International Journal of Engineering & Technology, 7 (2.26) (2018) 119-124

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A New Authentication Scheme with Elliptical Curve Cryptography for Internet of Things (IoT) Environments

M Durairaj[1]*, K Muthuramalingam[2]

[1]Assistant Professor, School of Computer Science, Engineering and Application, Bharathidasan University
[2] Assistant Professor, School of Computer Science, Engineering and Application, Bharathidasan University
**Email: bardmuthu@gmail.com*

Abstract

Internet of Things (IoT) consists of a large number of connected objects that are communicating with each other. To support trusted communication between IoT objects, the authentication procedures should be used and applied to the communicating entities. Internet of Things (IoT) is an emerging technology, which makes the remote sensing and control across the heterogeneous network a reality, and has good prospects in industrial applications. As an essential infrastructure, Wireless Sensor Networks (WSNs) play a crucial role in industrial IoT. Due to the resource-constrained feature of sensor nodes, the design of security and efficiency balanced authentication scheme for WSNs becomes a significant challenge in IoT applications. In this paper, an anonymous authentication scheme for WSNs in an Internet of Things environments.

Keywords: *Internet of Things, Authentication Scheme, Wireless Sensor Networks, Gate Way Node, Sensor Node, User*.

1. Introduction

In the early 90s, the word internet is used to express the technology of connecting computers all over the globe using wired or wireless links. Since then the internet has been effectively used for files sharing, web browsing, e-commerce, social media, etc. However, recent development and deployment of smart technologies have emerged the need for objects to be ubiquitously connected. Consequently, this necessitates the need for more sophisticated techniques to support new machine-to-machine (M2M) communication. To evolve a new world of connected objects, the Internet of Things (IoT) has introduced as the future of the internet [1, 2].

The development of IoT has many influences on human life. Human lifestyle is gradually changing toward smartness and intelligence which can be facilitated by the development of smart homes and smart communities as a part of the IoT [3]. Moreover, IoT applications support different daily activities such as route planning, navigation, transportation decisions, traffic and healthcare monitoring, elderly and children supervision, and many more [4].

As is the future of the Internet, the provision of security services, such as authentication, is an essential factor to encourage people to use new technologies and securely access various IoT resources. Users would not be convenient to share and exchange their data and personal information unless protection schemes are used to prevent any malicious behavior. Therefore, efficient security and authentication techniques are necessary for comprehensive and fast deployment of IoT.

2. Related Works

Table 1 gives the associated works carried out in the authentication process of the Internet of Things (IoT) environments. Cloud services are considered as the vital part of the IoT since it handles the full range of data.

Table 1: Related Works on Authentication techniques

Author Name	Paper Title	Methods or Steps used	Description
Moghaddam, Faraz Fatemi, et al [1]	A scalable and efficient user authentication scheme for cloud computing environments	Modified Diffie-Hellman Agent (MDHA), ZKP Diffie-Hellman	In this paper, client-based user authentication agent has been introduced to confirm an identity of the user on the client side.
Singh, Ashish, and Kakali Chatterjee [2]	A secure multi-tier authentication scheme in cloud computing environment	Multi-tier authentication	This paper proposes a reliable and more advanced multi-tier authentication scheme for accessing cloud services
Yang, Jen Ho, and Pei Yu Lin [3]	An ID-based user authentication scheme for cloud computing	One way hash function, XOR operation	This paper introduces a new ID-based user authentication scheme for cloud computing has proposed. The authors proved that the

