Open Access Library Journal
2016, Volume 3, e2802
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Fog Computing: Comprehensive Approach for Security Data Theft Attack Using Elliptic Curve Cryptography and Decoy Technology

Mai Trung Dong, Xianwei Zhou

Department of Communication Engineering, School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, China
Email: maitrungdong44@gmail.com, 2605473996@qq.com

How to cite this paper: Dong, M.T. and Zhou, X.W. (2016) Fog Computing: Comprehensive Approach for Security Data Theft Attack Using Elliptic Curve Cryptography and Decoy Technology. *Open Access Library Journal*, **3**: e2802.
http://dx.doi.org/10.4236/oalib.1102802

Received: August 6, 2016
Accepted: September 6, 2016
Published: September 9, 2016

Abstract

Fog computing extends cloud computing, provides the services like data, compute, storage and application to end user. It improves the quality of service and also reduces latency. According to Cisco, due to its wide geographical distribution, the Fog computing is well suited for real time analytics and big data. This article, by exploitation advantages of Fog computing Paradigm, analyzes its applications in a series of real scenarios, such as Smart Grid, smart traffic lights in vehicular networks, Wireless Sensor and Actuator Networks, Decentralized Smart Building Control, IoT and Cyber-physical systems and software defined networks, and reviews Comprehensive Approach for security Data Theft Attack the use of Elliptic Curve Cryptography (ECC) and decoy technology in such a constrained environment along with the other two aspects of ECC, namely its security and efficiency. In the article, the performance of ECC is compared with the other PKC applications which should prove that ECC performs well and is more suitable for Fog environments.

Subject Areas

Cloud Computing, Computer and Network Security, Information and Communication Theory and Algorithms

Keywords

Fog Computing, Elliptic Curve Cryptography (ECC), Network Security, Public-Key Cryptosystem (PKC), Rivest-Shamir-Adleman (RSA)

1. Introduction

Elliptic curves are rich mathematical structures that have shown usefulness in many

different types of applications. It was proposed for use as the basis for discrete logarithm-based cryptosystems, independently by Neal Koblitz of the University of Washington and Victor Miller of IBM. Elliptic curves were already being used in various cryptographic contexts. ECC has the upper hand in the efficiency of algorithm. Some devices have limited processing capacity, bandwidth, storage, and power supply like the newer wireless devices and cellular telephones. When used, efficiency of the resource use is very important in these devices. Elliptic Curve Cryptography provides encryption functionality requiring a smaller percentage of the resources required by other algorithms, so it is used in these types of devices. In most cases, the longer the key length, the more protection that is provided, but ECC can provide the same level of protection with a smaller key size than RSA. Since smaller keys as in ECC require fewer resources of the device to perform the mathematical tasks. ECC cryptosystems use the properties of elliptic curves in their public key systems. The elliptic curves provide ways of constructing groups of elements and specific rules of how the elements within these groups combine. The properties between the groups are used to build cryptographic algorithms.

Security and privacy issues are further disclosed according to current Fog computing paradigm. As an example, we study a typical attack, man-in-the-middle attack, for the discussion of security in Fog computing [1]. We investigate the stealthy features of this attack by examining its CPU and memory consumption on Fog device.

To further increase the safety of the system, we propose the approach Elliptic Curve Cryptography encryption which is good for sensitive data protection and the decoy technology for insider data protection from theft attack in Fog computing.

The organization of the paper is as follows. In Section 2, we review the ECC for portable devices and its application to affirm ECC accord for Fog computing Paradigm. In Section 3, we review ECC algorithms, key exchange of modality, digital signatures. In Section 4, we present experimental results by comparing RSA and ECC, result of User Model for the Search Profiling. We conclude the paper in Section 6.

2. Literature Review and Related Work

The difference between ECC and other conventional cryptosystems is that for a well-chosen curve, the best method currently known for solving the Elliptic curve discrete logarithm problem (ECDLP) is fully exponential, while sub-exponential algorithms exist for conventional cryptosystems. This difference largely contributes to the large disparities in their respective running times. It also means that ECC keys have much fewer bits than Discrete Logarithms Problem and Integer Factorization Problem based applications. There is currently no faster way to attack the ECDLP other than fully exponential algorithms (*Security Test by Certicon Pvt. Ltd.*).The contrast in key lengths of RSA, DSA and ECC are shown in the graph **Figure 1**.

2.1. ECC for Portable Devices and Its Application

In 1985. ECC has yielded highly efficient and secure When the ECC was first introduced.

