A Novel Authentication Method for Big Data Environment

S. Regha, M. Manimekalai

Abstract*: Security is essential for any networks. As the essential communication mode, the security mechanism for multicast isn't just the measure to guarantee verified communications, yet additionally the precondition for other security services. Attacks are one of the most significant worries for security experts. Attackers more often than not access an enormous number of computers by misusing their vulnerabilities to set up attack armed forces. This paper shows a twofold way validation mechanism which uses the usefulness of Elliptical Curve Cryptography, Kerberos System, and ElGamal algorithm. ECC algorithm used to encrypt the user information, whereas ElGamal used to encrypt the secret key itself to ensure more security in the networks.

***Keywords* : Security, Elliptical Curve Cryptography, Kerberos System, ElGamal, Encryption, Decryption.**

I. INTRODUCTION

The computer industry has created a collection of identification and authentication technologies like userID/Passwords, Biometrics, One Time Password, Smartcards, Lightweight Directory Access Protocol, Secure Socket Layer, Security Assertion Markup language (SAML), CardSpace address varying business, OpenID and security requirements[1]. Every organization adopts at least one of these technologies to verify data against misuse and unapproved access. In an organized domain, clients are allowed access to the system just when they give their imminent data (e.g., User name and secret key) safely to check and approve their personality. If an individual can demonstrate that, additionally knows something that no one but he could know, it is sensible to feel that an individual who professes to be. The reason for individual validation is to guarantee. The rendered services are being gotten to just by an authentic client. All Network clients expect to get to data and move data securely. To make sure, the secure transmission of data between the users in a network is a challenging task.

II. RELATED WORKS

Jiliang Zhou in [2] proposed an efficient and secures routing protocol based on Encryption and authentication for WSNs. BEARP especially mitigates loads of sensor nodes by transferring routing related tasks to BS, which not only maintains network-wide energy equivalence and prolongs network lifetime but also improves the security mechanism performed uniquely by the secure BS.

Pawani Porambage in [3] proposed an inescapable lightweight authentication and keying mechanism for WSNs in conveyed IoT based applications, in which the sensor nodes can build up protected connections with companion sensor nodes and end-clients.

Imran Memon in [4]] proposed the anticipate private client data and secure communication by asymmetric cryptography plot. The creators tackled the remote communication issue in A3 algorithms, for example, listening stealthily and this issue illuminated by asymmetric cryptography plot as a result of its power against this sort of attack by giving shared authentication make the system progressively secure.

Khalid Mahmood in [5] proposed a half and half Diffie–Hellman based lightweight authentication plan utilizing AES and RSA for session key generation. To guarantee message honesty, the upsides of a hash-based message authentication code are abused.

Kakelli Anil Kumar in [6] proposed a New Secure Multipath Routing Protocol for Military Heterogeneous Wireless Sensor Network for secure data transmission. A New Secure Multipath Routing Protocol utilizes Elliptic Curve Cryptography (ECC) to find confided in neighbor nodes and set up the multiple safe courses for dependable data conveyance in MHTWSN.

Sravani Challa in [7] proposed plan bolsters usefulness highlights, for example, dynamic sensor hub expansion, the secret key just as biometrics update, brilliant card disavowal alongside other usual highlights required for client authentication in remote sensor systems.

III. SIGNIFICANCE OF AUTHENTICATION

Utilizing of authentication mechanism lead to address the accompanying issues. The definition issues are given below:

- **Authentication:** Authentication means empowering the system to concede the approved clients to approach its assets. It gives direction where the access control mechanisms check the asserted identifier through specific methods.
- **Access Control:** The order wherein mechanisms and approaches are built up that confine access to PC assets to address clients.

Manuscript published on 30 September 2019
***** Correspondence Author

S. Regha*, Department of Computer Science, Shrimati Indira Gandhi College, Tiruchirappalli, India.
M. Manimekalai, Department of Computer Science, Shrimati Indira Gandhi College, Tiruchirappalli, India.