			proposed scheme has higher security levels and lower computation costs.
Tien-Ho Chen, Hsiu-lien Yeh, Wei-Kuan Shih [4]	An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing	Elliptic Curve Cryptosystem (ECC)	This paper proposes an ECC dynamic ID-based remote mutual authentication scheme for remote devices to solve the issues.
Tsai, Jia-Lun, and Nai-Wei Lo [5]	A privacy-aware authentication scheme for distributed mobile cloud computing services	bilinear pairing, One-way hash function	This paper proposes the trusted Smart Card Generator (SCG) service is not involved in individual user authentication process. The proposed scheme reduces authentication processing time required by communication and computation between cloud service providers and traditional trusted third party service. Formal security proof and performance analyses are conducted to show that the scheme is both secure and efficient.
Powell, Courtney, Takashi Aizawa, and Masaharu Munetomo [6]	Design of an SSO Authentication Infrastructure for Heterogeneous Inter-cloud Environments	single sign-on (SSO)	This paper outlines the plan of an authentication infrastructure for linking distributed heterogeneous cloud systems managed by different cloud management middleware to enable them to interoperate as an integrated inter-cloud system. This authentication infrastructure achieves single sign-on (SSO), which allows users to log in once and access the various cloud systems without being asked to log in again at each operation.
Peng, Siwei [7]	An Id-based Multiple Authentication scheme against attacks in wireless sensor networks	Symmetrical Encryption	This paper presents a novel authentication scheme to prevent these attacks. This Id-based Multiple Authentication (IMA) scheme based upon the mutual identity authentication and steganography to give a secure mechanism for data aggregation in WSNs.
Nguyen, Tien Dung, and Eui-Nam Huh [8]	A Dynamic ID-Based Authentication Scheme for M2M Communication of Healthcare Systems	Probabilistic Key management	This paper proposed a simple architecture M2M service apply any hospital which considers the mobility of doctors and patients. An efficient security scheme with dynamic ID-based authentication using crucial pairwise distribution is involved in the M2M system. It can be assured high security through security analysis under shared key attack and Sybil attack.
Chu, Fuzhi, et al [9]	An improved identity authentication scheme for the internet of things in heterogeneous networking environments	Elliptical Curve Cryptography	This paper proposes an identity authentication scheme based on identity authentication scheme based on elliptic curve algorithm for public and private key pair to meet the security requirements of the Internet of Things in heterogeneous networking environments.
Liu, Jing, Yang Xiao, and CL Philip Chen [10]	Authentication and access control in the internet of things	Elliptical Curve Cryptography, Role-based Access Control	This paper mainly analyzes existing authentication and access control methods, and then, it designs a feasible one for the Internet of Things.
Jan, Mian Ahmad, et al [11]	A robust authentication scheme for observing resources in the internet of things environment	Symmetrical Cryptography, XOR operation	This paper proposes a lightweight mutual authentication scheme which validates the identities of the participating devices before engaging them in communication for the resource observation.

3. Proposed Authentication Scheme for the Internet of Things

A new authentication scheme has proposed for securing the IoT environments. An Elliptical Curve Cryptography system has used to strengthening the encryption and decryption process [12,13]. This authentication scheme is composed of two main phases. i) Registration phase, ii) Login and Authentication phase.

3.1. Registration Phase

This registration phase has formed two stages. The first stage is the registration between the user and the gateway, and the second stage is the registration between the sensor node and the gateway.

Table 2: Plain points in the Elliptical Curve Cryptography

Pmsg(X)	Pmsg(Y)
54	3151
19	2118
37	3236
75	3398
145	3322
127	3051
110	36
93	1787

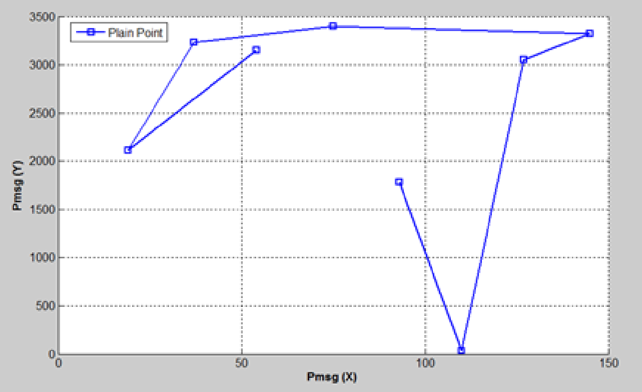

Fig.1: Plain Points in Elliptical Curve

Registration between user – gateway and sensor-gateway

Step 1: The user U selects the ID and password and picks the random integer b from the key pool for key generation using Elliptical Curve Cryptography. The Sensor S selects its ID and generates the random number y.

Step 1.1: The user selects a random number dA between the range [1, n-1].It is the private key of the user.