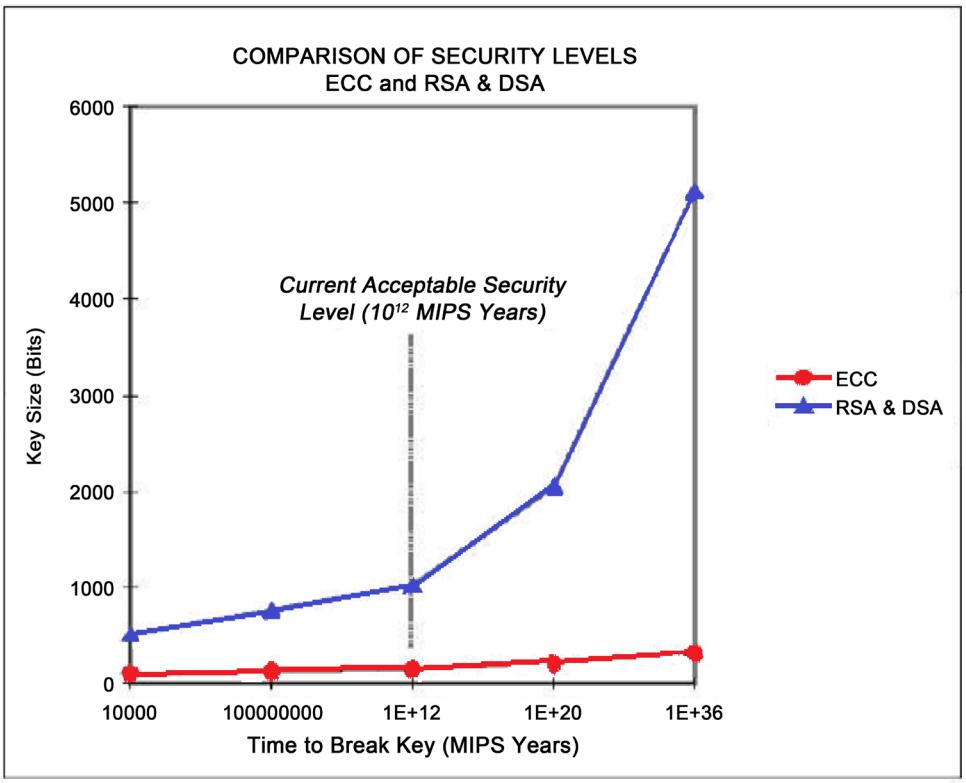

Figure 1. Comparative study of ECC and RSA/DSA.

Presently, many product vendors have incorporated ECC in their products, RSA Security has researched on efficient ECC algorithms, and even acquired a patent on a storage-efficient basis conversion algorithm. Moreover, it has also integrated ECC into some of its products, acknowledging the fact that ECC has begun to establish itself as both secure and efficient.

The incorporation of Elliptic Curve Digital Signature Algorithm in several government and major research institution security standards, including IEEE P1363, ANSI X9.62, ISO 11770-3 and ANSI X9.63. Another factor is the strong promotion of the use of ECC through a Canadian-based Certicom Corporation that specializes in information security solutions in a mobile computing environment through providing software and services to its clients. Now, ECC is becoming the mainstream cryptographic scheme in all mobile and wireless devices. Below is a short survey of ECC applications found in the market at present. Results of the survey can be broadly divided into categories: the PDAs, smart cards, internet, and PCs. as the as the applications of Fog computing.

SUN Microsystems company contributed to the implementation of an ECC cryptographic library and also a common hardware architecture for accelerating ECC (as well as RSA) to be used in open Secure Sockets Layer (SSL) In September of 2002, Open SSL is a developmental toolkit for the implementation of SSL and Transport Layer Security protocols, which are commonly used today in over-the-web transactions and secure document transfers. The company hopes to promote ECC standardization with SSL,

which is the dominant security protocol used on the web today.

The Treasury Department's Bureau of Engraving and Printing completed a four-month e-commerce pilot program involving the use of smart cards and ECC with Secure Electronic Transaction (SET) specifications in late 1998. SET is a standard that enables secure credit card transactions over the Internet. The pilot program tested the use of smart cards, embedded with ECC technology, in making online purchases. This program involved a total of nine companies, including MasterCard, Certicom who supplied the ECC algorithms, Digital Signature Trust Co. who supplied the MasterCard smart cards and Globe Set is a SET vendor, … Smart cards are very flexible tools and can be used in many situations. Smart Cards are one of the most popular devices for the use of ECC. Many manufacturing companies are producing smart cards that make use of elliptic curve digital signature algorithms. These manufacturing companies include Phillips, Fujitsu, MIPS Technologies and Data Key, while vendors that sell these smart cards include Funge Wireless and Entrust Technologies.

Because PDAs (*Personal Digital Assistant*) have more computing power compared to most of the other mobile devices, like cell phones or pagers they are considered to be a very popular choice for implementing public key cryptosystems. However, they still suffer from limited bandwidth and this makes them an ideal choice for using ECC. In the1998, 3Com4 Corporation teamed up with Certicom to implement ECC in future versions of its Palm Pilot organizer series and Palm Computing platform. This new feature will provide protection of confidential information on the hand-held organizers, user authentication in wireless communications and e-commerce transactions, and also ensure data integrity and proof of transactions.

Constrained devices have been considered to be the most suitable platforms for implementing the ECC. PC Guardian Technologies is one such company that created the Encryption Plus Hard-Disk and Encryption Plus Email software products. The former makes use of both RSA and ECDH while the latter makes use of a strong 233- bit ECC key to encode its private AES keys.

The Top Secret Messenger software was developed by Encryption Software Inc. It encodes the messages of some of the most popular instant messaging programs today, like ICQ and MSN. It can also be used with e-mail clients such as Microsoft Outlook and Outlook Express to encode e-mail messages. This product uses both private and PKC, including a 307-bit key for its implementation of the ECC.

ECC [2] is emerging as an attractive public-key cryptosystem for mobile/wireless environments. ECC proposes equivalent security with smaller key sizes, compared to conventional cryptosystems like RSA, which results in faster computations; reduced power consumption, as well as savings in memory space and bandwidth. Since mobile devices have limited CPU, power and network connectivity ECC is especially useful. However, to evaluate any public-key cryptosystem it is needed to analyze its impact in the context of a security protocol. This paper presents a analysis of the performance enhancements that can be expected in SSL, the dominant security protocol on the Web at present, by adding ECC support.