*Retrieval Number: C5319098319/2019©BEIESP
DOI:10.35940/ijrte.C5319.098319
Journal Website: www.ijrte.org*

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

- ***ID:*** It is where an asset asserts (or is distinguished through different methods) a particular and one of a kind identifier.
- ***Authorization:*** Which decides the benefits related with validated character.
- ***Security:*** The capacity of a system to ensure data, services, and assets against misuse by unapproved clients.

IV. PROPOSED NOVEL AUTHENTICATION APPROACH FOR BIG DATA ENVIRONMENT

The Kerberos convention utilizes a focal Key Distribution Center (KDC) which goes about as a confided in outsider. In Kerberos, the KDC and different substances utilize a "safe" clock to distinguish replay attacks and check token legitimacy. Kerberos utilizes the timestamp as an authenticator. The tickers are thought to be matched up with a modest quantity of realized clock float. The nodes in the systems are associated, and there is likewise an authentication server, which gives authentication administration to one another. Given a circulated set of services, we trust Kerberos is a suitable design for empowering between administration and client to support authentication. In this proposed work, the essential idea is that the data is encoded using an AES symmetric encryption algorithm [8]. The scrambled data is then put away. The symmetric key used to scramble the data is then encoded, using the ElGamal public key [9]. This way, the ideal approach to unscramble the symmetric key is by using the ECC private key [10].

The given data is first encrypted by a symmetric key, and that symmetric key is then encrypted using the ElGamal public key of the data owner. That is,

$$E_k(d) = \text{Ctext}$$

$$G_{pub}(k) = \text{EK}$$

Where E is the symmetric encryption operation, k is the symmetric key, Ctext is the ciphertext, G is the ElGamal encryption operation, the pub is the ElGamal public key of the data owner, and EK is the Encrypted symmetric key.

Considering the ECC algorithm, the private keys and public keys as huge numbers, this makes key partitioning possible and subsequently, partial Decryption is additionally understandable. In this way, if it is somehow arrived to partition the ECC private key Ctext into two sections Atext and Btext with the end goal that Atext + Btext = Ctext, the symmetric key could be somewhat decrypted utilizing Atext and the in part decrypted key can then be decrypted entirely utilizing Btext.

In Kerberos [11], the Key Distribution Center is considered as a certificate authority. The Key Distribution Center has every one of the certificates and the public key of each element, and every one of the substances has the certificate of KDC, with the goal that they can confirm the signature of KDC. Moreover, likewise, the Key Distribution Center has a secret key. Just Key Distribution Center thinks about this key, and no other substance has the learning of it. In this proposed multi-level authentication mechanism, the secret key (Symmetric-key) is encrypted with the ElGamal public key, and it has Decrypted with segmented ECC private key.