Step1.2: Then the user generates the public key using the formula PA = dA*G

Step 1.3: Similarly gateway selects a private key dB and generates its public key PB=dB*G.

Step 1.4: The user generates the security key K=dA * PB and the gateway also receives the security key K=dB * PA

Step 2: The user and sensor create the pair of signing and verifying keys and send a message to the Gateway. To sign a message m by the user, it performs the following steps:

Step 2.1: It calculates a cryptographic hash function e=HASH (m)

Step 2.2: The user then selects a random integer k from [1,n-1].

Step 2.3: The it computes a pair (r,s)

Step 2.4: r= x1 (mod n) where (x1,y1) =k*G

Step 2.5: s= k-1(e+ dA*r)

Step 2.6: This pair (r,s) defines the signature.

Step 2.7: The signature has sent to the gateway.

Step 3: Gateway stores the values, and sets the pair of private and public keys.

Step 4: Gateway computes the value of the password regarding ciphertext and sends a message to the user. The password of user and sensor can be converted into ciphertext using ECC encryption algorithm.

Step 4.1: Let m has any point M on the elliptic curve.

Step 4.2: The user and sensor node select a random number k from [1,n-1].

Step 4.3: The ciphertexts generated will be the pair of points (B1, B2) where

B1= k*G
B2= M + (k*G)

Step 5: When the user receives message stores value in Smart Card (SC).

Table 3: Cipher points in the ECC

Cmsg (X)	**Cmsg (Y)**
2705	8245
2818	745
2516	524
5156	1835
4764	7718
1915	6728
3338	987
6569	6442

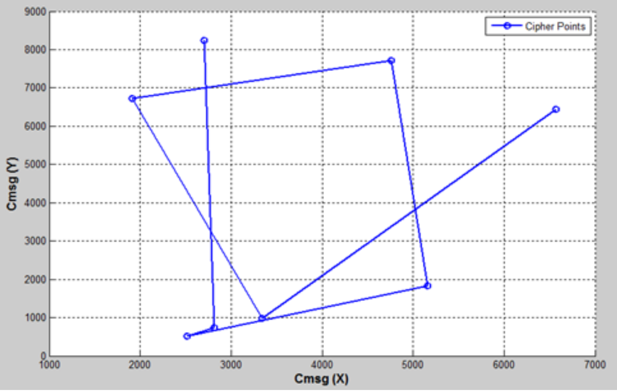

Fig.2: Cipher points in ECC

3.2. Login and Authentication Phase

Once the registration process got over, the user has to communicate with the sensor node via the gateway.

Step 1: User inserts Smart Cart into the terminal, and inputs the user id and password.

Step 2: It computes the values and compares the values with the SC.

Step 3: User selects the secret key from the Key pool using ECC.

Step 4: Then user computes the value using secret key and ciphertext.

Step 5: Then it generates the signature and sends the message to the Gateway.

Step 6: When the gateway node receives the message from the user and restores its secret value.

Step 7: It extracts the secret key from the value. The decryption process is carried out using this secret key.

Step 7.1: The gateway computes the product of B1 and its private key.

Step 7.2: Then the gateway subtracts this product from the second point B2.

M = B2-(dB*B1)
M is the original data sent by the user.

Step 8: The ciphertext has decrypted, and it verifies the signature with the secret key for authenticating the user.

Step 8.1: For authentication, the gateway needs to verify the pair (r,s) are in the range of [1,n-1].

Step 8.2: The gateway again calculates the hash function e as in signature generation.

Step 8.3: Then the gateway calculates w =s-1 mod(n).

Step 8.4: Then calculate u1= e*w (mod n) and u2 = r*w (mod n)

Step 8.5: Calculate (x1,y1)= u1*G + u2*PA.

Step 8.6: If x1 = r (mod n), then the signature is valid.

Step 9: If the signature is not valid, then again repeat the process from step 1.

4. Result and Discussion

In this paper, Elliptical Curve Cryptography provides two essential services for securing the IoT environments.

- **Securing the Information:** It has provided by using encryption and decryption.
- **Authenticating the Information:** Digital Signature has used for providing the authentication.