In paper [3], the authors proposed the authentication protocol using ECC in resource constrained mobile devices with reasonable performance compared to RSA. The protocols based on this ECC asymmetric cryptography can be directly used in mobile devices. This is addressed to the design of a protocol based on ECC asymmetric cryptography. An implementation for J2ME Wireless Tool Kit 2.5.1 is also described. This work is to be a large contribution to the development and widespread acceptance of m-commerce.

Controller Pilot Data Link Communications (CPDLC) is an Aeronautical Telecommunication Network (ATN) ground and air application that allows a direct exchange of text-based messages between Air Traffic Service (ATS) the aircraft and ground system. For the ground system to provide data link services to an aircraft, the first step in the connection management chain is the logon. It takes one logon from the aircraft to allow a ground system to connect with CPDLC application. The logon serves a number of purposes: providing an ATS unit with the type of applications supported by the avionics. For those reasons, data link security problem consists of two applications, the Context Management (CM) and the CPDLC. The CM-logon service allows the CM-air-user to initiate data link service and provides information on each data link application for which it desires a data link service. The CM-ground-user responds indicating whether or not the CM-logon was successful, and if successful, includes information on each data link application it can support.

Once a dialogue is established, CPDLC allows for the direct exchange of text-base message between a controller and a pilot. Thus, in the proposed elliptic curve based authentication protocol, the CM application is used to manage mutual authentication during initial contact, and subsequent CPDLC application messages are authenticated using ATN keyed message authentication code scheme. The protocol depends on the security of the elliptic curve primitives. These operations utilize the arithmetic of points which are element of the set of solutions of an elliptic curve defined over a finite field. The use of ECC techniques provides greater security using fewer bits, resulting in a protocol which satisfies the primary considerations (namely bandwidth and computation on straints) for the aeronautical information security.

In paper [4], firstly, the authentication entities which do not rely on the concrete heterogeneous network are abstracted by analyzing 3G-WLAN multi-kind he heterogeneous network model. And then a general authentication model is established and a new access authentication and key agreement method combined ECC techniques with public key method is proposed. In this scheme, encryption data uses the smaller key length ECC with the similar security coefficient, and authentication information is marked. Further, the encryption/decryption and signature algorithm are carefully selected and enhanced. Hence mobile device computation overhead is reduced. Finally, the analysis of security shows that the proposed scheme satisfies the security characteristics such as joint authentication, key control, key confirmation, confidentiality of the critical data, non-repudiation, data integrity, resistance to replay attack. And the analysis of performance also shows that the proposed scheme is efficient in regard to computation and communication overheads.

ECC for wireless devices and its applications Although the discrete logarithm problem was first deployed by Diffie and Hellman was defined precisely as the problem of finding logarithms with respect to a generator in the multiplicative group of the integers modulo a prime, this method can be enhanced to arbitrary groups and, specially, to elliptic curve groups. The elliptic curve public-key systems provide relatively small block size, high speed, and high security. The primary advantage that elliptic curve systems have over systems based on the multiplicative group of a finite field is the absence of a sub exponential-time algorithm that could find discrete logs in these groups. Consequently, we can use an elliptic curve group which is smaller in size while retaining the same level of security. Also in RSA cryptosystem, the security increases sub exponentially whereas in elliptic curve cryptosystem, the security increases directly exponentially. The consequence is smaller key sizes, bandwidth savings, and faster implementations features which are especially attractive for security applications where computational power and integrated circuit space is limited, such as smart cards, PC (personal computer) cards, and wireless devices.

In paper [5], the author security issues in WSNs and study the behavior of WSN nodes that perform PKC public key operation. We evaluate time and power consumption of cryptography algorithm for signature and key management by simulation.

In [6], one of the most secure classical ciphers is the One Time Pad (OTP). But the drawback of this cipher is the inconvenient key to be used and to be maintained by the receiving party in order to recover the transmitted message. Also, the fact that the key-size is equal or of the same order as the message size, puts a limit on the size of the message to be transmitted. This limits the capability of OTP by forcing this scheme to be used only for transmitting extremely short messages like passwords. Because of the extremely good cryptographic security provided to the messages, it is desirable to extend OTP to large messages as well. This paper discusses a technique where public key and the private key are generated with help of a Lychrel number and an Elliptic curve algorithm over a finite field. The Algorithm has the nature of OTP and also supports the encryption of longer messages.

This work explains a cost effective PKC based solution for security services like key-distribution and authentication which are required for wireless sensor networks. The author proposes a custom hardware assisted approach to implement ECC in order to obtain stronger cryptography as well as to minimize the power. Their compact and low-power ECC processor contains a Modular Arithmetic Logic Unit for ECC field arithmetic. The best solution has 6718 gates for the MALU and control unit (data memory not included) in 0.13 μm CMOS technology over the field F2131, which provides a reasonable level of security for the time being.

Here the consumed power is less than 30 μW when operating frequency is 500 kHz. In paper [7], they investigate the possibility for PK services for pervasive computing. They show that ECC processors can be designed in such a way to qualify for lightweight applications suitable for wireless sensor networks. Here, the term lightweight assumes low die size and low power consumption. Therefore, they propose a hardware processor

supporting ECC that features very low footprint and low-power.