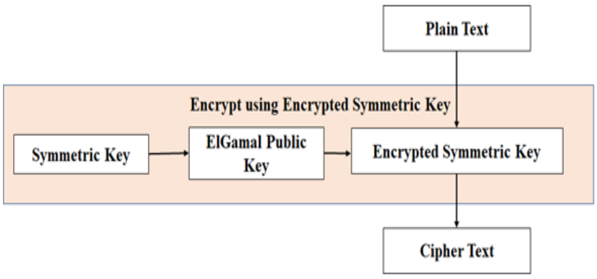

Fig. 1: Encryption of user data and key for Encryption the data

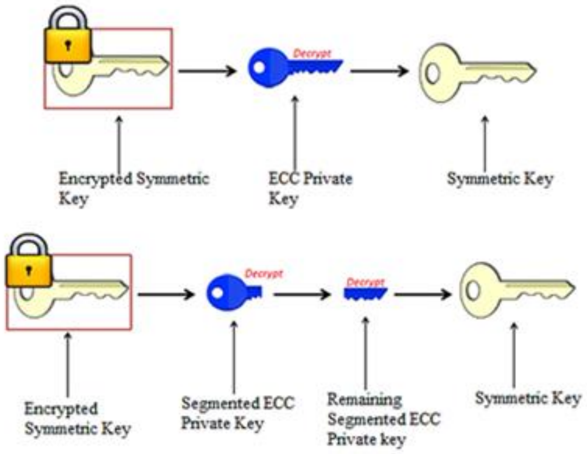

Fig.2: Decryption Process of the encrypted symmetric key

Abbreviations	Explanation
TGT	Ticket Granting Ticket
KDC	Key Distribution Center
sk	Session Key
Symk	Symmetric Key
ESymk	Encrypted Symmetric Key
K_X	Key for Client X generated by KDC
SK_U	The session key (sk) for server and user
DKDB	The encryption keys are stored in the key pool database
DataOwner	The Data owner determines who can access the data and give a license to the data
DataPer	Any user who has a license to access data proffered by the DataOwner

Step by Step Procedure of Proposed Authentication Approach

Registration Phase:

1: The DataOwner selects his/her ID and password.

2: The DataOwner request the server for sharing the data or resources.

3: DataOwner chooses the random number as the symmetric key (SymK).

4: KDC constitutes a private and public key by ElGamal encryption algorithm.

5: The SymK is then encrypted itself by KDC using ElGamal public key.

6: Then, the ESymK is used to encrypt the user information, and it is stored in KDC.

Login Phase:

1: The user assigns a request by using the ID and Password to TGT.

2: KDC creates a ticket and a session key (sk).

3: User chooses the secret key from the key pool using ECC. Then the secret key (SecK) is partitioned into two divisions for the decryption process.

4: The user computes the values using the SecK and the cipher key. The signature is generated by using SecK and the cipher key and sends to KDC

5: When the Key Distribution Center receives the messages from the user and restores its ciphertext.

6: It extracts the SecK from the value. The decryption process is
taken.

7: By using a partitioned secret key, the cipher key is decrypted, and ciphertext is decrypted with the symmetric key using Key Distribution Center, and it verifies the signature with the secret key.

8: Finally, the Key Distribution Center verifies the signature of the user, and gets the client certificate, provides the ticket and session key for the secure transmission

V. RESULT AND DISCUSSION

In this paper, the Kerberos system, Elliptical Curve Cryptography, ElGamal, Symmetric Key Encryption algorithms provide two essential services for securing the networks.

- Securing the Information: It is provided by using Encryption and Decryption.
- Authenticating the Information: Digital Signature and Kerberos has used for providing authentication.

A. Performance Analysis of using Kerberos system in the proposed authentication approach

Table 2 depicts the performance analysis of the Proposed Authentication mechanism with Kerberos, ECC, Elgamal with existing Kerberos technique. From table 1, it is clear that the proposed authentication system generates a token in minimum time when it is compared with the existing Kerberos System.

Table 2: Performance analysis of the existing Kerberos system with proposed authentication approach with Kerberos, ECC, ElGamal

Number of Requests	**Token Generation Time in ms**	
	Proposed Authentication Scheme	**Existing Kerberos System**
1000	128	130
2000	142	145
3000	145	148
4000	151	152
5000	158	160
6000	162	164
7000	169	171
8000	171	175
9000	178	182

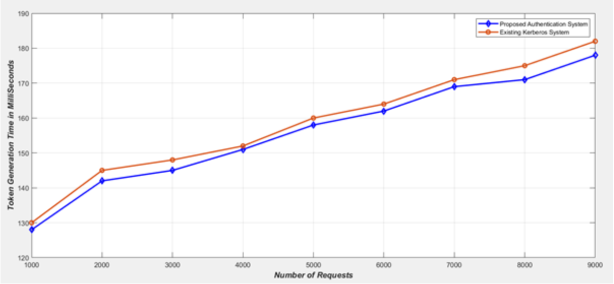

Fig.3: Graphical Representation of the token generation time (ms) for the proposed Authentication Scheme and Existing Kerberos System

B. Performance analysis of the proposed authentication approach using 8-bits security level

Table 3a gives the National Institute of Standards and Technology recommended security bit levels for existing ElGamal and ECC encryption method. The size of the key increases with the security bit level for ElGamal method. ECC utilizes only a small number of a key when comparing with ElGamal. Figure 4a depicts the graphical representation of the Encryption time taken by Elliptical Curve Cryptography, ElGamal, and proposed authentication approach at the 80-bit security level.

