ECDH public key signed by a certificate authority using ECDSA. Client's ECDH public key is sent to the server in the *ClientKeyExchange* message after validating the ECDSA signature. Afterwards each entity uses its own ECDH private key and the other's public key to perform an ECDH operation and arrive at a shared premaster secret [4].

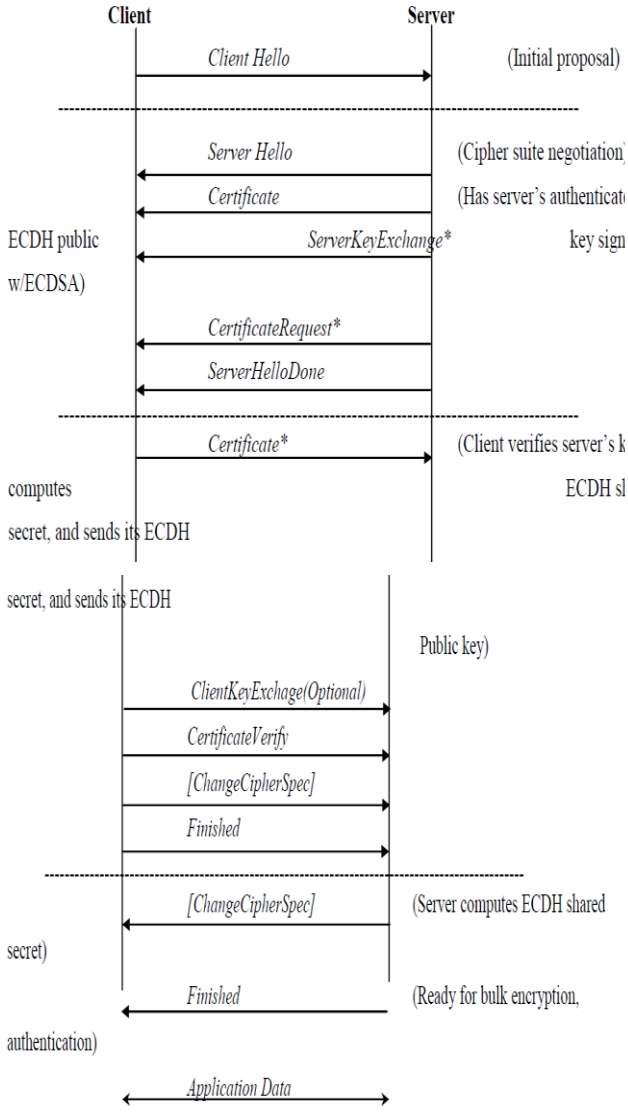

Fig 3: ECC –based SSL Handshake

4. ELLIPTIC CURVES CYPTOGRAPHY

Elliptic curve cryptography (ECC) was discovered in 1985 by Neal Koblitz and Victor Miller. Elliptic [7] curve cryptographic schemes are public-key mechanisms that provide the same functionality as RSA schemes. However, their security is based on the hardness of a different problem, namely the elliptic curve discrete logarithm problem (ECDLP). Currently the best algorithms known to solve the ECDLP is asymptotic that is based on probabilistic nondeterministic polynomial time (PNPT) [15] and have fully exponential running time, in contrast to the sub-exponential-time algorithms known for the integer factorization problem. [2] .

Desired level of security can be obtained with smaller key size in elliptic curve cryptography than with its RSA counterpart. For example, 256-bit elliptic curve key can provide the same level of security as a 3078-bit RSA key. Smaller key size gives rise to speed and efficient use of power, storage and bandwidth. Not every elliptic curve offers strong security properties thereby the standard organizations like NIST (National Institute of Standards Technology: A body that gives standard for the use of internet) and SECG (Standards for Efficient Cryptography Group) have published a set of recommended curves. Some curves can be solved in probabilistic polynomial time thereby could compromise security. The most recommended curves for use in the elliptic curve digital signature algorithm targeting five different security levels are given in this pattern; vize:

$$P192 = 2192 - 264 - 1;$$

$$P224 - 926 + 1$$

$$P256 = 2256 - 2224 + 2192 + 296 - 1$$

$$P384 = 2384 - 2128 - 296 + 232 - 1;$$

$$P521 = 2521 - 1:$$

Each curve is defined over a prime field by a generalized Mersenne prime [17, 18]. All curves have the same coefficient a = -3, supposedly chosen for efficiency reasons, and their group orders are all primes, meaning that $n = \#E(F_p)$ [9].