By using ECC, it has been lately shown that PKC is feasible on resource-constrained nodes. This feasibility, however, does not essentially mean attractiveness, as the obtained results are still not satisfactory enough. In paper [8], the author present results on implementing ECC, as well as the associated emerging field of Pairing-Based Cryptography, on two most popular sensor nodes. By doing that, he show that PKC is not only viable, but in fact attractive for WSNs. As far as pairing computations presented in this paper are the most efficient results on the MICA2 (8-bit/7.3828-MHz ATmega128L) and Tmote Sky (16-bit/8.192-MHz MSP-430) nodes.

2.2. Modeling User Behaviors and Decoy Technology

In 2011 Malek Ben Salem *et al.* [9] [10] defined Masquerade attacks lare a serious computer security problem like identity theft and fraud. They conjecture that individual users have unique computer search behavior which can be profiled and used to detect masquerade attacks. The behavior captures the types of activities that a user performs on a computer and when they perform them. The use of search behavior profiling for masquerade attack detection permits limiting the range and scope of the profiles they compute about a user, thus limiting potentially large sources of error in predicting user behavior that would be likely in a far more general setting. In 2012, Salvatore J. Stolfo *et al.* [11] explained a novel approach to securing personal and business data in the Cloud. They propose monitoring data access patterns by profiling user behavior to determine if and when a malicious insider illegitimately accesses someone's documents in a Cloud service.

3. Proposed System

The proposed system is the algorithm given in [12] [13] and using ECC instead of RSA. Decoy technology which removes the problem of user authentication in Fog Computer. While the advantage of using ECC is, it provides equivalent security level as RSA in less key size. Due to which any system will require less power for computation which is useful for the devices used in *Fog computing Paradigmas well as the ones in cloud computing*. The comparative **Table 1** for key size of RSA and ECC is given below [14].

After careful analysis the system has been identified to have the following modules and System Architecture (**Figure 2**):

1) ECC encryption and decryption(Diffie-Hellman key exchange)
2) User Behavior Profiling
3) Decoy documents.

Elliptic Curve over real numbers is the curve with following equation of the form:

$$y^2 = x^3 + ax + b, \quad (a,b) \in R$$

Elliptic Curve over the field Z_p is the curve with the coefficients in Z_p and in the form:

$$y^2 \bmod p = \left(x^3 + ax + b\right) \bmod p, \quad (a,b,x,y) \in Z_p$$

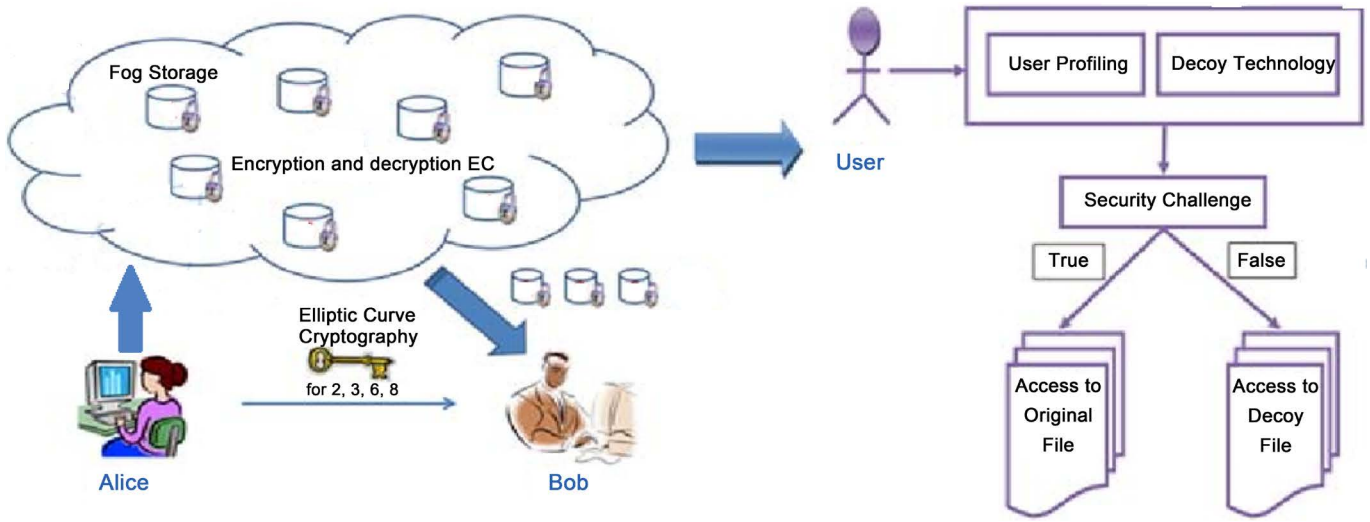

Figure 2. System architecture.

Elliptic Curve over the field $GF(2^m)$ is the curve with the coefficients in $GF(2^m)$, the formulation of this curve is different from that of the curve over the field Z_p.

$$y^2 + xy = x^3 + ax + b, \quad (a, b, x, y) \in GF\left(2^m\right)$$

Elliptic Curve Crytography (ECC) [15]

One-way function for Elliptic Curve Crytography is created as follows:

In the group of Abel $E_p(a, b)$ created from Ellipic curve over the field Z_p, consider the equation:

$Q = P + P + \cdots + P = kP$ (Q is the total of k P points, $k < p$)

With K and P, calculating Q can be done easily. However, if giving P and Q, it is hard to calculate k. This is the discrete logarithm of Elliptic curve.

Diffie-Hellman key exchange

We use the same one-way function of Elliptic Curve to consider a Diffie-Hellman key exchange protocol.