Table 3a: Encryption time is taken by ECC, ElGamal and Proposed Authentication Approach at the 80-bit security level

Number of Encryption Bits	**Encryption time in seconds**		
	Proposed Authentication approach	**ElGamal**	**ECC**
8 bits	0.0672	0.0515	0.5887
64 bits	0.4679	0.3354	3.1887
256 bits	0.9865	0.7796	8.9221

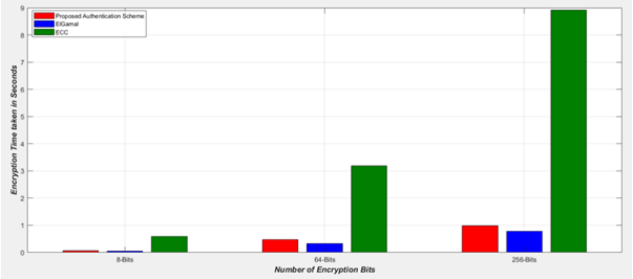

Fig.4a: Graphical representation of the Encryption time taken in seconds by proposed Authentication approach, ElGamal, and ECC for number of encryption bits

Table 3b depicts the decryption time in seconds by the proposed Authentication approach, ElGamal and ECC at the 80-bit security level. Figure 4b gives the graphical representation for the decryption time taken in seconds for the proposed authentication approach, ElGamal and ECC.

Table 3b: Time is taken for Decryption by RSA, ECC and proposed Two-fold Authentication Mechanism at the security bit level of 80

Number of Decryption Bits	**Decryption time in seconds**		
	Proposed Authenticatio n approach	**ElGamal**	**ECC**
8 bits	2.4376	0.8634	1.4376
64 bits	6.5178	6.7172	6.7277
256 bits	22.9874	23.5354	22.9982

Retrieval Number: C5319098319/2019©BEIESP
DOI:10.35940/ijrte.C5319.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

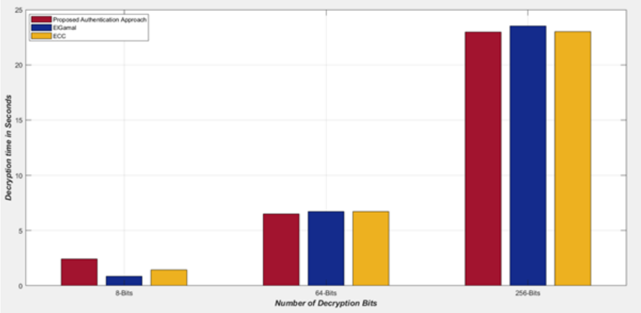

Fig.4b: Graphical representation of the Decryption time taken by Proposed authentication approach, ElGamal and ECC for the 80-bit security level

Table 3c depicts the total time taken for Encryption and Decryption by the proposed authentication approach, ElGamal and ECC at the 80-bits security level for the varying number of encryption and decryption bits. Figure 4c depicts the graphical representation of the total time taken for Encryption and Decryption by the proposed authentication approach, ElGamal, and ECC approaches.

