International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 10 | Oct 2019 www.irjet.net p-ISSN: 2395-0072

Revisiting Security Aspects of Internet of Things for Self-Managed Devices

Sapna[1], Dr. ShashiKumar D.R[2]

[1]Assistant Professor, Department of Information Science and Engineering, Cambridge Institute of Technology, Karnataka, India
[2]Professor and Head of the Department, Department of Computer Science and Engineering, Cambridge Institute of Technology, Karnataka, India

---

Abstract - *Focusing on designing a trusted data exchange system in an IoT ecosystem using an appropriate architecture and key management techniques for ensuring the safety of the data is considered. For computers and wearable devices with restricted computing power and battery capacity, a lightweight cryptographic algorithm or greater sensor node efficiency is not yet achieved. Although many cryptosystems and algorithms are considered secured and robust, they are not considered for the devices that are resource constrained. Thus there is a requirement for an efficient algorithm to be implemented for the resource constraint devices. In this survey we will consider various security schemes for IoT with respect to security challenges like confidentiality, integrity, availability and vulnerabilities and provide solution for them.*

Key Words: IoT, key management, security, cryptosystems, ECC

1. INTRODUCTION

The popular domain of the current technological and digital world is Internet of Things. The digital era is trending in current network technologies. Data transferred from one system to another system, one computer system to other mobile devices is a common scenario .But the data communication can also take place between various things, objects, components like from washing machine to a mobile device, from a table to a fan, from a garden to a tap and many more. As the digital data generated on timely basis is increased in terms of terabytes, petabytes and trillions of bytes, there is a need for securing the data across the gateway of networks during communication. Securing the data involves providing authentication mechanisms and thus proving authorization to a system for communication. This paper reviews the various approaches for IOT security considerations and their limitations for further work.

IoT is a worldwide network infrastructure that connects physical and virtual items using information capture besides communication capabilities. This structure includes current Internet and communication network advancements. This system proposes explicit object-recognition, sensor and linking ability as per the source intended as the improvement of autonomous cooperative amenities as well as applications. These methods will remain branded with a great grade of independent information capture, incident transmission, system connectivity as well as interoperability.

2. RELATED WORK AND MOTIVATION

2.1. IoT Security considerations requirement and architecture

The architecture offered in this paper[1] is IoT reference model with Open systems. In this Technique, the model includes three mechanisms related to security that exists in each layer independently namely

- Authorization with Validation
- Encoding with Key Supervision
- Confidence with Identity Supervision

Currently in network layer, one may use 64-bit algorithm for encryption. On the other side, a 256-bit encryption algorithm can be used in information aggregation or information centralization layer. The disadvantage is that each layer-vendor needs the characteristics to be implemented and more processing power may be required. This architecture is used in smart applications.

2.2 Securing IoT with Elliptic Curve cryptography

In the proposed[2] IoT protocol for security using Elliptical Curve Cryptography mechanism, the IoT device can set secret session key using the normal p-192 Diffie-Hellman protocol. This protocol is demonstrated using MIRACL crypto library.

Figure1. highlights the architecture of IoT. All the sensor nodes are connected to the IoT handheld devices which also interact with the server and then with a gateway which in turn communicates with the clouds and databases.

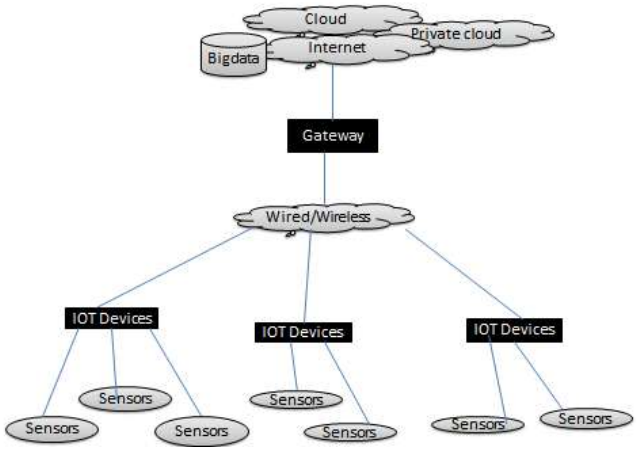

Figure 1. Architecture of IoT[2]