First we choose a big integer q, where q is a prime number (if using Elliptic Curve over the field Z_p) or q is in the form of 2^m (if choosing Elliptic Curve over the field $GF(2^m)$, and choose 2 corresponding parameters a, b to form a group of $E_q(a, b)$. It is called G base points of the group if there is an integer n so that $nG = 0$. The smallest integer n is called the grade of G.

In Diffie-Hellman key exchange, we choose a G point with high grade of n, and the key exchange protocol between Alice and Bob is operated as follows:

1) Alice chooses a number $n_A < n$ and keeps it in secret. Then in $E_q(a, b)$, she calculates $P_A = n_A G$ and sends P_A to Bob.
2) Similarly, Bob chooses a number n_B, calculates P_B and sends P_B to Alice
3) Alice creates a secret session key as $K = n_A P_B = n_A n_B G$
4) Bob creates a secret session key as $K = n_B P_A = n_B n_A G = n_A n_B G$ (Abel group is commutative) as same as Alice's key.

Trudy can intercept P_A and P_B, but can calculate only

P_A *and* $P_B = n_A G + n_B G = (n_A + n_B) G$

In order to calculate $K = n_A n_B G$, Eve must find n_A, n_B *from* P_A, P_B *and* G. However, this is impossible.

Elliptic Curve Digital Signature Algorithm Signing

For signing a message M by sender Alice, using Alice's private key d

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 $r = x_1 \pmod n$, where $(x_1, y_1) = k * G$. *If* $r = 0$, go to step 2
4) Calculate $s = k - 1(e + dr) \pmod n$. *If* $s = 0$, go to step 2
5) The signature is the pair (r, s)

Elliptic Curve Digital Signature Algorithm Verification

For Bob to authenticate Alice's signature, Bob must have Alice's public key Q

1) Verify that r and s are integers in [1, $n - 1$]. If not, the signature is invalid
2) Calculate $e = HASH(M)$
3) Calculate $w = s - 1 \pmod n$
4) Calculate $u_1 = ew \pmod n$ & $u_2 = rw \pmod n$
5) Calculate $(x_1, y_1) = u_1 * G + u_2 * Q$
6) The signature is valid *if* $x_1 = r \pmod n$

ECC Encryption and Decryption

Similar to the key exchange, when encrypting/decrypting, we also choose the parameters to create group Abel $E_q(a, b)$ and choose one G base point with high grade of n.

The private and public key components in EC encryption is defined as follows:

$$K_R = (d, G, q, a, b)$$

$$K_U = (E, G, q, a, b)$$

where $d < n$ and $E = dG$, d is a secret number selected by the key creator. Due to the nature of the one-way function, d can not be derived from E and G. Since then, there are two ways to implement encryption/ decryption as follows:

- Elgamal method:

Assuming that Alice wants to send message M to Bob. First, Alice switches from bit sequence form to point form $P_M = (x, y)$. CM code (using Bob's public key) is counted as a pair of point:

$$C_M = (kG, P_M + kE)$$

where k is a random number chosen by Alice

To decryption using the private key, Bob will multiply the first point in C_M with d, then take the second point to minus the result of:

$$P_M + kE - dkG = P_M + kdG - kdG = P_M$$

In the decryption protocol, Alice already hide P_M by adding P_M to kE. To decrypting, Bob need to take kE away. In stead of directly sending k to Bob to calculate kE (Eve can intercept), Alice sends kG signal. Based on kG and d, Bob can calculate kE. And Eve,

although she knows G and kG, she still can not calculate k due to the nature of one-way function.

- Menezes-Vanstone method:

Alice's M message is divided into 2 parts $M = (m_1, m_2)$ such that $m_1, m_2 \in Z_p$ Alice chooses one random number k, combines with Bob's public key, Alice can calculate P point as follows:

$$P\left(x_P, y_P\right) = kE$$

C_M code consists of three main parts:

$$C_M = \{c_1, c_2, c_3\} = \{kG, x_P m_1 \bmod p, y_P m_2 \bmod p\}$$

To decrypt using the private key from kG signal, Bob calculates:

$$P\left(x_P, y_p\right) = dkG$$

since then, calculates the inverse of x_p^{-1} and y_P^{-1} in modulo p. Finally, the code is as follows:

$$M = \{m_1, m_2\}\left\{x_p^{-1}c_1 \bmod p, y_P^{-1}c_2 \bmod p\right\}$$

Similar to Elgamal method, in spite of knowing GvàkG, Eve also can not calculate k and P.

- User Profiling: User profiling is a recognised technique that can be applied here to model how, when, and how much a user accesses their information in the Fog. Such 'normal user' behavior can be unceasingly checked to determine whether anomaly access to a user's information is occurring [16].

- Decoys: Decoy information, like decoy documents, are delivered to the attacker when an unlicensed access is detected. The file which sent to attacker is in encoded format. However, when adversaries try to use the system, they are absolutely attracted towards decoy information as their job is to explore sensitive data and steal it for financial and other benefits. The decoy technology is very useful as it deceives malevolent insiders. When the decoy technology is used along with user profiles, it is achievable to know the suspected behavior of users and that way it is achievable to prevent insider data theft attacks. This way the proposed application deceives malicious users to behave that way and avoid insider theft attack. The experimental results revealed that the combination of both the techniques such as user profile management and also the decoy technology could yield best results [17].

4. Experimental Results

Proposed system assures that man-in-middle attack is possible only when users are not authenticated and in proposed system, it's first authenticating user and then only allowing him/her to communicate with other users. The authentication is provided by using public key cryptography and decoy technology. In this public key cryptography is implemented using both conventional cryptosystems like RSA and ECC to verify which algorithm is going to consume more amount of resources. From the results, it is conclude

that ECC is far better than RSA for resource constrained devices as for Fog devices.