Table 3c: Total Taken for Encryption and Decryption by proposed authentication approach, ElGamal and ECC method

Number of Encryption/Decryption Bits	Total time taken in seconds		
	Proposed Authentication approach	ElGamal	ECC
8 bits	2.5048	0.9149	2.0236
64 bits	6.9857	7.0526	9.9164
256 bits	23.9739	24.315	31.9203

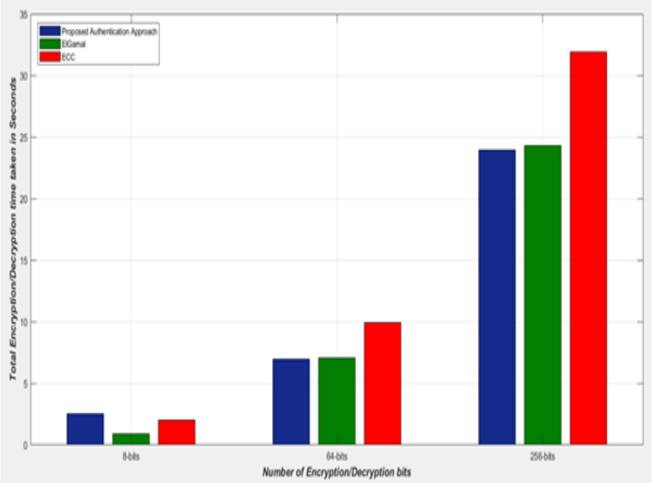

Fig.4c: Graphical representation of the Total Encryption/Decryption time taken in seconds by proposed authentication approach, ElGamal and ECC methods for varying number of bits

C. Performance analysis of the proposed authentication approach using 112-bits security level

Table 4a depicts the encryption time taken by the proposed authentication approach, ElGamal and ECC 112-bits security level for varying number of encryption bits. Figure 5a gives the graphical representation for encryption Time taken by the proposed authentication approach, ECC and ElGamal at the security bit level of 112:

Table 4a: Encryption time taken by ECC, ElGamal and Proposed Authentication Approach at the 112-bit security level

Number of Encryption Bits	Encryption time in seconds		
	Proposed Authentication approach	ElGamal	ECC
8 bits	0.0429	0.0377	3.3212
64 bits	0.2974	0.2857	9.9968
256 bits	0.5877	0.5837	22.8337

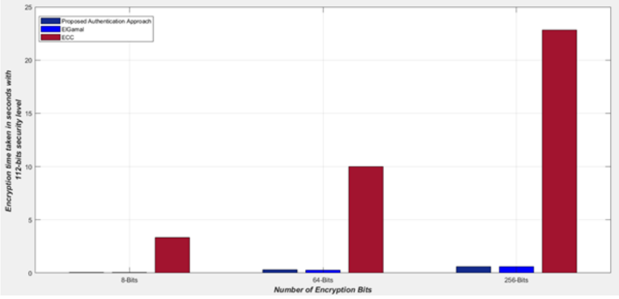

Fig.5a: Graphical representation of the encryption time taken in seconds by proposed authentication approach, ECC and ElGamal for 112-bits security level

Table 4b depicts the decryption time taken by the proposed authentication approach, ElGamal and ECC 112-bits security level for varying number of decryption bits. Figure 5b gives the graphical representation for decryption time taken by ElGamal, ECC, and proposed authentication approach at the security bit level of 112.

Table 4b: Decryption time is taken by ECC, ElGamal and Proposed Authentication Approach at the 112-bit security level

Number of Decryption Bits	Decryption time in seconds		
	Proposed Authentication approach	ElGamal	ECC
8 bits	2.5778	3.9275	2.7883
64 bits	7.8432	21.4328	7.7333
256 bits	26.7332	104.255	26.5351

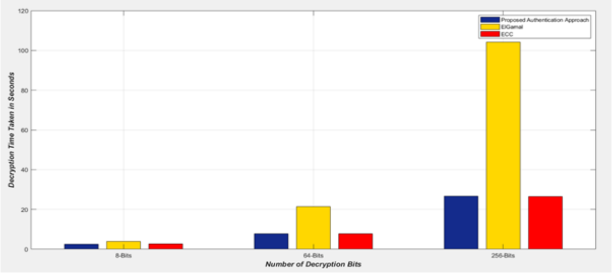

Fig.5b: Graphical representation of the decryption time taken in seconds by proposed authentication approach, ECC and ElGamal for 112-bits security level

Table 4c depicts the decryption time taken by the proposed authentication approach, ElGamal and ECC 112-bits security level for varying number of encryption/decryption bits. Figure 5c gives the graphical representation for encryption/decryption time taken by ElGamal, ECC, and proposed authentication approach at the security bit level of 112.