The major challenge in IoT is sensors. These small devices are constantly designed and intended for short power utilization by means of a tiny silicon shape aspect and frequently have restricted bandwidth as well as computational drive owing towards an 8/16 bit microprocessor. ECIOT protocol that is proposed allows encryption and decryption of the message for transfer of message among gateway as well as IOT device based on elliptical curve.

MIRACL expanded as Multiprecision Integer with Rational Arithmetic Cryptography Library an open source gold standard SDK is intended for Elliptic Curve Cryptosystems (ECC) software library frequently regarded by developers[3][4].The application of an ECIOT procedure based on this crypto package demonstrates obviously that Diffie Hellman consumes less funds on the system based on elliptic curve cryptosystem when related to Diffie Hellman on the basis of factorial problems.

In this protocol NIST p192 [5] prime field of an elliptic curve having a specific equation of a curve is recommended and coined priorly in Weierstrass formula with finite field for faster computation in IoT [6][7]. Because of the limited computational power of the 8/16-bit processor, modular reversal operation consumes more time for IoT devices. Also in integer-recoding, scalar multiplication along with addition as well as subtraction procedure was applied in ECIOT system. This technique helps in minimizing the hamming burden for integer and thus IoT devices need to expend lesser amount of memory and power for computation of session key.

2.3 ECC - enabled intercom communication mechanism between IPv4 and IPv6

This strategy [8] aims at providing security by the application of elliptic curve cryptosystem (ECC) so as to attain integrity, privacy, validation as well as non-repudiation. Small processing energy and highly resource-restricted portable and IoT appliances are the reasons why ECC is used for security. Here a fresh router scalability is suggested called as 1:N address and security system.

The model suggested includes couple of heterogeneous system networks namely IPv4-only and another one through IPv6-only hosts. Dual-stacked router was used as a translator. Dual-stacked router programmed based on the addressing system suggested is used to translate the IPv4 addresses into IPv6 and vice versa.

The suggested addressing system incorporates IPv4 address in the IPv6 prefix for IPV6 address that is IPv4-translated as well as IPV6 address that is IPv4-convertible. The IPv4 translated IPv6 id is a IPv6 id representing the IPv4 device in the IPv6 system of network .Also an IPv4-convertible IPv6 id is a IPv6 id allotted for the IPv6 device aimed at stateless conversion purposes. Both of these addressing systems apply the same 32-bit network-specific address allocated by the provider of the service as higher order bits in this proposed addressing scheme.

Elliptic curve cryptosystem is similar to RSA and El Gamal public-key crypto system. N.Koblitz[9] and Miller[10] launched it in the 1990s. ECC safety relies on the issue of Discrete logarithm of the elliptic curve[11]. It is difficult to figure out an answer for ECDLP using a bigger primitive key value within polynomial time[12]. As per all the public-key

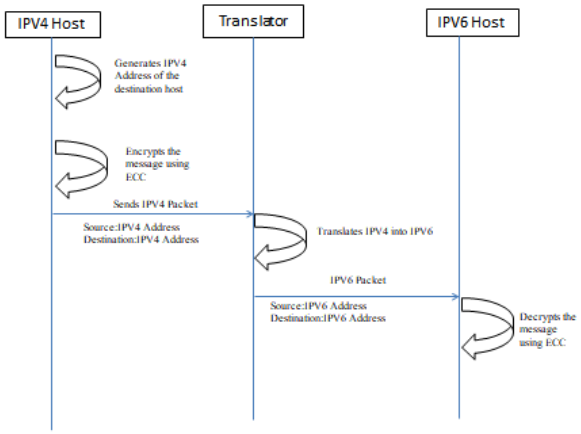

Figure 2 System diagram aimed at communication started by IPv4 [8]

cryptography with fundamental arithmetic operation, ECC includes multiplication point[13]. In a translator, thus an elliptic curve cryptosystem provides information integrity, secrecy, privacy, legitimacy, and more prominently to avoid deceiving. Although several other cryptosystems are accessible, the motive for selecting elliptic curve cryptosystem is because of its capacity being applied in resource-restricted systems, lower key magnitude, lower bandwidth ingesting, and quicker execution [14]. Each user

in ECC requires a public key intended for encryption as well as a personal decryption / signature key.

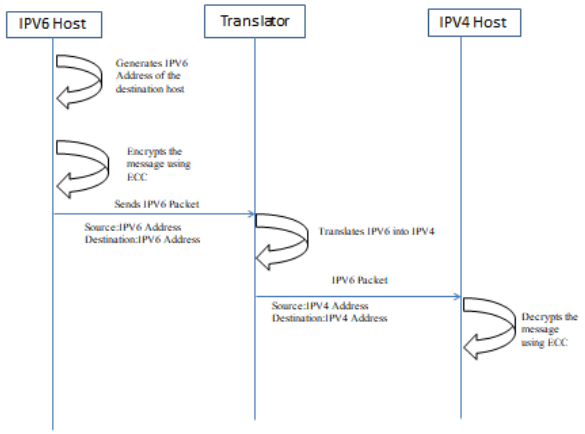

Figure 3 System diagram aimed at communication started by IPv6 [8]

The suggested model[8] is assessed by means of PC emulator, calculating round tour delay, packet accessibility, as well as hash generation interval, in addition to comparing the outcomes. Findings indicate that the ECC takes much less time than the RSA, resulting in enhanced safety with relatively less time.

2.4 An effective text encryption method with Elliptic Curve Cryptosystem

In contrast to any added public key cryptography, ECC is lightweight, effective and safer. Different techniques to translate input signal to elliptic curve point are suggested in this paper. Nevertheless for big input sizes they all lack safety, scalability and inefficiency in computation. It therefore requires a scalable as well as computationally effective procedure.

In this work [15], by arranging the ASCII keys with respect to input data as abundant as probable, the number of elliptic curve operations is reduced. Consider, for instance, the size of the input document is n numeral of data with characters, then if conversion of individual character as a point separately, the amount of elliptic curve operations is O(n) with respect to addition as well as multiplication. If the values are grouped and then applied, the process of an elliptic curve, the amount of addition operation as well as scalar multiplication operation is decreased and the period for encoding and decoding is therefore reduced. Grounded by this remark, two distinct procedures for input data using elliptic curve data point transformation is proposed to decrease the price of communication along with the price of computation.

An issue is formulated as trails: Merge a set of character type of data(their ASCIIs) with a text message and set a big amount to

- Reduce the amount with respect to addition operation as well as operation with scalar multiplication events
- Minimize encoding and decoding time
- Reduce communication costs and
- Protect the system with respect to multiple attacks

In elliptic curve cryptosystem, an input text-data is plotted to data point on an elliptic curve. Characters one by one or cluster (group of characters at a time) is shown by cluster to map input text-data to a point on an elliptic curve. In character representation, ASCII key-value of a character is represented as a point in an elliptic curve. But when groupwise mapping is considered a cluster's ASCII key-values are joined to represent a big amount by means of some feature (Totality of positional mass using base b, later mapped towards a point in an elliptic curve).Using the division method, a set of ASCII key-values is produced at the decryption end of the big amount and characters are then acquired.

This paper [15] recommends two algorithms to map signal to an elliptic curve point, namely DYNCBASE and DIGTBASE. Groups are created in both algorithms by mixing a list of ASCII values to generate big numbers for the input document. Then use Elliptic curve encoding system at the completion of the transmitter and decoding at the completion of the transmitter. The procedures suggested are performing superior than the current procedure and remain suitable for big input message. The algorithms provide the similar safety standard as the further encryption based on ECC. For the input message, the procedures are appropriate for all language type, i.e. they are scalable.