In this paper, Elliptical Curve Cryptography has utilized to ensure the security of the information and authenticating the user, sensor and gateway node in the Internet of Things environments.

This paper implements the proposed authentication scheme with ECC and RSA to analyze the performance of the scheme. Three data inputs of 8bits, 64 bits, and 256 bits are considered based on the ECC and recommendation of NIST.

Table 4: NIST Recommended Security Bit Level

Security Bit Level	ECC	RSA
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Table 5a: 8bits Encryption Time for ECC and RSA Algorithms in proposed Authentication Scheme

Security Bit Level	Encryption Time in Seconds	
	ECC	RSA
80	0.4776	0.0406
112	2.2121	0.0288
128	3.7874	0.0416
192	4.6377	0.0497

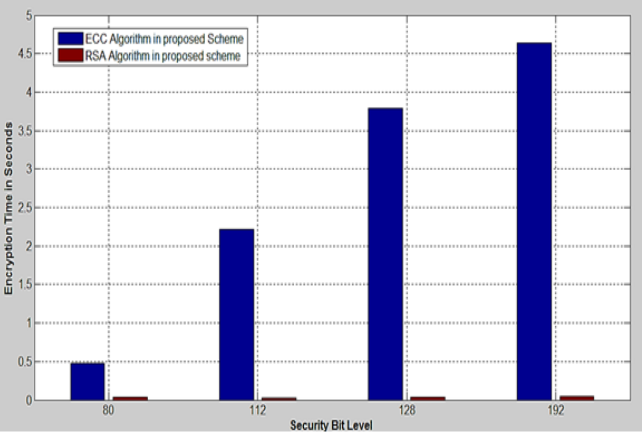

Fig.3a: 8bits Encryption Time for ECC and RSA algorithm in proposed Authentication scheme for various security bit levels

Table 5b: 8bits Decryption Time for ECC and RSA Algorithms in proposed Authentication Scheme

Security Bit Level	Decryption Time in Seconds	
	ECC	RSA
80	1.4376	0.8634
112	1.6774	2.8186
128	1.8781	6.8518
192	2.1133	12.5563

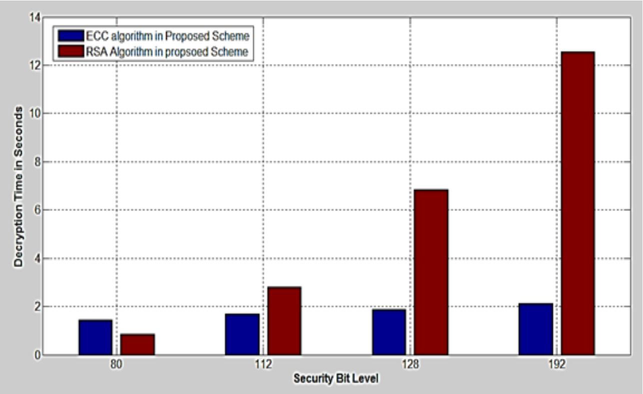

Fig.3b: 8bits Decryption Time for ECC and RSA algorithm in proposed Authentication scheme for various security bit levels

Table 5c: 8bits Total Encryption and Decryption Time for ECC and RSA Algorithms in proposed Authentication Scheme

Security Bit Level	Total Time in Seconds	
	ECC	RSA
80	1.9152	0.904
112	3.8791	2.8474
128	5.6655	6.8934
192	6.7510	12.606

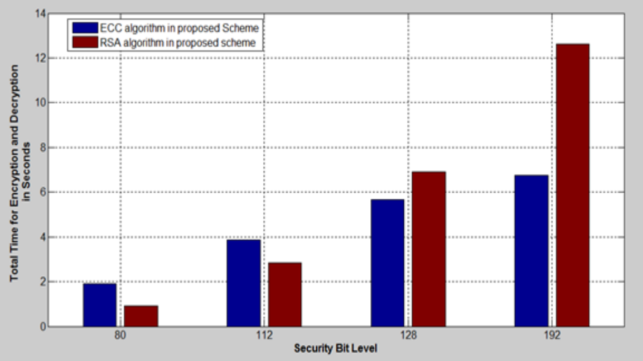

Fig.3c: 8bits Total Encryption and Decryption Time for ECC and RSA algorithm in proposed Authentication scheme for various security bit levels