The basic operation in ECC is the point multiplication i.e. multiplication of an elliptic curve point P by an integer (denoted *e*P)* which yields another point on the curve. The Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) are the elliptic curve equivalence of Diffie-Hellman and DSA. In ECC, we have what is called the base point *P* which is fixed for each curve and is used to calculate the public key. A random integer k is chosen and is kept private and forms the secret key. The result of the multiplication Q = k* P forms the public key of the cryptosystem.

5. ECC IMPLEMENTATION IN TRANSPORT LAYER SECURITY

Elliptic curves can arise in several locations in the TLS protocol. The elliptic curve cipher suites for TLS are specified in RFC 4492 [9]. All of the cipher suites specified in this RFC use the elliptic curve Diffie-Hellman (ECDH) key exchange. The ECDH keys may either be long-term (in which case they are reused for different key exchanges) or ephemeral (in which case they are regenerated for each key exchange).

Eliptive Curve Diffie-Hellman (ECDH)

The two primary implementation of ECC is the implementation of the ECDH and ECDSA protocols in SSL. ECDH establishes a shared key between two parties by first agreeing on the *named curves* (parameters) to be used. The protocol is based on additive elliptic curve group. In this protocol, a curve E with parameters a, b and base point P is set up under some selected prime field or binary field. The order of the base point P is n. Communicating parties end up with the same value C at the end of the protocol. Such a value is a point on the curve and a part of it is used as a secret key to secret-key encryption algorithm.

ECDSA

An elliptic curve E defined over *GF(p)* or $GF(2^K)$ with large group of order *n* and a point *P* of large order is selected and made public to all users. Then, the following key generation

primitive is used by each party to generate the individual public and private key pairs. Furthermore, for each transaction the signature and verification primitives are used. ECDSA is briefly outlined in [2] below,

ECDSA Key Generation - The user A follows these steps:

INPUT: Elliptic curve domain parameters (p, E, P,n).

OUTPUT: Public key Q and private key d.

1. Select d ∈R [1,n−1].

2. Compute Q = dP.

3. Return(Q,d).

ECDSA Signature Generation - The user A signs the message m using these steps

INPUT: Domain parameters D = (q,FR, S,a,b, P,n,h), private key d, message m.

OUTPUT: Signature (r, s).

1. Select k ∈R [1,n−1].

2. Compute $kp = (x_1, y_1)$ *and convert* x_1 *to an integer* x_1

.3. Compute r = x1 mod n. If r = 0 then go to step 1.

4. Compute e = H(m).

5. Compute $s = k - 1(e + dr) \bmod n$ *If s = 0 then go to step 1.*

6. Return(r, s).

ECDSA Signature Verification-

INPUT: Domain parameters *D = (q*,FR, *S,a,b, P,n,h),* public key *Q*, message *m*,signature *(r, s).*

OUTPUT: Acceptance or rejection of the signature.

1. Verify that *r* and *s* are integers in the interval [1,*n*−1]. If any verification fails then return("Reject the signature").

2. Compute $e = H(m)$ *e = H(m).*

3. Compute $w = s^{-1} \bmod n$

4. compute $u_1 = ew \bmod n$ *and* $u_2 = ew \bmod n$

5. Compute $X = u_1 p + u_2 Q$

6. If $X = \infty$,

then return("Reject the signature");

7. Convert the *x*-coordinate *x*1 of *X* to an integer *x*1; compute *v* = *x*1 mod *n*.

8. If *v* = *r* then return ("Accept the signature");

Else return ("Reject the signature").

Why Elliptic Curves Cryptography?

There are a number of reasons that could be adduced in the applications of elliptic curves over other cryptographic schemes with attendant of such communication devices within the critical Internet infrastructures. Amongst them are:

Trends: Technology is becoming smaller like PDA's, Smart phones, embedded systems and etc. Most of these devices are built with limited resources (memory) and computational power. Most of these devices are connected and they communicate hence there is need for security in the communication. ECC provides relatively short encryption key and the keys grow only linearly for increased level of security. On the other hand, RSA keys grow exponentially for increased level of security; hence not good enough for such devices that have limited memory and computational power. This makes ECC the cryptosystem of choice for such devices in the future.