Table 4c: Encryption and Decryption time taken by ECC, ElGamal and Proposed Authentication Approach at the 112-bit security level

Number of Encryption/Decryption Bits	Encryption and Decryption Time in Seconds		
	Proposed Authentication approach	ElGamal	ECC
8 bits	2.5048	0.9149	2.0236
64 bits	6.9857	7.0526	9.9164
256 bits	23.9739	24.315	31.9203

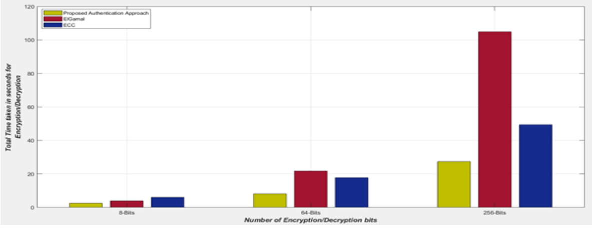

Fig.5c: Graphical representation of the encryption/decryption time taken in seconds by proposed authentication approach, ECC and ElGamal for 112-bits security level

D. Performance analysis of the proposed authentication approach using 128-bits security level

Table 5a depicts the encryption time taken by the proposed authentication approach, ElGamal and ECC 128-bits security level for varying number of encryption bits. Figure 6a gives the graphical representation for encryption Time taken by the proposed authentication approach, ECC and ElGamal at the security bit level of 128.

Table 5a: Encryption time taken by ECC, ElGamal and Proposed Authentication Approach at the 128-bit security level

Number of Encryption Bits	Encryption time in seconds		
	Proposed Authentication approach	ElGamal	ECC
8 bits	0.0618	0.0527	4.8985
64 bits	0.4965	0.3874	16.2882
256 bits	0.8234	0.7611	37.6658

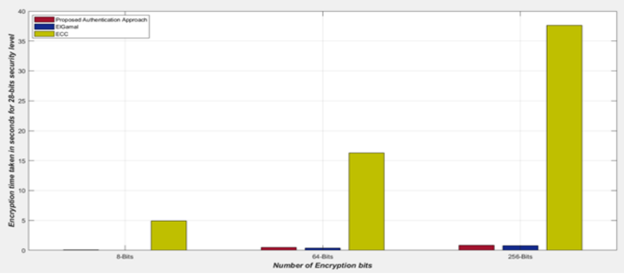

Fig.6a: Graphical representation of the Encryption time taken in seconds by the proposed authentication scheme, ElGamal, ECC with 128-bits security level

Table 5b depicts the decryption time taken by the proposed authentication approach, ElGamal and ECC 128-bits security level for varying number of decryption bits. Figure 6b gives the graphical representation for decryption Time taken by the proposed authentication approach, ECC and ElGamal at the security bit level of 128.

Table 5b: Decryption time is taken by ECC, ElGamal and Proposed Authentication Approach at the 128-bit security level

Number of Decryption Bits	Decryption time in seconds		
	Proposed Authentication approach	ElGamal	ECC
8 bits	3.1221	7.7629	2.9892
64 bits	8.9941	46.6782	8.5582
256 bits	27.7872	209.8248	27.6282

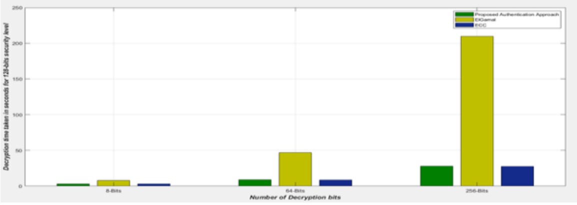

Fig.6b: Graphical representation of the decryption time taken in seconds by proposed authentication approach, ElGamal, ECC for 128-bits security level

Table 5c depicts the total Encryption and decryption time taken in seconds by the proposed authentication approach, ElGamal and ECC 128-bits security level for varying number of decryption bits. Figure 6c gives the graphical representation for total Encryption and decryption time taken in seconds by the proposed authentication approach, ECC and ElGamal at the security bit level of 128.