Above table, 5a gives the encryption time of Elliptical Curve Cryptography and RSA in the proposed authentication scheme for IoT environment. Table 5b represents the decryption time of ECC and RSA in proposed scheme and table 5c depicts the total encryption and decryption time for various security bit levels. Considering the above tables, ECC takes more time for encryption and decryption for lower security bits levels (80 and 112 bits), whereas, for higher security bit levels, RSA takes more time for executing the encryption and decryption. Figure 3a, 3b, and 3c give the graphical representation of the 8bits encryption, decryption and total time of ECC and RSA in the proposed authentication scheme for various security bit levels.

Table 6a: 64bits Encryption Time for ECC and RSA Algorithms in proposed Authentication Scheme

Security Bit Level	Encryption Time in Seconds	
	ECC	RSA
80	2.2776	0.2455
112	9.8966	0.1746
128	15.1771	0.2763
192	20.1419	0.2496

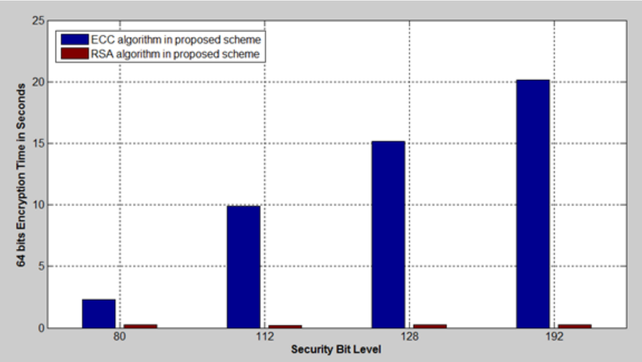

Fig. 4a: 64 bits Encryption Time for ECC and RSA algorithm in proposed Authentication scheme for various security bit levels

Table 6b: 64 bits Decryption Time for ECC and RSA Algorithms in proposed Authentication Scheme

Security Bit Level	Decryption Time in Seconds	
	ECC	RSA
80	5.8188	5.6281
112	6.8444	20.3217
128	7.4493	45.5691
192	7.5896	76.6553

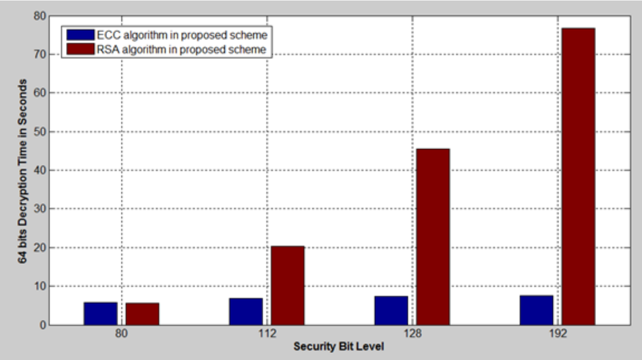

Fig.4b: 64 bits Decryption Time for ECC and RSA algorithm in proposed Authentication scheme for various security bit levels

Table 4c: 64 bits Total Encryption and Decryption Time for ECC and RSA Algorithms in proposed Authentication Scheme

Security Bit Level	Total Time in Seconds	
	ECC	RSA
80	8.0964	5.8736
112	16.741	20.4963
128	22.6264	45.8494
192	27.7315	76.9049

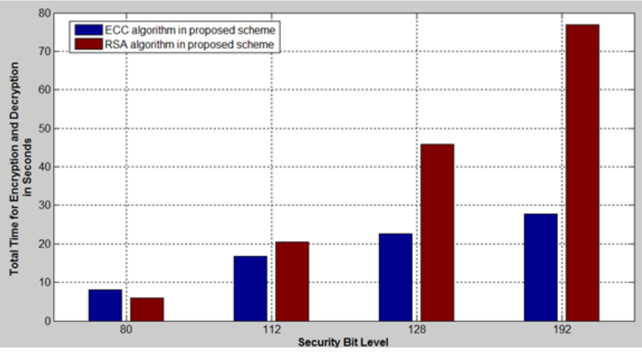

Fig. 4c: 64 bits Total Encryption and Decryption Time for ECC and RSA algorithm in proposed Authentication scheme for various security bit levels