2.5 A New Effective CP- ABE Curve Cryptography using Elliptic Curve for IoT

Author suggested a novel approach of pairing-free information access controller system centred on Ciphertext-procedure attribute-based encoding (CP-ABE) by means of elliptic curve cryptosystem, abbreviated PFCP-ABE, In this paper[16], they substitute complex bilinear pairing on elliptic curves with easy scalar multiplication, thus lowering the general overhead computation. And they have developed a fresh manner of important allocation that can withdraw a user or else an attribute instantaneously without even updating the keys of additional users throughout the stage of revoking the attribute. In addition, the system uses the access structure of the Linear System of Secret Sharing (LSSS) to improve the expression of the access strategy.

In ABE scheme, the access arrangement specifies that an suitable user must need the matching characteristics in it. For instance, a Boolean formulation P ∧ Q ∧(R ∨ S) signifies that the individual who can decipher the cipher text need to

have qualities pattern P,Q,R or P,Q,S. This could also be represented in a more understandable way as shown in the figure 4, similar to an access tree.

They substituted complex bilinear coupling with easy scalar multiplication with elliptic curves in the suggested paper[16], resulting in a significant reduction in general user overhead. A fresh way of distributing key is intended to allow the system to withdraw a user or else an attribute immediately by not updating the keys of extra users. In practical implementation, this system implemented communicative LSSS access format to satisfy different access controller requirements. The assessment demonstrated the safety of the scheme and its efficiency was demonstrated by the experiments.

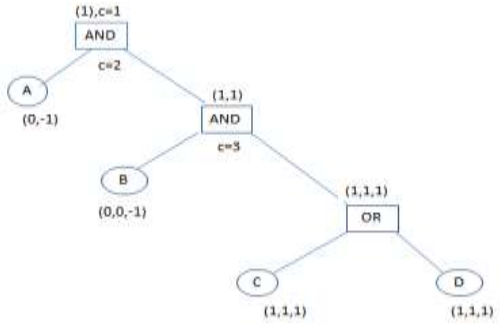

Figure 4. Labelling the access tree to produce an LSSS matrix

$$A = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \begin{matrix} p(1) = A \\ p(2) = B \\ p(3) = C \\ p(4) = D \end{matrix}$$

2.6 IoT Wireless device security

By raising the number of devices linked via the Internet through a network, IoT end users generate an estimation that customers count reaches billions by 2020, but it increases safety problems towards a extraordinary level and is therefore one and only one of the main concerns with respect to IoT safety as well as wireless devices[18].The suggested notion in the corresponding paper [17] is in the direction of generation of a very secure cryptosystem to guarantee data security, i.e. the normally encoded information can be easily violated via the attackers. The elliptic curve cryptosystem is the novel face of information security encoding.

At a stage of adding ECC, the concept suggested in the paper[17] is concerned with enhancing the safety of such machines and safeguarding data on or across the system. ECC is evolving as a unique and the greatest security practice aimed at network encoding, but any type of disruption between the transmissions when applying ECC can be a very tough task to accomplish.

ECC's encoding technique is greatly as well as stronger for breaking through and totaling this for the entire IoT network will adopt the standard level of IoT safety across all the systems and also for wireless devices as they will be the network's most susceptible targets and are most susceptible to threats. Under system of IoT safety, ECC will be applied to each layer or node at which the information is transmitted, generating a fresh random signal under these wireless systems at point which will guarantee their safety at a high place.

Key Size of ECC	Security Equivalent of RSA
224 bit	2048 bit
256 bit	3072 bit
384 bit	7680 bit
521 bit	15360 bit

Table 1 : Evaluation of Key size [17]

The key size comparison shown above demonstrates how th e ECC is better than the current techniques.

2.7 Cryptanalytics of a Protected Authentication System for IoT as well as cloud service provider using Elliptic Curve Cryptosystem

Kumariet. al. scheme [19] includes three stages as follows:

- Initialization stage - In this stage selection of secret key is done randomly.
- Registration stage -The registration stage has twofold steps. First step includes computation of separate identity say I by the embedded device and using this identity along with password it is sent to cloud service provider S. Once the cloud service provider S receives, it creates a dissimilar identity for embedded equipment and protects every related facts with respect to this identity.
- Login and validation stage

The author [19] stated their structure is secure from various assaults and offers for all safety requirements. But as per the review, we demonstrate that the job remains insecure in contradiction with various assaults like stolen-secret key attack verifier, stolen-identity attack verifier, non-session key security, lots of login attack as well as insider attack.

2.8 Validated Scyther Session Key IoT Establishment

In this paper[20] a term specific contract system grounded on elliptical curve cryptography is proposed. Also in Scyther, the system was simulated to validate it against different assaults. This paper uses Sycther [21] to model and officially verify the ECDH protocol. A protocol was suggested to

establish a session key among nodes in an IoT system. The planned protocol requires validation counter to active as well as passive attacks with the help of scythe. Establishment of Session Key remains as basic service to attain confidentiality, verification plus integrity. Term key is developed using symmetric or unequal methods. Term key methods using symmetric methods have constraints that comprise node seizure, scalability, as well as the establishment of a protected source of communication [22].

Approaches created using asymmetric cryptosystems are useful and strong in establishing a session key between two sides. There are stringent computational instruments used in IoT networks. It is not really possible to use traditional asymmetric techniques because they include high overhead cost in terms of computation. Elliptical curve cryptosystem had made lot of promise with respect to enabling of effectual cryptographic facilities in the system of networks including low energy devices .1024 bits of RSA delivers a similar security power like 160 bit of ECC. Based on ECC, Diffie Hellman is a light weight as well as an important method to set up an IoT session key. Since no authentication is provided in ECDH, it is susceptible to Man-in-the-Middle Attack(MIMA).[23][24][25] This paper uses Sycther to model and formally verify the ECDH protocol[26].A protocol for setting active term key among networking nodes in an IoT system has been suggested. The suggested protocol was authorized using Scyther in contrary to active as well as passive assaults.

Elliptical Curve Cryptography is an asymmetric method found through Victor Miller and Neil Koblitz in 1985. ECC's essence is to create quicker and more effective cryptographic processes by smaller keys. ECC power is grounded on elliptical curve computational hardness ecdlp's discrete logarithm problem[27][28][29].

Equation for elliptic curve is denoted as : $m^2 = n^3 + bn + c$,

wherein m, n, b and c will be chosen within prime fields or else from real numbers. An ECC arc using b= - 4 and c= -0.67 is represented in Figure5 [30].

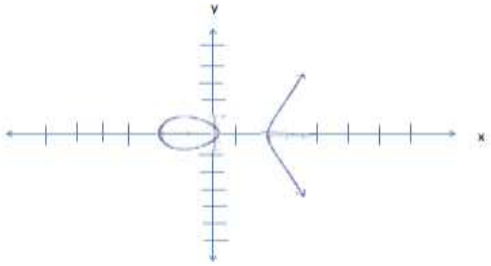

Figure 5: ECC arc using b= -4 c=-0.67 for the equation: $m^2 = n^3 – 4n + 0.67$

The significance of the IoT session key was highlighted[20]. It addressed a factual session key creation protocol for IoT, ECDH and highlighted its constraints. In Scyther, ECDH stayed demonstrated and evaluated contrary to different intimidations. Elliptic Curve Diffie–Hellman's Scyther assessment showed that it was susceptible to MIMA Attack.

MIMA Attack is not prone to the suggested protocol as rep resented in the Sycther analysis.

2.9 Lightweight ECC schema for IoT security with delicate Zero Watermarking

ECC [31] is an approach that offers security as well as privacy for a resource-specific IoT situation with great computational competence and also reduced energy intake. Yet, using EC Digital Signature (ECDSA) intended for IoT consumers involves composite actions in the creation and validation of signatures by great memory utilization. The author thus suggests a lightweight ECC Watermark schema which overcomes that limitation of ECC-based processes through a fragile zero watermarking method for authentication than digital signature. Evaluation of the current approach with related further present ECC technologies that includes ECC standard, EC-Schnorr and ECC Montgomery is done.

It is vital to ensure the integrity, confidentiality along with privacy of delicate information and people through the IoT ecosystem system. But adjusting security with confidentiality in resource-hungry, small-power as well as dissimilar networks through high productivity is an interesting task. ECC[32] is capable of meeting these requirements. As ECC needs low power, less computation, low memory but provide robust safety and secrecy in a resource-restricted IoT system, it is referred as an option for IoT network security. ECC stands as a public-key cryptography as well as public-key infrastructure centered on the complexity in calculating discrete logarithms on the set of points recognized in the elliptic curve on a finite field[32]. This also compromises the safety of standard public-key-based cryptosystem at the same level with significantly reduced sizes [33]. Various schemes are:

i) Typical ECC scheme

Elliptic Curve Integrated Encoding Scheme (ECIES) is used by the standard ECC system. For message transfer among source and destination node, mutual nodes must decide on the similar Elliptic Curve E on a binary field as a $n^2+mn= m^3+bm^2+c$ equation, where b, c $\in\{0,1\}$.Let C and D be two points on E as C=(x1,y1) and D=(x2,y2) with C≠D. Thus it is possible to calculate point point O = C+D = (x3,y3). This system includes the following steps with these coordinate points:

- Key Generation and Exchange Phase
- Encryption phase

- Transmission phase
- Decryption phase

ii) EC- Schnorr Scheme

The distinction between EC-Schnorr and standard ECC is with respect to the process of signature creation. Compared to standard ECC scheme, the amount of modular processes is condensed to minimize the computational cost of signature generation.

iii) ECC-Montgomery Scheme

As a conventional ECC schema ECC-Montgomery too resembles all its measures. Only the distinction, as stated in [34], is in the signature generations steps and the procedure from [34] is applied to implement Montgomery ECDSA.

iv) ECC Watermark Scheme

The ECC Watermark system proposed [31] is centred on fragile watermarking zero. A fragile zero-watermark is produced since the areas of the information packet header instead of adding continuous alteration by inserting additional parts into the packet payload. This system of watermark essentially gives the receiving device the legitimacy of the sender device by inspecting the watermark of the sender. Furthermore, application of ECC for encoded packets offers powerful safety as well as information secrecy by creating multiplication of curve points and adding complicated and harder to decrypt attackers. The ECC Watermark Scheme stages are as follows:

• Key Generation and Exchange Phase

• Encryption Phase

• Transmission Phase

• Decryption Phase

Analysing and comparing the system results of various schemes in this work is done: ECC Watermark, standard ECC, EC-Schnorr and ECC-Montgomery schemes in terms of memory and calculation costs. The proposed [31] ECC Watermark system, the creation and verification of watermarks need considerably less period and memory to process. This is primarily since the multiplication points of elliptic curve is needless for the creation of watermarks as well as the authenticity of a sender device is checked at a receiver node by inspecting the header source IP and protocol of the watermark data packet. With an enhanced packet information volume, after encoding information at a source device, it is noted that the ECC Watermark system has greater performance effectiveness with respect to computational price at a destination device and price of memory.

3. CONCLUSIONS

The continuing state of the IoT shows that important research remains to be done to secure embedded computer equipment. Despite the increase in the count of IoT devices as well as fresh techniques and science journals over the previous few years, safety solutions and improvements have not held pace. Publicly known breaches of safety initiation vectors point to vulnerable and/or overlooked IoT devices and the amount of stolen documents continues to increase. The quantity of information handled by IoT devices rises at exponential rates, which implies greater exposure of delicate information and raises the need for discussion among safety scientists to be encouraged.

Recent attempts have failed to cover the entire safety spectrum, revealing opportunities for studies in various fields, including intelligent object hardening and detection capacities. Current issues and difficulties should be taken as possibilities for enhancement that must be accomplished through a strict method that includes early design safety goals and the competent and effective implementation of standardized safety solutions in manufacturing phases. Final consumers also need to comprehend the device's primary goal and how to meet their demands under rigorous control and scrutiny in order to handle the interconnectivity danger that is always present.

REFERENCES

[1] Daniel Minoli ,Kazem Sohraby et al, **IoT security (IoTSec) considerations, requirements, and architectures**, 14th IEEE Annual Consumer Communications & Networking Conference (CCNC) Las Vegas, NV, USA, 2017.

[2] Darshana Pritam Shah, Pritam Gajkumar Shah, Revisting of Elliptical Curve Cryptography for Securing Internet of Things (IOT), 2018 Advances in Science and Engineering Technology International Conferences (ASET), Abu Dhabi, United Arab Emirates 2018.

[3] https://github.com/miracl/MIRACL

[4] D. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography. New York: Springer, 2004.

[5]] https://eprint.iacr.org/2013/734.pdf

[6] N. Koblitz, "Elliptic curve cryptosystems," in Mathematics of Computation vol. 48, ed: American Mathematical Society, 1987.

[7] V. Miller, Uses of elliptic curves in cryptography vol. 218: Springer, Heidelberg, 1986

[8] D. Akilandeswari, S. Albert Rabara and T. Daisy Premila Bai, ECC-Enabled Translation Mechanism for Intercommunication Between IPv4 and IPv6, 2018

International Conference on Communication and Signal Processing (ICCSP)

[9] Koblitz, N., "Elliptic curve cryptosystems". Mathematics of Computation, Vol.49, pp. 203-209, 1987

[10] V.Miller, "Uses of elliptic curves in cryptography," Crypto 1985, LCNS 218: Advances in Cryptology, Springer-Verlag, 1986.

[11] Moncef, A., Amar, S. "Elliptic curve cryptography and its applications", Proceedings IEEE International Workshop on Systems, Signal Processing and their Applications (WOSSPA), 9th-11th May, Algeria, pp. 247-250, 2011.

[12] C. Paar and J. Pelzl, Understanding cryptography, a textbook for students and practitioners. Springer Science & business Media, 2009

[13] Nejmeddine ALIMI, Younes LAHBIB, Mohsen MACHHOUT & Rached TOURKI, "On elliptic curve cryptography implementations and evaluation," IEEE in proceedings of 2nd International Conference on Advanced Technologies for Signal and Image Processing, ATSIP'2016, pp. 35-40, 2016.

[14] Xiang Wang, Liping Wang, Yuanchen Bai, Zhenxue He, Tao Wang, bin Xu, He Zhang, Xiaocui Wang, "Optimization of elliptic curve cryptography resisting power attack scalar multiplication algorithm in security system on chip," IEEE UIC-ATC-ScalCom-CBDCom-IoP, pp. 1397-1401, 2015.

[15] Prasenjit Das, Chandan Giri, An Efficient Method for text Encryption using Elliptic Curve Cryptography, 2018 IEEE 8th International Advance Computing Conference (IACC), Greater Noida, India.

[16] Sheng Ding, Chen Li, Hui Li, A Novel Efficient Pairing-free CP-ABE Based on Elliptic Curve Cryptography for IoT, IEEE Access ,2018

[17] Rishav Gauniyal, Dr. Sarika Jain, IoT Security in Wireless Devices, Proceedings of the Third International Conference on Electronics Communication and Aerospace Technology [ICECA 2019] IEEE Conference Record # 45616; IEEE Xplore ISBN: 978-1-7281-0167-5

[18] Shams Shapsough, Fadi Aloul, Imran A Zualkernan (2018), "Securing Low-Resource Edge Devices for IoT Systems", 2018 International Symposium in Sensing and Instrumentation in IoT Era (ISSI), Pages: 1-4, Year: 2018

[19] Adesh Kumari ; Vinod Kumar ; M. YahyaAbbasi et al, The Cryptanalysis of a Secure Authentication Scheme Based on Elliptic Curve Cryptography for IOT and Cloud Servers, 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida (UP), India.

[20] Ashaq Maqbool, Mohsin UI Islam et al, Scyther Validated Session Key Establishment in IoT, 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India

[21] Operational Semantics and Verification of Security Protocols[M], Berlin Heidelberg: Springer -Verlag, pp. 78-103, 2012.

[22] Xiao, Y., Ravi, V. K. and Sun, B., 2007 " A Survey of Key Management Schemes in Wireless Sensor Networks, " Elsevier Journal of Computer Communications., Vol 30, pp 2314-2341

[23] Energy Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks: Crtien etal at IFIP International Federation for Information Processing 2009

[24] Huang, X. Shah, P. G and Sharma, D. 2010 "Protecting from attacking the man-in-middle in wireless sensor networks with elliptic curve cryptography key exchange, " 4th IEEE International Conference on Network and System Security, pp. 588–593

[25] Gura, N., Patel, A., et. al 2004 " Comparing Elliptic Curve Cryptography and RSA on 8 bit CPU, " Workshop on cryptographic hardware and embedded systems

[26] Operational Semantics and Verification of Security Protocols[M], Berlin Heidelberg: Springer -Verlag, pp. 78-103, 2012.

[27] Menzes, B., "Network Security and Cryptography", Cengage Learning

[28] Hankerson, D. et al. "Guide to Elliptic Curve Cryptography" Springer.

[29] Gura, N., Patel, A., Wander, A. S, Eberle, H. and Chang Shantz, S., 2004 "Comparing elliptic curve cryptography and RSA on 8-bit CPUs". Cryptographic Hardware and Embedded Systems, vol. 3156, pp. 119– 132. Springer

[30] www.certicom.com accessed on 14-02-2019

[31] Kinza Sarwar, Sira Yongchareon et al, Lightweight ECC with Fragile Zero Water marking for Internet of ThingsSecurity, 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering.

[32] Amara, M. and A. Siad. Elliptic Curve Cryptography and its applications. in Systems, Signal Processing and their Applications (WOSSPA), 2011 7th International Workshop on. 2011. IEEE.

[33] Chatzigiannakis, I., A. Vitaletti, and A. Pyrgelis, A privacypreserving smart parking system using an IoT elliptic curve based

[34] Hossain, M.S. and G. Muhammad, Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring. Computer Networks, 2016. 101: p. 192-202.

BIOGRAPHIES

Mrs. Sapna obtained her B.E degree in Computer Science and Engineering from Visvesvaraya Technological University (VTU). She was awarded Master's degree in Computer Networks and Engineering from Visvesvaraya Technological University (VTU). She is pursuing Ph.D degree from Visvesvaraya Technological University (VTU). Currently, she is an Assistant professor in the Department of Information Science and Engineering, Cambridge Institute of Technology, Visvesvaraya Technological University (VTU). Her specializations include Computer Networks and security, Machine Learning. Her current research interests are Security in Internet of Things.

Dr.Dandinashivara Revanna Shashikumar received BE degree from Mysore University and ME degree from Bangalore University, Bangalore and Ph.D in Information and Communication Technology at Fakir Mohan University, Balasore, Orissa. He is currently working as Professor and HoD, Dept. of Computer Science, Cambridge Institute of Technology, Visvesvaraya Technological University (VTU). His research interests include Microprocessors, Pattern Recognition, and Biometrics, Computer Networks, Data mining and Data Warehouse He has published 20 research publications in referred National and International Journals. He is the reviewer for some of the International journals.