Table 5c: Total Encryption and decryption time taken in seconds by proposed authentication approach, ElGamal, ECC for 128-bits security level

Number of Encryption/Decryption Bits	Encryption and Decryption Time in Seconds		
	Proposed Authentication approach	ElGamal	ECC
8 bits	3.1839	7.8156	7.8877
64 bits	9.4906	47.0656	24.8464
256 bits	28.6106	210.5895	65.294

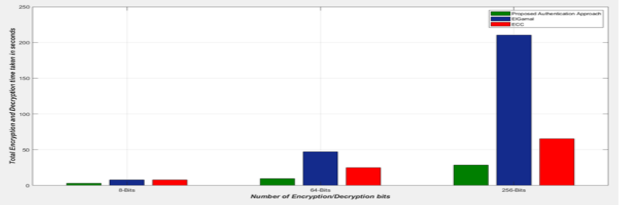

Fig.6c: Graphical representation of the total Encryption and decryption time taken in seconds by proposed authentication approach, ElGamal, ECC for 28-bits security level

E. Performance analysis of the proposed authentication approach using 192-bits security level

Table 6a depicts the encryption time taken by the proposed authentication approach, ElGamal and ECC 192-bits security level for varying number of encryption bits. Figure 7a gives the graphical representation for encryption Time taken by the proposed authentication approach, ECC and ElGamal at the security bit level of 192.

Table 6a: Encryption time taken by ECC, ElGamal and Proposed Authentication Approach at the 192-bit security level

Number of Encryption Bits	Encryption time in seconds		
	Proposed Authentication approach	ElGamal	ECC
8 bits	0.6989	0.05862	5.7488
64 bits	0.4276	0.3587	21.2528
256 bits	0.8649	0.7738	77.7256

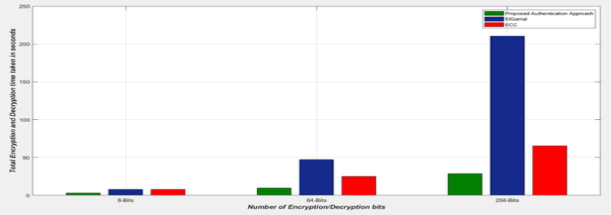

Fig.7a: Graphical representation of the encryption time taken in seconds by Proposed authentication approach, ElGamal, ECC for 192-bits security level

Table 6b depicts the decryption time taken by the proposed authentication approach, ElGamal and ECC 192-bits security level for varying number of decryption bits. Figure 7b gives the graphical representation for decryption Time taken by the proposed authentication approach, ECC and ElGamal at the security bit level of 192:

Table 6b: Decryption time is taken by ECC, ElGamal and Proposed Authentication Approach at the 192-bit security level

Number of Decryption Bits	Decryption time in seconds		
	Proposed Authentication approach	ElGamal	ECC
8 bits	3.4333	13.665	3.224
64 bits	8.7894	77.7664	8.6787
256 bits	32.6656	259.8284	32.3544

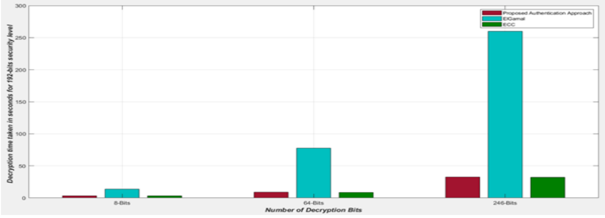

Fig.7b: Graphical representation of the Decryption time taken in seconds by proposed authentication approach, ElGamal, ECC for 192-bits security level

Table 6c depicts the total Encryption and decryption time taken in seconds by the proposed authentication approach, ElGamal and ECC 192-bits security level for varying number of decryption bits. Figure 7c gives the graphical representation for total Encryption and decryption time taken in seconds by the proposed authentication approach, ECC and ElGamal at the security bit level of 192.

