Improved Elliptic Curve Cryptography with RFID Protocol Based on DNA Technique

Er. Rawinderjit Singh[1], Er.Sanjeev Mahajan[2]

[1]*M.Tech Scholar, Department of Computer Science & Engineering, Beant College of Engineering & Technology, Gurdaspur*
[2]*Associate Professor, Department of Computer Science & Engineering, Beant College of Engineering & Technology, Gurdaspur*

***Abstract*— RFID based systems are one of the mainly generally widen applications for tagging as well as maintain tracking purposes in IOT deployment. Confined sources of RFID programs creating the presenting of a solid and effective safety program really complicated process. The protected ECC-centered validation process to get rid of the present RFID vulnerabilities raise be apprehensive communication way among marked as well as bookworm. This paper represents the performance of ECC based encryption technique using DNA based encryption. The most important goal of this paper is to recover the computational speed.**

***Keywords*—** *RFID, ECC Based Authentication Protocol and DNA Cryptography*

I. Introduction

Radio Frequency Identification (RFID) is just a wireless equipment for the applications of intelligent recognition of digital labels actually connected with things having an RFID audience [1]. Lately, RFID techniques are commonly used in present cycle administration, drugstore administration, selection administration, digital cost techniques, intelligent cost selection, distance cards, clinic individual attention, jar research within seaports and extra programs [4]. Generally in most such programs, method for the verification of RFID labels by an RFID audience is important toward promise the strength of the RFID labels if they found in the location of the reader. An excessive amount of attention has been directed at RFID systems due to the simple its deployment around a broad collection of applications. In fact, RFID programs are getting extremely common and cement methods in many different programs such as for instance as an example distinguishing, goal monitoring, feeling surrounding situations of marked items, guarding individual security and etc.; certainly there is a huge rising for such process implementations [1]. Consequently of the therefore several benefits, a huge number of study researchers have started to improve RFID programs lately [4]. With the quick growth of RFID tickets, several types of protection demands have today been exposed within RFID interaction network. In plenty of programs, label control move and collection proofs with label solitude, common validation as well as information confidentiality are believed as one of the most important demands [5]. Moreover, in a number of programs, an RFID label may possibly modify their operator numerous occasions all through their living cycle. Hence all data linked to the label must certainly be transferred from the previous operator to the most recent owner. Thus, in the protected label control move method, the most recent operator solitude, the previous operator solitude and the authorization healing must certainly be effectively pleased [6–9].

1.1 ECC Based Authentication protocol

ECC- based common validation protocol fulfils the RFID safety necessities. Also, it employs elliptic contour Diffie–Hellman (ECDH) essential contract method on the way to start a protected transmission between label and reader. It enables each celebration presenting their elliptic contour public-private essential couple then employs it to authenticate each other and obtain a brand new adjustable essential which works extremely well to encrypt statement. That method is determined by ECC and taken their energy commencing ECDLP and ECFP. It provides two phases: initialized phase, and confirmation phase.

1.2 Elliptic curve Diffie-Hellman protocol:

Elliptic curve Diffie–Hellman (ECDH) key agreement protocol is used for establishment of a protected statement channel among label and bookworm. ECDH allow all party have its public-private key in pair after that use it for authentication of each other and create a new key which is changeable and can be used to encrypt the communication [5]. The ECDH protocol is very easy to implement.

1.3 DNA cryptography

The DNA strands may be helpful to encode data. In security process ,the data has been produced through DNA.As the DNA cryptography could be the emerging subject just several formulas have today been planned and it's extremely definitely not the specific time implementation [11].Even even though DNA cryptography is useful but it's not as efficient than old-fashioned cryptography, But maybe it's alongside present cryptography to provide cross security[12].This security strategy been applied to protect the very first knowledge which also contains the couple of methodologies to keep and encrypt the information as it pertains to DNA sequences. The advantage of DNA security strategy is indeed it handles the couple of expanded ASCII where all type of digitized data might be encrypted. The DNA sequences might be synthesized and merged with denatured DNA or dummy DNA lengths of DNA database.

Encryption: It obtains more than one input DNA strand (considered to function as the plaintext message) append for them more than one at random construct "secret key" strands. · Resultant "tag plaintext" DNA strands are buried by integration them in a great many supplementary "distracter" DNA strands which could as well be construct by arbitrary assembly.

Decryption: It shows the familiarity with the "secret key" strands. · Declaration of DNA strands could be decrypted via several probable identified recombinant DNA division methods: Plaintext communication strand might be alienated elsewhere by hybridization with the complement of the "secret key" strands may exist put in hard hold on attractive bead or on a organized facade.

II. RELATED WORK

Want, Roy et al. [1] represented the values of RFID, discuss its main technology and application, and review the challenge organization will expressed in deploy this technology. Jannati, Hoda. et al. [3] show that Zuo's protocol is susceptible to de-synchronization assault and label impersonate in the attendance of immoral getting on holder. This paper also proposes solution to attach the refuge flaw of Zuo's GOT protocol. Ahmadian, Zahra et al. [4] proposed and well-organized ultra lightweight confirmation protocol. Though it maintain the arrangement of the additional obtainable especially trivial protocols, the process worn in it is absolutely dissimilar due to utilize of novel initiate statistics reliant permutation and evasion of modular arithmetic operation and biased logical operation such as AND OR. Tan, Chiu C, et al. [5] proposed suppler confirmation protocols that provide similar fortification with no necessitate for a middle catalog. We also propose a protocol for locked investigate for RFID tag. We consider that as RFID application turn into common, the capability to firmly explore for RFID tags will be more and more helpful. Zuo, Yanjun. et al. [6] proposed a set of protocols for secure and private search for tags based on their identity or convinced criterion they must gratify. When RFID enabled systems become persistent in our life, tag investigate become crucial. Astonishingly, the problem of RFID search has not been extensively addressed in the journalism. Zheng, Yuanqing et al. [9] proposed make use of thick approximation to professionally combined a large amount of RFID tag in order and swap such information with a two-phase approximation protocol. By approximation the connection of two dense approximation, the proposed two-phase dense approximation-based tag piercing protocol considerably reduce the penetrating time compare to all probable solution we can openly make use of commencing obtainable study.

III. PROPOSED METHODOLGY

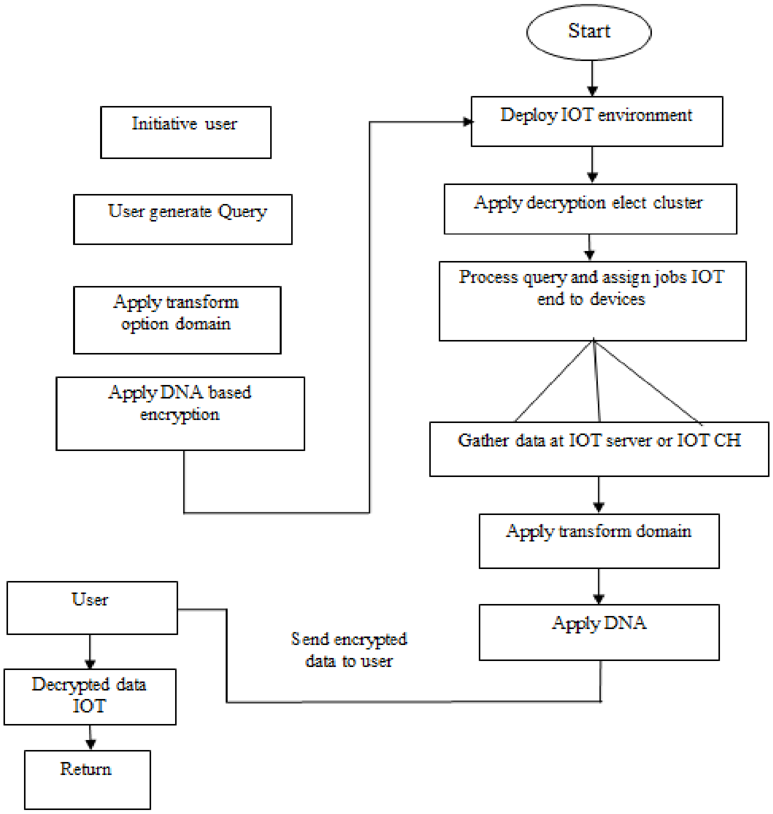
Start
Deploy IOT environment
Apply decryption elect cluster
Process query and assign jobs IOT end to devices
Gather data at IOT server or IOT CH
Apply transform domain
Apply DNA
Send encrypted data to user
Initiative user
User generate Query
Apply transform option domain
Apply DNA based encryption
User
Decrypted data IOT
Return

Fig 1: Flowchart of Proposed Methodology

IV. Gaps in Literature

The most of the existing technique have certain shortcomings because it has neglected things some of them are:

1. The speed of data transmission is still an challenging issue.
2. The use of ECC in IOT platform is still an open area of research.
3. The use of DNA based encryption technique is ignored by the most of the existing techniques by researchers in the field of IOT.

V. Analysis of Results

This section covers the cross authentication between existing and proposed techniques. The projected algorithm is tested on different plaintext. The comparison is done to show that the performance of the projected algorithm is superior to the existing techniques. For testing and execution the planned system is evaluate by means of MATLAB tool u2013a. At this time we will evaluate the performance of elliptic curve based cryptography technique with DNA based cryptography technique and evaluate the parameters. The tabular and graphical evaluations have been completed flanked by accessible and projected method on the source of parameter similar to Entropy, Time and Space.

1. Entropy:

In computing, entropy is the unpredictability collection by an operating structure or application for makes use of in cryptography or additional uses that want arbitrary facts. A lack of entropy can have a negative impact on performance and security.

$$E = -\sum_{p=0}^{255} h(p) \log_2 h(p)$$

Table no 1: Comparison of entropy

Nodes	Existing Results	Proposed Results
10	7.9999	6.3438
12	7.1364	6.7546
14	7.6627	6.2234
16	6.312	6.2042
18	5.9271	5.3378
20	6.5286	5.7949
22	6.2139	5.2804
24	5.1612	4.3022
26	5.7298	5.1883
28	5.2835	5.2004
30	5.0708	4.8507

Figure 2 has shown the graph that there is increase in entropy value of proposed method over existing method. This increase represents improvement in the encryption speed.

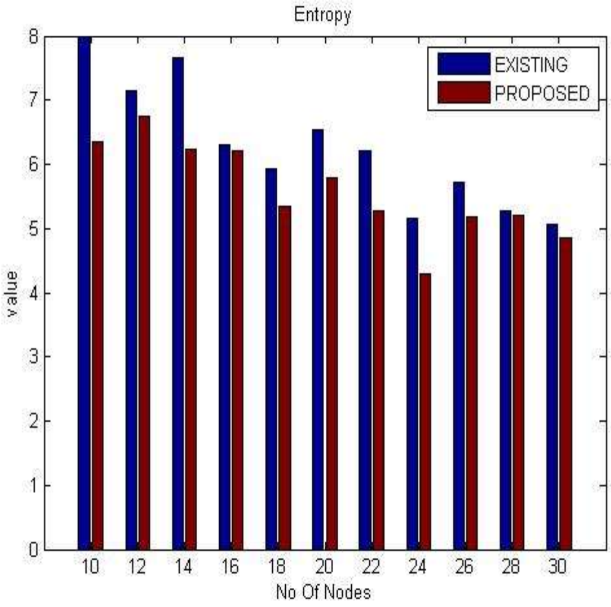

Figure 2: Performance analysis of Entropy

2. Time

The encryption occasion is base on the running time difficulty of the algorithm, duration of the key, and the plaintext dimension to exist encrypted through a variety of encryption algorithms.

Table no 2: Comparison of time

Nodes	Existing Results	Proposed Results
10	42.8949	35.5347
12	44.9947	43.0795
14	53.8295	45.6138
16	51.296	50.5962
18	53.5927	49.2983
20	63.0245	57.2663
22	65.4007	57.3729
24	60.4076	58.7316
26	70.106	64.7016
28	69.7101	68.8219
30	71.3036	68.7877

Figure 3 has shown the graph that there is decrease in time taken by proposed method in relation to existing method. This decrease represents improvement in the speed of data transfer.

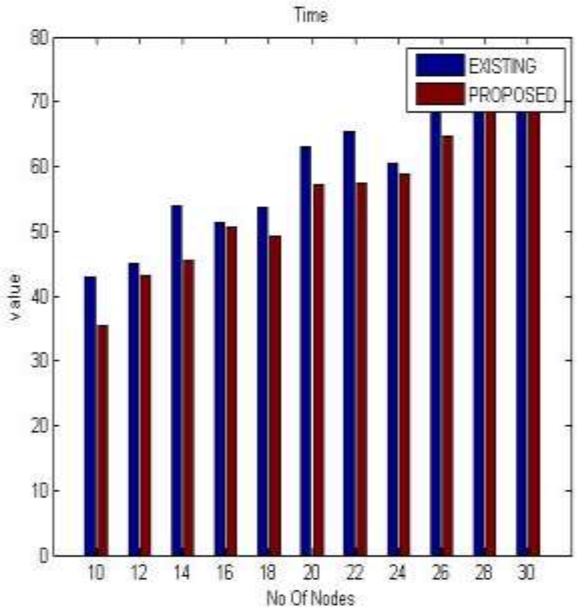

Figure 3: Performance analysis of Time

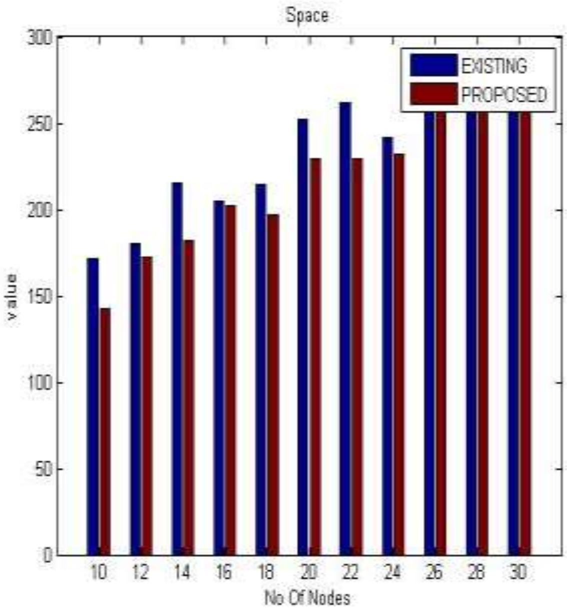

Figure 4: Performance analysis of space

3 Space:

Space Complexity of an algorithm is total space *in use through the* algorithm with high opinion to the enter size. Space complication includes mutually secondary gap and gap used by effort. Auxiliary Space is the extra space or temporary space.

Table no 3: Comparison of space

Nodes	Existing Results	Proposed Results
10	171.5797	142.1387
12	179.9789	172.3179
14	215.3179	182.4554
16	205.184	202.3846
18	214.3707	197.1933
20	252.0979	229.0652
22	261.6026	229.4918
24	241.6304	231.9264
26	280.4242	258.8064
28	278.8403	275.2875
30	285.2143	275.1508

Figure 4 has shown the graph that there is decrease in value of space used by proposed method in relation to existing method.

VI. CONCLUSION

Sequence of the internet technology has led to the appearance of internet of things (IoT). One of the recognizable deployments of IOT is all the way through radio-frequency recognition (RFID) expertise. It has been observed that in existing work has represent radio-frequency classification verification protocol base on elliptic curve cryptography (ECC) to get rid of the vulnerabilities as well as utilize selliptic curve Diffie–Hellman (ECDH) key conformity protocol to produce a impermanent mutual key used to encrypt the later transmit communication but still the speed of data transmission is still an challenging issue and the use of ECC in IOT platform has not been considered. This paper has proposed DNA based elliptic curve cryptography technique and improves the computational speed. The proposed technique is designed and implemented in the Matlab 2010a by using data analysis toolbox. The simulation result shows that by applying DNA based elliptic curve cryptography technique by using various parameters i.e. entropy, space andtime. T his proposed method show improved consequences as compare to the obtainable method. It achieves the high computational speed over the existing method.

REFERENCES

[1]. Want, Roy. "An introduction to RFID technology." IEEE pervasive computing 5.1 (2006): 25-33.

[2]. Luigi Atzori a , Antonio Iera b , Giacomo Morabito c “The Internet of Things: A survey” Computer Networks 54 (2010) 2787–2805

[3]. Y.P. Raiwani “Internet of Things: A New Paradigm” International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013

[4]. Miles, Stephen B., Sanjay E. Sarma, and John R. Williams, eds. RFID technology and applications. Vol. 1. Cambridge: Cambridge University Press, 2008.

[5]. Jannati, Hoda, and Abolfazl Falahati. "Cryptanalysis and enhancement of a secure group ownership transfer protocol for RFID tags." Global Security, Safety and Sustainability & e-Democracy. Springer Berlin Heidelberg, 2012. 186-193.

[6]. Ahmadian, Zahra, Mahmoud Salmasizadeh, and Mohammad Reza Aref. "Desynchronization attack on RAPP ultra lightweight authentication protocol." Information processing letters 113.7 (2013): 205-209.

[7]. Tan, Chiu C., Bo Sheng, and Qun Li. "Secure and server less RFID authentication and search protocols." IEEE Transactions on Wireless Communications 7.4 (2008): 1400-1407.

[8]. Zuo, Yanjun. "Secure and private search protocols for RFID systems." Information Systems Frontiers 12.5 (2010): 507-519.

[9]. Lee, Yong Ki, et al. "Low-cost untraceable authentication protocols for RFID." Proceedings of the third ACM conference on Wireless network security. ACM, 2010.

[10]. Hoque, Md Endadul, et al. "Enhancing privacy and security of RFID system with server less authentication and search protocols in pervasive environments." Wireless personal communications 55.1 (2010): 65-79.

[11]. Zheng, Yuanqing, and Mo Li. "Fast tag searching protocol for large-scale RFID systems." IEEE/ACM Transactions on Networking (TON) 21.3 (2013): 924-934.

[12]. Chen, Min, et al. "An efficient tag search protocol in large-scale RFID systems with noisy channel." IEEE/ACM Transactions on Networking (TON) 24.2 (2016): 703-716.

[13]. Piramuthu, Selwyn. "Vulnerabilities of RFID protocols proposed in ISF." Information Systems Frontiers 14.3 (2012): 647-651.

[14]. Safkhani, Masoumeh, et al. "On the security of Tan et al. server less RFID authentication and search protocols." International Workshop on Radio Frequency Identification: Security and Privacy Issues. Springer Berlin Heidelberg, 2012.

[15]. Sundaresan, Saravanan, et al. "Secure tag search in RFID systems using mobile readers." IEEE Transactions on Dependable and Secure Computing 12.2 (2015): 230-242.