The Test command can be selected and some text is inserted to encrypt and decrypt. The application shows the algorithm used, the original text inserted, the encrypted text and the same text after decryption. Time can also be seen that is taken to make the whole operation in milliseconds (Figure 3).

The main focus of the article is to verify whether the Elliptical Curve Cryptography is better for fog environments like mobile phones than RSA.

There are three different characteristics that were decided to compare between these two cryptographic algorithms, namely performance, security and space requirements.

1024-bit RSA key has roughly the same strength as a 160-bit ECC key, and a 2048-bit RSA has about the same strength as a 210-bit ECC key. Based on this comparison was made with the speed and memory space of 2048-bit RSA operations to 210-bit ECC, 1024-bit RSA operations to 160-bit ECC, 768-bit RSA operations to 132-bit ECC and 512-bit RSA operations to 106-bit ECC. And the results are shown in Table 1.

In Figures 4-6: Graphs were drawn based on a series of results, where encryption strength is taken from 10 bits to 4086 bits.

Based on the graphs drawn above on different aspects like key generation time, memory space and encrypt/decrypt time comparing conventional cryptosystems like RSA and ECC, we can say that ECC is far better for Fog computing.

In Figure 7, user profiles are accurate enough to detect unauthorized access. It is represented horizontal axis is user number and vertical axis shows the AUC. When

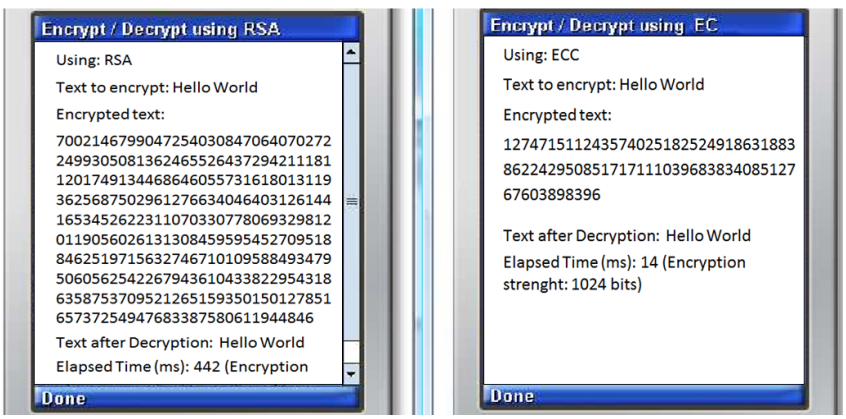

Figure 3. Encryp/Decrypt using RSA and ECC for comparison.

Table 1. Comparison of ECC and RSA.

ECC Key Size	RSA Key Size	ECC Key Generation Time	RSA Key Generation Time	ECC Memory Requirement	RSA Memory Requirement	ECC Encrypt /Decrypt Time	RSA Encrypt /Decrypt Time
106 bits	512 bits	57 ms	383 ms	108 bytes	157 bytes	11 ms	77 ms
132 bits	768 bits	98 ms	889 ms	117 bytes	236 bytes	17 ms	160 ms
160 bits	1024 bits	108 ms	2609 ms	125 bytes	313 bytes	16 ms	388 ms
210 bits	2048 bits	121 ms	18399 ms	140 bytes	621 bytes	15 ms	1867 ms

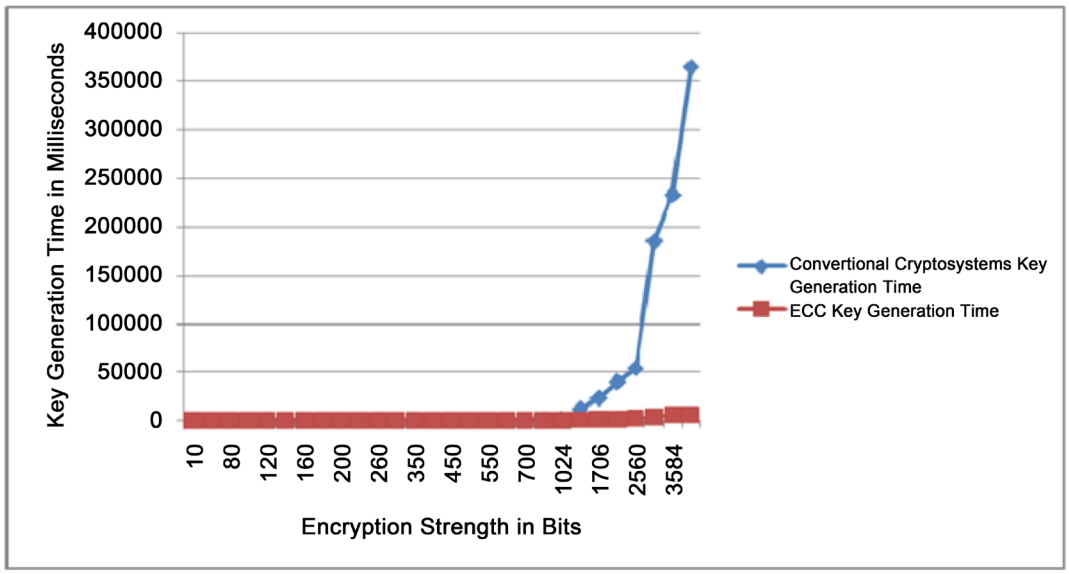

Figure 4. Comparison of conventional cryptosystems like RSA and ECC key generation time.