Scalability and Performance: Websites using ECC need fewer server processing cycles, allowing for more simultaneous SSL/TLS connections and faster page loading [6]. Experimental results indicate that the performance advantage of ECC over RSA increases at higher key sizes. The performance efficiency of ECC enables it to be incorporated into clients that range from mobile devices like PDA and cell phones to high end clients like PC's.[8]. This yields a more satisfying user experience and increase in throughputs (more jobs get done within a given time).

Demand for higher levels of security: As processor speeds increase and the number of Internet-connected devices grows, potential attackers will have more resources at their disposal to attack the cryptography used in secure connections. This will necessitate further increases in RSA key sizes and worsen the performance bottleneck. Already, 512-bit RSA is considered insecure and most transactions use 1024-bit keys. Before the end of this decade, RSA keys will need to grow to 2048-bits [3]. With this reason, ECC is a good choice to embrace for its shorter key size.

Compliance, Guidelines: The ECC algorithm is endorsed by the NSA (National Security Agency), and is compliant with the NIST 800-131A guidelines. A new guideline from NIST is to migrate from 1024-bit keys to 2048-bit keys as of 1/1/20141[1]. Furthermore, in parallel with the adjustment to the minimum key size by NIST, the US Government has issued and adopted guidelines for alternative algorithms for encryption and signing adding Elliptic Curve Cryptography (ECC) and Digital Signature Algorithms (DSA).[6]

Running Time of Algorithm: Of the three well known public key cryptosystem namely - integer factorization, discrete logarithm and elliptic curve discrete logarithm- elliptic curves cryptography has the most inefficient running time. The best known method of solving elliptic curve discrete logarithm problem is Pollard-rho algorithm and the running time is the square root of *n* ie fully exponential. Best known algorithms for integer factorization and discrete logarithm has sub exponential running time thereby making ECC cryptography the hardest to attack hence relatively less vulnerable.

5.0 A Structural Implementations of the ECC in Cloud Computing Cloud computing simply means accessing computing, software and storage power as 'a service' from a third party using a pay-as-you-go model. It eliminates the need for costly IT related investment and commitment on the part of the consumers [11]. Its "on demand" form allows consumers to adapt rapidly and less costly to fast changing IT usage. The hardware and software built can serve many users and provide multiple solutions, thereby, reducing operational cost for the providers. "Cloud computing is divided into three types according to the abstraction level of the capability

provided and service model of providers namely - Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Some technological advancement like hardware virtualization, utility computing, Web 2.0, Autonomic computing and Data Automation centre have paved way for the invention of cloud computing" [11].

Despite the numerous benefits of cloud computing a lot of consumers are still reluctant to migrate to it because of the security issues. Their concerns are justified given that they are not in control of their data when it is outsourced to the cloud. Businesses, organizations and governments parastatal are worried that their competitors may be sharing the same resources on the cloud which may gain unauthorized access to some sensitive information stored in the cloud. More so, consumers' data may be prone to malicious attackers.

There exist different proposed models for ensuring security on the cloud. [13, 16] have proposed a secure cloud storage framework (SCSF) using ECC based PKI (Public key infrastructure) that allows for secure storage and access of data as well as sharing the data with multiple users securely and also authenticate then with the ECDS. The framework divided the cloud storage into a private part where a user can store his unshared data and a shared part where a user can store the data he wishes to share with other authenticated users. "In both private data and shared data parts, user encrypts data using symmetric encryption algorithms with different session keys, and only in shared data part, users encrypt the session key using ECC public key algorithm with their private key, and also decrypt the encrypted session key using ECC public key algorithm with corresponding user's public key" [13]. This security model is illustrated in the diagram below:

Starting point

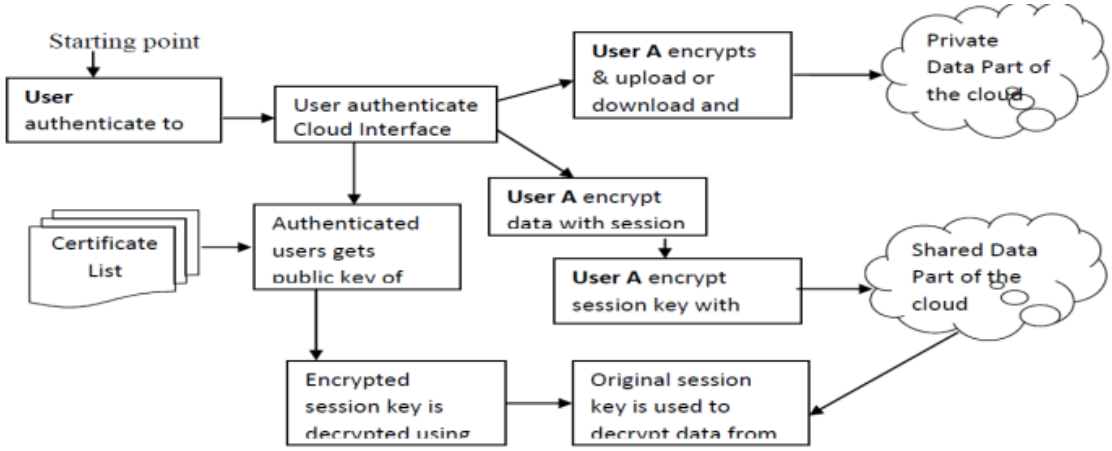

Figure 4: A Practical of secure Cloud Topology

Behind the implementation of all the schemes proposed above are the essential symmetric key and public key encryption schemes. The attribute based scheme, the TPM and host of other security mechanisms ultimately implement the symmetric key encryption and the public key encryption (ECC, RSA or ELGamal) algorithms. However, given the numerous benefits of ECC discussed in the last section, it has proven to be the cryptographic scheme of choice for the authentication, encryption and verification. Amongst the benefits of the ECC based over RSA based PKI mentioned in [13] includes comparable security as RSA with smaller key-length, less computation cost (ECC scalar point multiplication require less computational cost than RSA modular exponentiation operation) and less communication cost (ECC shorter key size reduces the message-size).

7.0 Suggestion for Future Research

The paper dealt generally the theoretical concepts of the Mobile cloud considerations. Therefore like in [16], where the security was done by simulations process; the security of Mobile cloud could further improve based on Android programming language with the ECC as the main algorithm. The research may further expanded into the comparison of ECC with the quantum cryptography (assuming the experimental tools are easily accessible)

8.0 Conclusion

Fig 4: A pictorial representation of Secured Cloud Storage Framework (SCSF) proposed by [13]

The Certificate authority is responsible for giving digital signature to users to certify the y and private key of the users.

Another security model is the Trusted Platform module (TPM) suggested to be used for security on the cloud by [14]. TPM is type of microprocessor that is created to give security infrastructure like secure cryptographic key generation, limitation to their use and random number generation.

Attribute based encryption schemes which are in many variant including Cipher Policy Attribute Based Encryption scheme (CP-ABE) and Key policy Attribute based encryption (KP-ABE) is another example of security schemes that exist. ABE is a form of public-key encryption where users are associated with some attributes for cryptographic access control. A user may be associated with one attribute, multiple attributes and many users may be associated with single attribute. The right combination of these attributes that matches the attributes of the cipher text allows a user to decrypt some messages [12]. This security scheme can be very useful in the cloud given that a user on the cloud may not know the exact identities of all other people who should be able to access the data, but rather he/she may only have a way to describe them in terms of descriptive attributes or credentials. Attribute Based Encryption gives the facility to do just that. For instance using attribute based encryption, employees of an organization can simply access some data just by having the attribute of being an employee in that organization thereby giving flexibility for the data access control.

Elliptic curves cryptography (ECC) is one of the public-key cryptographic algorithms. Though RSA is the most commonly applicable cryptosystem scheme nowadays for the web security, ECC may overtake it due to the proliferation of smaller devices and increasing security needs. ECC is used by SSL/TLS which are the premier web security protocols that could be suitable for mobile cloud algorithm due to its low cost in power consumption. SSL/TLS was originally developed for HTTP (main protocol for accessing the web) but is also used by other protocols such as FTP and SMPTP. As we move towards cloud computing and Internet of things(IOT) where smaller and more constrained devices like sensors, home appliances, personal medical devices may not have enough computational resources to use RSA as their cryptographic system.

Clear needs for an efficient public-key cryptosystem have been identified in this paper including lower capability threshold for smaller sized devices to perform strong cryptography and an increase in server's capacity to handle secure connections. Elliptic Curve Cryptography (ECC) promises to fulfill this need. This next-generation algorithm provides stronger security and better server utilization than current standard encryption methods, but requires shorter key lengths. It is important to be cautious of implementation problems that may bring about cryptographic vulnerabilities despite the security qualities offered by ECC. This is because most real world cryptographic vulnerabilities result from implementation issues like design flows, side-channel attack and software bugs and not from breaking the hardness of the problem [9]. Finally making use of the standard curves recommended by NIST help gives a stronger and reliable security in web communications either on the Cloud or otherwise.

6. REFERENCES

[1] Z. Brakerski, C. Gentry, And V. Vaikuntanathan,"(Leveled) Fully Homomorphic Encryption Without Bootstrapping," In Itcs, 2012

[2] Kleinberg, J. and Lawrence, S. (2001). The Structure of the Web. SCIENCE Vol. 294, Page 1849-1850 www.sciencemag.org. (30th March, 2014).Darrel, H., Menezes A., Vanstone S. (2004). Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc 2004. Volume 19 preface

[3] Gupta, V., Stebila, D., Shantz, S. C.(2004). Integrating elliptic curve cryptography into the web's security infrastructure.

[4] Gupta, V., Stebila, D., Fung, S., Shantz, S. C, Gura, N., Eberle, H. (2004). Speeding up Secure Web Transactions Using Elliptic Curve Cryptography. NDSS

[5] William S.(2007) Data and Computer Communications. Eight Edition, Pearson Prentice Hall.

[6] Ajay K., Antony J., Gaurav K., Hari V., Hoa L., Ning C., Rick A.(2013) White Paper: Elliptic Curve Cryptography (ECC) Certificates Performance Analysis.

[7] Koblitz, N. (1987). Elliptic Curve Cryptosystem. Journal of mathematics computation. 48, 177

[8] sharat. N. New Generation Cryptosystems using Elliptic Curve Cryptography.

[9] Joppe W. Bos, J., Alex H., Nadia H., Jonathan M., Michael N., Eric W.(2013)

[10] Elliptic Curve Cryptography in Practice. IACR Cryptology ePrint Archive 2013: 734 (2013)

[11] Vipul G., Sumit G., Sheueling C. S., Douglas S. (2002) Performance analysis of elliptic curve cryptography for SSL. Workshop on Wireless Security 87-94.

[12] Rajkumar B., James, B., Andrzej, G. (2001).Cloud Computing Principles and Paradigms.John Wisely, New Jersey

[13] Bethencourt . J., A. Sahai, and Waters.(. B. 2007).Cipher Policy Attribute-Based Encryption. IEEE Symposium on Security and Privacy, 321-334

[14] XiaoChun Y., ZengGuang L., Hoon J. L. (2014). An Efficient and Secured Data Storage Scheme in Cloud Computing Using ECC-based PKI. IEEE 16th International Conference on Advanced Communication and Technology (ICACT)

[15] 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 Computer Applications, Volume 66, No 23

[16] Jonathan K, Yehunde L. (2008), Introduction to Modern Cryptography; Chaman & Hall/CRC; Taylor and Francis Group; ISSN 978-1-58488-531-1 (all paper)

[17] Victor O. Waziri, Ojeniyi J. Adebayo, Hakimi Danladi, Audu Isah, Abubakar S. Magaji, Muhammad Bashir Abdullahi (2013):Network Security in Cloud Computing with Elliptic Curve Cryptography; Network Communication Technogies; Vol 2 No. 2, ISSN 1927-064X, E-ISSN 1927-0658; published by Canadian Center of Science Education

[18] Bell, E.T. and Mathematical Association of America (1951). Mathematics, queen and servant of science. McGraw-Hill New York. p. 228

[19] Maugh II, Thomas H. (2008-09-27). "UCLA mathematicians discover a 13-million-digit prime number". Los Angeles Times. Retrieved 2011-05-21.