Above table, 6a gives the 64bits encryption time of Elliptical Curve Cryptography and RSA in the proposed authentication scheme for IoT environment. Table 6b represents the 64 bits decryption time of ECC and RSA in proposed scheme and table 6c depicts the total encryption and decryption time of 64bits for various security bit levels. Considering the above tables, ECC takes more time for encryption and decryption for lower security bits levels (80 and 112 bits), whereas, for higher security bit levels, RSA takes more time for executing the encryption and decryption. Figure 4a, 4b, and 4c give the graphical representation of the 64bits encryption, decryption and total time of ECC and RSA in the proposed authentication scheme for various security bit levels.

Table 7a: 256 bits Encryption Time for ECC and RSA Algorithms in proposed Authentication Scheme

Security Bit Level	Encryption Time in Seconds	
	ECC	RSA
80	7.8331	0.6687
112	38.8117	0.4926
128	57.5477	0.6522
192	76.6145	0.6829

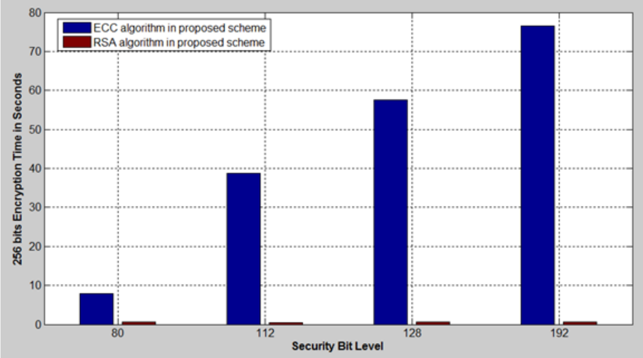

Fig.5a: 256 bits Encryption Time for ECC and RSA algorithm in proposed Authentication scheme for various security bit levels

Table 7b: 256 bits Decryption Time for ECC and RSA Algorithms in proposed Authentication Scheme

Security Bit Level	Encryption Time in Seconds	
	ECC	RSA
80	21.9962	18.4266
112	25.4442	103.1446
128	26.5171	208.7175
192	31.2633	310.1758

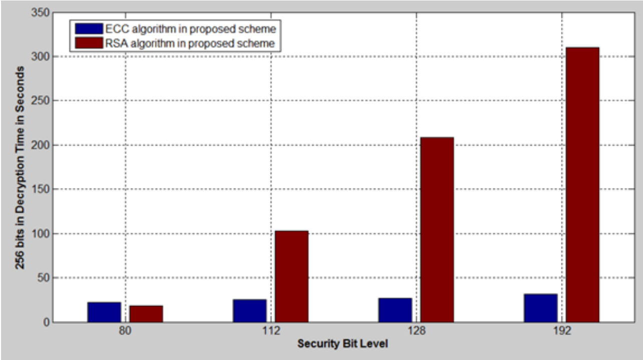

Fig.5b: 256 bits Decryption Time for ECC and RSA algorithm in proposed Authentication scheme for various security bit levels

Table 7c: 256 bits Total Time of Encryption and Decryption for ECC and RSA Algorithms in proposed Authentication Scheme

Security Bit Level	Encryption Time in Seconds	
	ECC	RSA
80	29.8293	103.8133
112	64.2559	103.6372
128	84.0648	209.3697
192	107.8778	310.8587

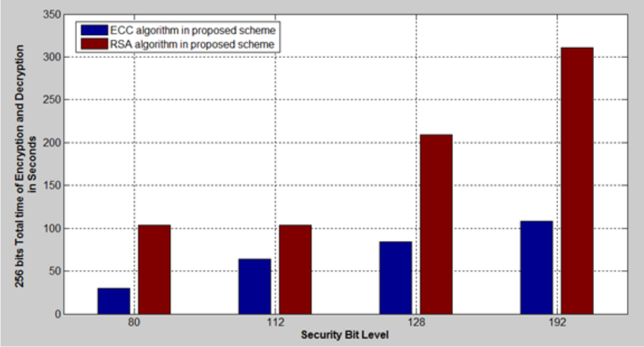

Fig.5c: 256 bits Total time of Encryption and Decryption for ECC and RSA algorithm in proposed Authentication scheme for various security bit levels

Above table, 7a gives the 64bits encryption time of Elliptical Curve Cryptography and RSA in the proposed authentication scheme for IoT environment. Table 7b represents the 256 bits decryption time of ECC and RSA in proposed scheme and table 7c depicts the total encryption and decryption time of 256 bits for various security bit levels. Considering the above tables, ECC takes more time for encryption and decryption for lower security bits levels (80 and 112 bits), whereas, for higher security bit levels, RSA takes more time for executing the encryption and decryption. Figure 5a, 5b, and 5c give the graphical representation of the 256 bits encryption, decryption and total time of ECC and RSA in the proposed authentication scheme for various security bit levels.

5. Conclusion

In this paper, a new authentication scheme with Elliptical Curve Cryptography (ECC) scheme in the context of the Internet of Things (IoT). The proposed authentication scheme composed of two phases: i) Registration phase and ii) Login and an Authentication phase. ECC takes less time for decryption than RSA in the higher security level. ECC performs in less total time for Encryption and decryption of details among User, Gateway, and Sensor nodes. When it has compared with the various security bit levels, the proposed authentication scheme with ECC algorithm outperforms than the proposed scheme with RSA.

References

[1] Moghaddam, Faraz Fatemi, et al. "A scalable and efficient user authentication scheme for cloud computing environments." *Region 10 Symposium, 2014 IEEE*. IEEE, 2014.

[2] Singh, Ashish, and Kakali Chatterjee. "A secure multi-tier authentication scheme in cloud computing environment." *Circuit, Power and Computing Technologies (ICCPCT), 2015 International Conference on*. IEEE, 2015.

[3] Yang, Jen Ho, and Pei Yu Lin. "An ID-based user authentication scheme for cloud computing." *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on*. IEEE, 2014.

[4] Chen, Tien-Ho, Hsiu-lien Yeh, and Wei-Kuan Shih. "An advanced ECC dynamic id-based remote mutual authentication scheme for cloud computing." *Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on*. IEEE, 2011.

[5] Tsai, Jia-Lun, and Nai-Wei Lo. "A privacy-aware authentication scheme for distributed mobile cloud computing services." *IEEE systems journal* 9.3 (2015): 805-815.

[6] Powell, Courtney, Takashi Aizawa, and Masaharu Munetomo. "Design of an SSO authentication infrastructure for heterogeneous inter-cloud environments." *Cloud Networking (CloudNet), 2014 IEEE 3rd International Conference on*. IEEE, 2014.

[7] Peng, Siwei. "An Id-based Multiple Authentication scheme against attacks in wireless sensor networks." *Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on*. Vol. 3. IEEE, 2012.

[8] Nguyen, Tien Dung, and Eui-Nam Huh. "A Dynamic ID-Based Authentication Scheme for M2M Communication of Healthcare Systems." *Int. Arab J. Inf. Technol.* 9.6 (2012): 511-519.

[9] Chu, Fuzhi, et al. "An improved identity authentication scheme for internet of things in heterogeneous networking environments." *Network-Based Information Systems (NBiS), 2013 16th International Conference on*. IEEE, 2013.

[10] Liu, Jing, Yang Xiao, and CL Philip Chen. "Authentication and access control in the internet of things." *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on*. IEEE, 2012.

[11] Jan, Mian Ahmad, et al. "A robust authentication scheme for observing resources in the internet of things environment." *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on*. IEEE, 2014.

[12] Shankar, K., and P. Eswaran. "RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography." *China Communications* 14.2 (2017): 118-130.

[13] Shankar, K., and P. Eswaran. "RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique." *Journal of Circuits, Systems and Computers* 25.11 (2016): 1650138.