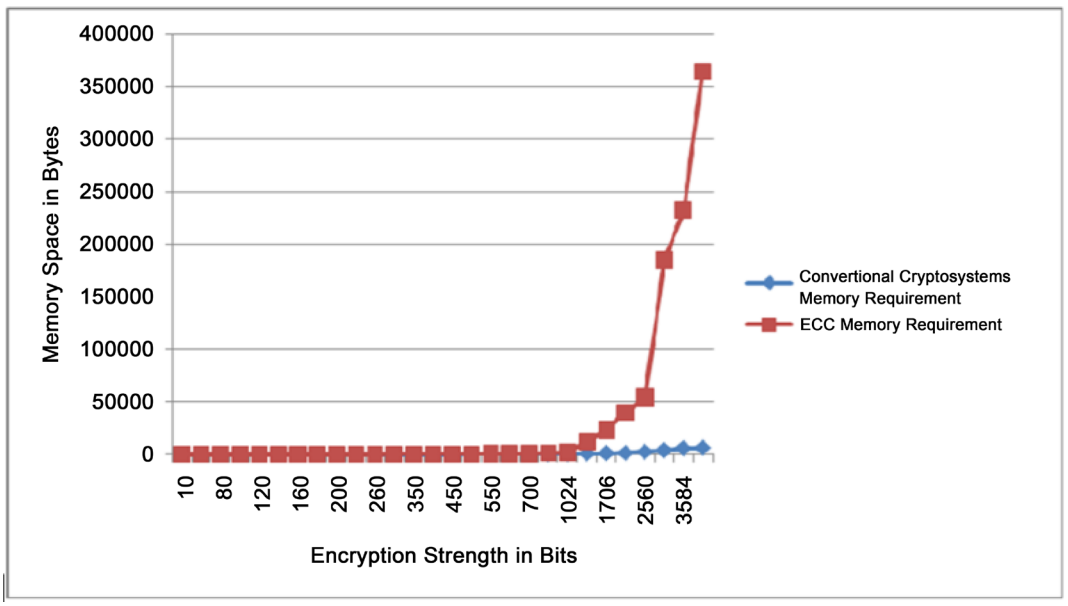

Figure 5. Comparison of conventional cryptosystems like RSA and ECC memory requirement.

such unlicensed access is detected, one can react by presenting the user with a challenge question or with a decoy document to validate whether the access was indeed unlicensed, similar to how we used decoys in a local file setting, to validate the alerts issued by the abnormality detector that monitors user file search and access behavior.

5. Conclusion

The basic idea is that we can limit the damage of stolen data if we decrease the value of that stolen information to the attacker. We can achieve this through a "preventive" disinformation attack and combining with ECC is a method to perform encryption for

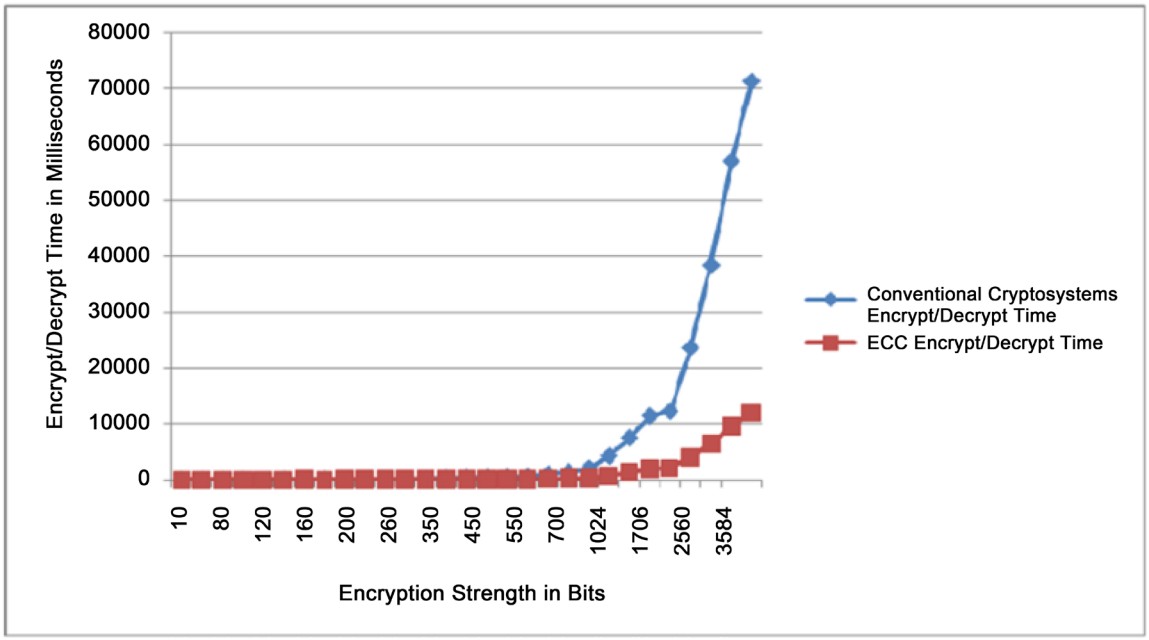

Figure 6. Comparison of conventional cryptosystems like RSA and ECC encrypt/decrypt time.

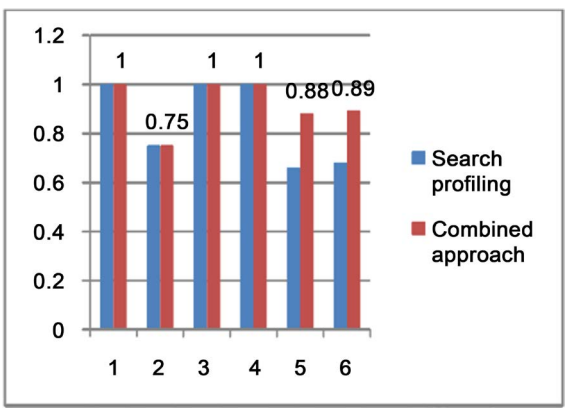

Figure 7. AUC comparison by user model for the search profiling.

application devices of Fog computing and to secure image transmission over internet. Elliptic curves are believed to provide good security with smaller key sizes, something that is very useful in many applications. Smaller key sizes may result in faster execution timings for the schemes, which is beneficial to systems where real time performance is a critical factor. We present these comparisons illustrate the appeal of elliptic curve cryptography especially for applications of Fog computing that have high security.

References

[1] Stojmenovic, I. and Wen, S. (2014) The Fog Computing Paradigm: Scenarios and Security Issues. *Proceedings of the* 2014 *Federated Conference on Computer Science and Information Systems*, **2**, 1-8. http://dx.doi.org/10.15439/2014F503

[2] Kumar, A., Jerome, A., Khanna, G., Veladanda, H., Ly, H., Chai, N. and Andrews, R. (2013) Elliptic Curve Cryptography (ECC) Certificates Performance Analysis. *Symantec Corpora-*

tion World Headquarters, 350 Ellis Street Mountain View, CA, May 2013. www.symantec.com

[3] Gayoso Martinez, V., Hernandez Encinas, L. and Sanchez Avila, C. (2009) Elliptic Curve Cryptography. Java Platform Implementations. *Proceedings of the International Conference on Information Technologies* (*InfoTech*-2009), Bulgaria, 17-20 September 2009, Vol. 1.

[4] HouhuifangJixinsheng, Houhuifang Liu guangqiang (2008) A Novel Access Authentication Scheme Based On ECC For 3G-WLAN Interworking Network. *IEEE International Conference on Computer Science and Software Engineering* 2008.

[5] Amin, F., Jahangir, A.H. and Rasifard, H. (2008) Analysis of Public-Key Cryptography For Wireless Sensor Networks Security. *World Academy of Science*, *Engineering and Technology*, 31 July 2008.

[6] Karuna Kamath, K. and Shankar, B.R. (2010) One Time Pad via Lychrel Number and Elliptic Curve. *International Journal of Computational and Applied Mathematics*, **5**, 157-161.

[7] Batina, L., Mentens, N., Sakiyama, K., Preneel, B. and Verbauwhede, I. (2006) Low-Cost Elliptic Curve Cryptography for Wireless Sensor Networks. *ESAS* 2006, LNCS 4357, Springer-Verlag Berlin Heidelberg, 6-17.

[8] Szczechowiak, P., Oliveira, L.B., Scott, M., Collier, M. and Daab, R. (2005) NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks. CAPES (Brazilian Ministry of Education) grant 4630/06-8 and FAPESP grant 2005/00557-9.

[9] Ben-Salem, M. and Stolfo, S.J. (2011) Modeling User Search-Behavior for Masquerade Detection. In: *Proceedings of the* 14*th International Symposium on Recent Advances in Intrusion Detection*, Springer, Heidelberg, 1-20.

[10] Li, J., Chen, X.F., Li, M.Q., Li, J.W., Lee, P.P.C. and Lou, W.J. (2014) Secure Deduplication with Efficient and Reliable Convergent Key Management. *IEEE Transactions on Parallel And Distributed Systems*, **25**, 1615-1625.

[11] Stolfo, S.J., Ben Salem, M. and Keromytis, A.D. (2012) Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud. *IEEE Symposium on Security and Privacy Workshop* (*SPW*), 24-25 May 2012. http://dx.doi.org/10.1109/SPW.2012.19

[12] Kalpana, P., *et al.* (2012) Data Security in Cloud Computing using RSA Algorithm. *International Journal of Research in Computer and Communication Technology*, *IJRCCT*, **1**, 143-146.

[13] Kaur, A. and Singh, S. (2013) An Efficient Data Storage Security Algorithm Using RSA Algorithm *International Journal of Application or Innovation in Engineering & Management* (*IJAIEM*), **2**, 536-540.

[14] Bafandehkar, M., MdYasin, S., Mahmod, R. and Hanapi, Z.M. (2013) Comparison of ECC and RSA Algorithm in Resources Constrained Devices. IEEE.

[15] Nautiyal, I. and Sharma, M. (2014) Encryption Using Elliptic Curve Cryptography Using Java As Implementation Tool. *IJARCSSE*, **4**, 620-625.

[16] Ben-Salem, M. and Stolfo, S.J. (2011) Modeling User Search-Behavior for Masquerade Detection. In: *Proceedings of the* 14*th International Symposium on Recent Advances in Intrusion Detection*, Springer, Heidelberg, 1-20. http://dx.doi.org/10.1007/978-3-642-23644-0_10

[17] Ben-Salem, M. and Stolfo, S.J. (2011) Combining a Baiting and a User Search Profiling Techniques For Masquerade Detection in Columbia University Computer Science Department. Technical Report # cucs-018-11. 13-28 https://www.researchgate.net/publication/266891208