Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 9, August 2021: 6120-6129

A XOR Based Cryptography Using Cloud Agent for Security in WSN and IoT Networks

[1]Pushpinder Singh, [2]Sukhpreet Kaur
[1]Assistant Professor, [2]Research Scholar
[1]University College Ghanaur (Patiala), India
[2]Punjabi University, Patiala

Abstract

Computerized advances affected individuals' lives. Most of these computerized gadgets depend on cloud capacity to meet their memory needs. A huge number of pictures, recordings, and sound documents are being moved to distributed storage. Large number of individuals all throughout the planet access these media consistently. Unapproved admittance to these media should be stayed away from. One of the flimsy parts for information breaks is the client end encryption. This paper proposes a procedure for further developing cloud information security by consolidating the AES and blowfish encryption and decoding calculations. AES-256 is utilized as the main layer, followed by blowfish as the subsequent layer, in the crossover arrangement. The yield of the principal layer is contribution to the second layer and the eventual outcome is examined. The proposed strategy likewise talks about other consolidated approaches, for example, AES with other customary calculations however the proposed strategy gives huge results contrasted with different methodologies

Keywords: Cryptography, XOR, Cloud, AES, Cipher

1. Introduction

Cryptography: It is the process of transforming the secret data or information into a unreadable or scrambled form. In fact, it is the art of writing the message secretly. The concept of cryptography depends on five factors. These are discussed below [1]

(a) Plain text: The message or information that we want to send secretly. The set of plain text is represented by P.

(b) Cipher text: It is the scrambled or unreadable form of information or message. The set of cipher text is represented by C.

(c) Key: It is the rule with the help of which data is scrambled. The set of keys is represented by K.

(d) Encryption Function: It is the method using which the cipher text is generated. The set of encryption function is represented by E(x).

(e) Decryption Function: It is the inverse function of E(x). It is the effort to generate the original message. The set of decryption function is represented by D(x). Thus cryptography is depends on {P, C, K, E(x), D(x)}

The encryption is divided into two methods that is symmetric and asymmetric encryption where the keys are exchanged are per defined policies. The major goals of cryptography are:

Data integrity
Non-Repudiation
Access control
Authentication
Confidentiality
CRYPTOGRAPHY GOALS

Figure 1: Goals of Cryprography

2. Review of Literature

In [1] author had used a methodology of a certificate-less open key is introduced whereby the Industrial Internet of Things (IoT) can be anchored. In this methodology, the arbitrary open key is presented instead of people in the general key of the client. The proposed SCF-MCLPEKS approach has been discovered successfully and executed in less time in contrast to the methodology by Peng. In [2] Near Field Communication (NFC) is formulated and displayed by researchers in this patent. The proposed methodology incorporates the novel cryptography key utilizing the NFC and relationship with the EEPROM so a higher level of security can be accomplished.

Author had proposed a Lattice-Based Secure Cryptosystem (LSCSH) [3] for the usage of higher security in keen urban communities-based condition. The proposed methodology makes utilization of a lightweight key trade system with the anchored validation module having different layers so security can be advanced. The Access Right Verification Mechanism is utilized so the authentication can be set for the hubs in the communication situation.

In [4] author had proposed a Hybrid encryption Algorithm and the examination demonstrated that in the term of Speed and time of execution, the proposed encryption Algorithm works effective. Fundamentally, the proposed model is the blend of symmetric AES, GCM and NTRU kilter calculations so security and quicker execution are accomplished.

In paper [5] author had presented a lightweight Key foundation plot called Identity based accreditation (IBC) instrument for enhancing the communication security and protection for the key foundation. The reenactment results demonstrated that the proposed plan is protected, versatile against security assaults and fulfills the incorporated security key for IoT applications.

In [6] author had addressed the security and protection issues in the vehicle to the matrix (V2G) system of the Internet of Thing and furthermore proposed a lightweight key assertion convention for getting to be organized progressively secure and solid protection. The viability of the proposed model is spoken to by the correlation with the ECC based convention.

In [7] a CP-ABE had been proposed to protect the client properties esteems against AA dependent on 1-out-of-n obvious exchange strategy. Credits Bloom Filter adopted to secure the characteristic kinds of access arrangement in the Cipher-Text. The outcomes exhibited that the proposed model is better in the term of capability and security.

In [8] author had used a Datagram Transport Layer Security (DTLS) to addresses the difficulties through of the key commitment. The proposed method is used to exchange the key in a secured way. In [9] author used MEMK (Memory productive multi-key) calculation for the variation of the RSA. This model can trade the data between cloud to IoT and IoT to cloud. The proposed Algorithm utilized the RSA conspire with a Diophantine type of non-direct condition. The reenactment results demonstrated that MEMK is better in the term of encryption, decoding time.

In [10] a hybrid method is proposed to secure the information and to control the plot for IoT in the Fog Computing on CP-ABE and ABS. The adequacy of the proposed plan is spoken to when taken by the proposed plan for encryption, decoding and marking for the client is little and imperative. The reproduction results demonstrated that the proposed plan is secure against the assaults.

In [10] author had proposed a secure mark based Authenticated key foundation plot for IoT turn out to be progressively secure and dependable. The proposed plan security is tried by utilizing the Burrows Adadi Needham rationale, casual security and furthermore casual security confirmation utilizing broadly acknowledged robotized approval of the internet security convention and NS2 test system.

In [12] author had proposed an improvement method to balance the tradeoff among assets and execution since they both are essential in IoT arrange. In this work, a bent Edward bend with a proficiently endomorphism is additionally utilized. The creator likewise portrayed that how endomorphism misused to speed up the twofold scalar increase. 100-piece security level trade-off offers among security and execution.

A secure IoT (SIT) method proposed in [13] help in performing the lightweight encryption calculation. This is a 64-bit figure and constantly required a 64bit key to play out an undertaking and scramble information. The reenactment results demonstrated that the proposed plan gives generous security in the only five encryption rounds.

[14] The work displays a lightweight and secure client validation convention dependent on Robin cryptosystem with the attributes of the computational asymmetry. The proposed model helps dynamic security highlights. The reenactment results demonstrated that the proposed model is reasonable for furnishing security and higher productivity with a progressively adjusted way.

[15] This paper proposed a protected, haze registering based distribute buy in lightweight convention utilizing Elliptic Curve Cryptography (ECC) for the IoT organize. Fundamentally, ECC gives shorter key length, lessen message size, and lower the assets uses and fig hubs offload a portion of the computational and capacity overhead. This plan gives better versatility and less overhead, for example, stockpiling and communication.

[16] This paper proposed a Shared key synchronization technique to guarantee a start to finish security. The proposed plot synchronizes the common key without communication among gadgets

and DSM when detecting gadgets acquired a mutual key from his neighbor. The proposed plan is better from earlier DPBSV and DLSef display

[17] Author proposed another plan for enhancing the key assertion and client confirmation for heterogeneous WSN. This proposed model handles and takes out all security attacks. The security results demonstrated that this model provides higher security.

[18] This work presents Symmetric Key (S3K) for security in the IOT. S3K is a lightweight and achievable to use in the asset compelled gadgets and at the same time versatile to countless gadgets.

[19] The creator of this paper proposed a model security framework with a straightforward security highlight. The principle objective of this paper is to address the security issue and give a powerful framework.

[20] This paper proposed another framework for access control in IoT utilizing block chain innovation. This new framework influences and consistency offered block chain-based cryptography, for example, bit-coin to give more grounded and straightforward access control instrument.

[21] This paper shows the safe system design with the key trade highlight utilizing nearby robotized approved substances. The fundamental focus of this paper is to give secure system engineering. The result demonstrated that this model is preferred adaptability over SSL/TLS.

[22] This work is based on the capability-based access control model. This model uses IP based technology for the IoT based scenario. The tradeoff between security and performance is better

[23] The author proposed CLEFIA based on a lightweight block cipher algorithm. The CLEFIA is a hardware implementation and its crypto processor supports for optional key size of length 128, 192, or256 bits and it is updated version of the Generalized Feistel network.

[24] A new approach, for example cross breed Diffie-Hellman based verification plan utilizing AES and RSA for the session key age is proposed in this paper. This scheme is less 23% communication overhead than existing schemes.

[25] The author proposed a new approach to overcome the problem of the E2E security in IoT. The application and security concepts are discussed in this paper and the Cooja simulator is used to simulating the work.

[26] This paper proposed an approach by using the principle of the Lightweight identity based elliptical curve cryptography scheme and Lamport OTP algorithm. This new approach is having smaller key size and OTP for never compromising with security.

[27] This Paper proposed elliptical curve cryptography algorithm for the deal with security issues in the IoT network. Basically, ECC optimization is available for secure communication.

[28] This paper presents the framework for benchmarking of the lightweight block cipher on a multitude of the embedded platform. This platform evaluates the RAM, Footprints, and binary code size.

[29] This model architecture was developed with a focus to become the network more secure than the existing systems. This proposed model adopted better key management schemes between sensor nodes and a smart gateway. The outcome has proved that communication overhead is reduced by 26%.

[30] The proposed approach adopted Elliptic Curve Cryptography construction and the Hellman key exchange method to remove the problem of security.

[31] This paper proposed a data encryption-based model for increasing the privacy of the network and reduce the encryption time. The main focus of this paper was to develop a more secure and higher privacy-based network scheme.

[32] The author of this paper has proposed a novel framework to furnish HTTP and CoAP specialist co-ops with an authorization layer. The proposed approach is able to handle multiple smart objects with limited computational power.

[33] This paper represents the public key-based security in the IoT network. In this, the author, firstly defined components for a secure end to end communication and then introduce the public key mechanism. The computational and communication overhead is defined work effectiveness.

[34] The author developed an IP based Internet-of-Thing framework and presents in this paper. The simulation results show that this model reduces the memory overhead by 64% and computation by 97% and network transmission by 68%.

[35] This paper represents a Lightweight collaborative key exchange scheme for increasing the security of the IoT network. The proposed approach is better in the term of energy consumption reduced by 80% energy as compared to the existing approach.

[36] The author proposed a Threshold Cryptography Group Authentication (TCGA) based model. This model verified the devices available in the network to increase the security and becomes the network more reliable. This scheme is lightweight and able to detect attacks and stop them.

[37] This paper proposed an approach regarding the employment of CP-ABE on highly resource-constrained sensor nodes in the IoT environment. The Collaboration among the sensor nodes deployed in the network is higher in this approach.

[38] The author of this paper proposed a Blowfish algorithm in the FPGA using VHDL programming language. The FPGA resource consumption calculated in this paper and analyzed the performance of the blowfish algorithm. The results proved that this approach performs better in the term of security, encryption time.

[39] This paper presents the lightweight mutual authentication scheme which is validated to identify the joined device in the network before they are accessing the resources of the network and access the communication channel. The main motive of this research was to detect and prevent the attacks.

[40] This paper presents the need to develop the framework for the implementation of the lightweight version of the DTLS protocol in the IoT. The main focus of this paper was to become network secure and increase the security of the network.

3. Evaluation of Key Cryptography Approaches for the Security

An enormous assessment of the varying key cryptography approaches is finished utilizing RSA, AES and MD5 calculations with the XOR based key trade. These mixes are adopted in light of the fact that these strategies are generally utilized with the higher level of security and honesty in different stages including Cloud, IoT, Fog, Mist, Edge and numerous others.

The others can be taken; however, these are having some more noteworthy levels of scientific functions and definitions which enhance the general security. These calculations are sheltered and provide security to its clients using a complex arithmetic system. The calculations are strenuous to crack due to prime numbers factorization, which is rigid to factorize. Additionally, to muddle information these methodologies utilize the general population key and the key is kept public, in this way in the general key it is anything but hard to share people. In situations where substantial information should be muddled by related channels, the calculations can be modest. It needs a foreigner to confirm the steady quality of general keys. In public key framework information shared through the calculation could be endangered through go between who may temper with people.

Focuses allude to the scoring factor in the accompanying assessments. In genuine practice, there is no specific unit of unpredictability. It is assessed in Big-O documentation in the investigation of calculations. Enormous O documentation permits to determine the multifaceted nature of a calculation in a straightforward recipe, by expelling lower-arrange factors and consistent elements. For instance, one may state that an arranging calculation has O (n * lg(n)) unpredictability, where n is the quantity of things to sort. These are not having any units, but rather assessed in focuses or score or qualities. Huge O documentation is utilized to portray the execution or unpredictability of any calculation. Big O explicitly portrays the direst outcome imaginable, and can be utilized to depict the execution time required or the space utilized (for example in memory or on the circle) by a calculation. These are assessed in Advance Java based stage.

We have created and coordinated the code of these methodologies with some higher end APIs so the security and honesty related to these methodologies can be assessed. In addition, the methodologies are incorporated to the cloud-based stages with Java code so numerous points of view can be assessed

Following are the empirical results in Table 1 obtained from the evaluation results and overall analytics of the outcome from implementation so that the cumulative performance of the approaches can be evaluated.

Table 1: Parameter Based Evaluation of Algorithms

	RSA	**MD5**	**AES**	**XOR**
Execution Time (ms)	0.13	0.07	0.05	0.04
Complexity (Points)	71.16	40.17	32.19	27.74
Cost Factor (Points)	87	69	49	31
Performance (Points)	65	71	83	93

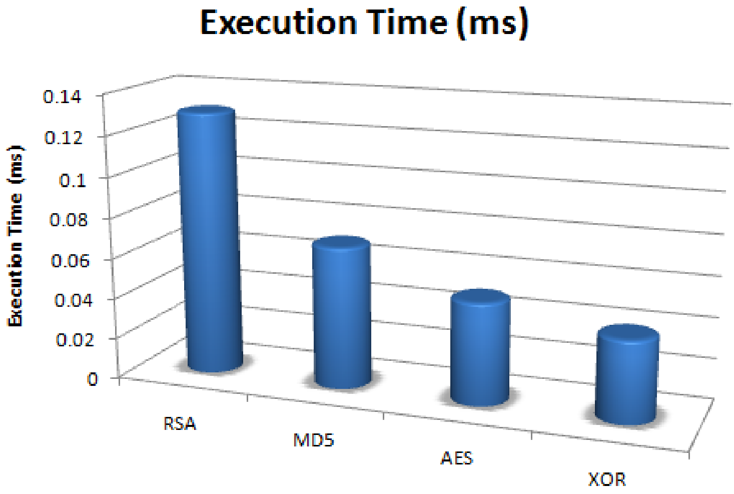

Figure 2: Comparative Evaluation of the Approaches

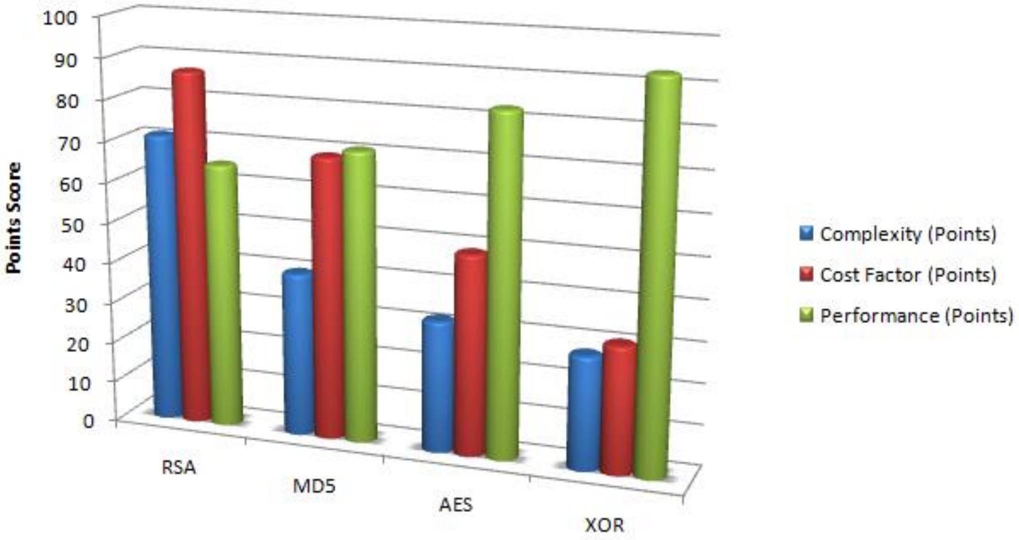

Figure 3: Comparative Evaluation of the Approaches

Conclusion

From the results and graphical view in Figure 2 and Figure 3, it is evident that the XOR based cryptography approach is still effective on multiple parameters. There is need to work on the highly effectual approach for security, including quantum cryptography that can secure the network environment with a greater level of integrity and privacy in networks. Further the cryptography can be integrated with the automated data sharing protocols to ensure the better data security and lesser load.

References

1. Ma M, He D, Kumar N, Choo KK, Chen J. Certificate-less searchable public key encryption scheme for industrial internet of things. IEEE Transactions on Industrial Informatics. 2018 Feb;14(2):759-67.

2. Minatel PH, Lee SH, Pinto BS, Boeira FC, inventors; Samsung Electronica da Amazonia Ltda, assignee. Method for Verifying Authenticity, Configuring Network Credentials and Cryptographic Keys for Internet of Things (IoT) Devices Using Near Field Communication (NFC). United States patent application US 15/365,069. 2018 May 31.
3. Chaudhary R, Jindal A, Aujla GS, Kumar N, Das AK, Saxena N. LSCSH: Lattice-Based Secure Cryptosystem for Smart Healthcare in Smart Cities Environment. IEEE Communications Magazine. 2018 Apr 1;56(4):24-32.
4. Trivedi, D. M., & Raval, T. J. (2018). Proposed Cryptographic Approach for Securing IOT Device.
5. Sani AS, Yuan D, Yeoh PL, Bao W, Chen S, Vucetic B. A Lightweight Security and Privacy-Enhancing Key Establishment for Internet of Things Applications. In2018 IEEE International Conference on Communications (ICC) 2018 May 20 (pp. 1-6). IEEE.
6. Shen J, Zhou T, Wei F, Sun X, Xiang Y. Privacy-preserving and lightweight key agreement protocol for V2G in the social internet of things. IEEE Internet of Things Journal. 2018 Aug;5(4):2526-36.
7. Han Q, Zhang Y, Li H. Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things. Future Generation Computer Systems. 2018 Jun 1; 83:269-77.
8. Banerjee U, Juvekar C, Wright A, Chandrakasan AP. An energy-efficient reconfigurable DTLS cryptographic engine for End-to-End security in iot applications. InSolid-State Circuits Conference-(ISSCC), 2018 IEEE International 2018 Feb 11 (pp. 42-44). IEEE.
9. Thirumalai C, Kar H. Memory Efficient Multi Key (MEMK) generation scheme for secure transportation of sensitive data over Cloud and IoT devices. InPower and Advanced Computing Technologies (i-PACT), 2017 Innovations in 2017 Apr 21 (pp. 1-6). IEEE.
10. Huang Q, Yang Y, Wang L. Secure data access control with Cipher-Text update and computation outsourcing in fog computing for Internet of Things. IEEE Access. 2017 Jul; 5:12941-50.
11. Challa S, Wazid M, Das AK, Kumar N, Reddy AG, Yoon EJ, Yoo KY. Secure signature-based authenticated key establishment scheme for future IoT applications. IEEE Access. 2017; 5:3028-43.
12. Liu Z, Großschädl J, Hu Z, Järvinen K, Wang H, Verbauwhede I. Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things. IEEE Transactions on Computers. 2017 May 1;66(5):773-85.
13. Usman M, Ahmed I, Aslam MI, Khan S, Shah UA. Sit: A lightweight encryption algorithm for secure internet of things. arXiv preprint arXiv:1704.08688. 2017 Apr 27.
14. Jiang Q, Zeadally S, Ma J, He D. Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. IEEE Access. 2017; 5:3376-92.
15. Diro AA, Chilamkurti N, Kumar N. Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing. Mobile Networks and Applications. 2017 Oct 1;22(5):848-58.
16. Puthal D, Nepal S, Ranjan R, Chen J. A synchronized shared key generation method for maintaining end-to-end security of big data streams.

17. Farash MS, Turkanović M, Kumari S, Hölbl M. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Networks. 2016 Jan 1; 36:152-76.
18. Raza S, Seitz L, Sitenkov D, Selander G. S3K: scalable security with symmetric keys—DTLS key establishment for the Internet of things. IEEE Transactions on Automation Science and Engineering. 2016 Jul;13(3):1270-80.
19. Huang X, Craig P, Lin H, Yan Z. SecIoT: a security framework for the Internet of Things. Security and communication networks. 2016 Nov 10;9(16):3083-94.
20. Ouaddah A, Abou Elkalam A, Ait Ouahman A. FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and Communication Networks. 2016 Dec;9(18):5943-64.
21. Kim H, Wasicek A, Mehne B, Lee EA. A secure network architecture for the internet of Things based on local authorization entities. InFuture Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on 2016 Aug 22 (pp. 114-122). IEEE.
22. Hernández-Ramos JL, Jara AJ, Marín L, Skarmeta Gómez AF. DCapBAC: embedding authorization logic into smart things through ECC optimizations. International Journal of Computer Mathematics. 2016 Feb 1;93(2):345-66.
23. Bae GC, Shin KW. An efficient hardware implementation of lightweight block cipher algorithm CLEFIA for IoT security applications. Journal of the Korea Institute of Information and Communication Engineering. 2016;20(2):351-8.
24. Mahmood K, Chaudhry SA, Naqvi H, Shon T, Ahmad HF. A lightweight message authentication scheme for Smart Grid communications in power sector. Computers & Electrical Engineering. 2016 May 1; 52:114-24.
25. Vučinić M, Tourancheau B, Rousseau F, Duda A, Damon L, Guizzetti R. OSCAR: Object security architecture for the Internet of Things. Ad Hoc Networks. 2015 Sep 1; 32:3-16.
26. Shivraj VL, Rajan MA, Singh M, Balamuralidhar P. One-time password authentication scheme based on elliptic curves for Internet of Things (IoT). InInformation Technology: Towards New Smart World (NSITNSW), 2015 5th National Symposium on 2015 Feb 17 (pp. 1-6). IEEE.
27. Marin L, Pawlowski MP, Jara A. Optimized ECC implementation for secure communication between heterogeneous IoT devices. Sensors. 2015 Aug 28;15(9):21478-99.
28. Dinu D, Le Corre Y, Khovratovich D, Perrin L, Großschädl J, Biryukov A. Triathlon of lightweight block ciphers for the internet of things. Journal of Cryptographic Engineering. 2015 Jul:1-20.
29. Moosavi SR, Gia TN, Rahmani AM, Nigussie E, Virtanen S, Isoaho J, Tenhunen H. SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Computer Science. 2015 Jan 1; 52:452-9.
30. Sciancalepore S, Capossele A, Piro G, Boggia G, Bianchi G. Key management protocol with implicit certificates for IoT systems. InProceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems 2015 May 18 (pp. 37-42). ACM.

31. Shafagh H, Hithnawi A, Dröscher A, Duquennoy S, Hu W. Talos: Encrypted query processing for the internet of things. InProceedings of the 13th ACM Conference on Embedded Networked Sensor Systems 2015 Nov 1 (pp. 197-210). ACM.

32. Cirani S, Picone M, Gonizzi P, Veltri L, Ferrari G. Iot-oas: An oauth-based authorization service architecture for secure services in iot scenarios. IEEE sensors journal. 2015 Feb;15(2):1224-34.

33. Shafagh H, Hithnawi A. Security comes first, a public-key cryptography framework for the internet of things. InDistributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on 2014 May 26 (pp. 135-136). IEEE.

34. Hummen R, Shafagh H, Raza S, Voig T, Wehrle K. Delegation-based Authentication and Authorization for the IP-based Internet of Things. InSensing, Communication, and Networking (SECON), 2014 Eleventh Annual IEEE International Conference on 2014 Jun 30 (pp. 284-292). IEEE.

35. Saied YB, Olivereau A, Zeghlache D, Laurent M. Lightweight collaborative key establishment scheme for the Internet of Things. Computer Networks. 2014 May 8; 64:273-95.

36. Mahalle PN, Prasad NR, Prasad R. Novel Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT).

37. Touati L, Challal Y, Bouabdallah A. C-cp-abe: Cooperative Cipher-Text policy attribute-based encryption for the internet of things. InAdvanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on 2014 Jun 17 (pp. 64-69). IEEE.

38. Prasetyo KN, Purwanto Y, Darlis D. An implementation of data encryption for Internet of Things using blowfish algorithm on FPGA. InInformation and Communication Technology (ICoICT), 2014 2nd International Conference on 2014 May 28 (pp. 75-79). IEEE.

39. Jan MA, Nanda P, He X, Tan Z, Liu RP. A robust authentication scheme for observing resources in the internet of things environment. InTrust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on 2014 Sep 24 (pp. 205-211). IEEE.

40. Lakkundi V, Singh K. Lightweight DTLS implementation in CoAP-based Internet of Things. InAdvanced Computing and Communications (ADCOM), 2014 20th Annual International Conference on 2014 Sep 19 (pp. 7-11). IEEE.