Table 6c: Total Encryption and decryption time taken in seconds by proposed authentication approach, ElGamal, ECC for 192-bits security level

Number of Decryption Bits	Decryption time in seconds		
	Proposed Authentication approach	ElGamal	ECC
8 bits	4.1322	13.724	8.9728
64 bits	9.217	78.1251	29.9315
256 bits	33.5305	260.6022	110.08

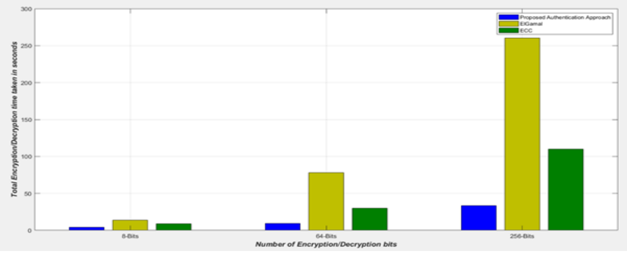

Fig.7c: Graphical representation of the total Encryption and decryption time taken in seconds by proposed authentication approach, ElGamal and ECC for 192-bits security level

VI. CONCLUSION

In this paper, a novel authentication approach with the Kerberos system has proposed in the context of securing the big data environment. The proposed authentication approach composed of two phases: i) Registration phase and ii) Login and an Authentication phase. Proposed authentication approach takes less time for Decryption than ElGamal and ECC in the higher security level. Proposed authentication approach performs in less total time for Encryption and Decryption of details among the user, Kerberos system, and the server. When it has compared with the various security bit levels, the proposed authentication approach with the Kerberos system it performs better than the ElGamal and ECC.

REFERENCES

1. Yao, Xuanxia, et al. "A lightweight multicast authentication mechanism for small scale IoT applications." IEEE Sensors Journal 13.10 (2013): 3693-3701.
2. Zhou, Jiliang. "Efficient and secure routing protocol based on encryption and authentication for wireless sensor networks." *International Journal of Distributed Sensor Networks* 9.4 (2013): 108968.
3. ‘Porambage, Pawani, et al. "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications." International Journal of Distributed Sensor Networks 10.7 (2014): 357430.
4. Memon, Imran, et al. "Enhanced privacy and authentication: An efficient and secure anonymous communication for location-based service using asymmetric cryptography scheme." Wireless Personal Communications 84.2 (2015): 1487-1508.
5. Mahmood, Khalid, et al. "A lightweight message authentication scheme for Smart Grid communications in the power sector." Computers & Electrical Engineering 52 (2016): 114-124.
6. Kumar, Kakelli Anil, Addepalli VN Krishna, and K. Shahu Chatrapati. "New secure routing protocol with elliptic curve cryptography for military heterogeneous wireless sensor networks." Journal of Information and Optimization Sciences 38.2 (2017): 341-365.
7. Challa, Sravani, et al. "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks." Computers & Electrical Engineering 69 (2018): 534-554.
8. Cheng, Chi, et al. "Securing the Internet of Things in a quantum world." *IEEE Communications Magazine* 55.2 (2017): 116-120.
9. Simplicio Jr, Marcos A., et al. "Lightweight and escrow-less authenticated key agreement for the internet of things." *Computer Communications* 98 (2017): 43-51.
10. Shen, Han, et al. "Efficient RFID authentication using elliptic curve cryptography for the internet of things." *Wireless Personal Communications* 96.4 (2017): 5253-5266.
11. Li, Hui, et al. "Securing Offline Delivery Services by Using Kerberos Authentication." IEEE Access 6 (2018): 40735-40746.

Retrieval Number: C5319098319/2019©BEIESP
DOI:10.35940/ijrte.C5319.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication