International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-10 Issue-4, April 2021

Survey on Securing IoT Data using Homomorphic Encryption Scheme

Anita Chaudhari, Rajesh Bansode

***Abstract**: In today's world everyone is using cloud services. Every user uploads his/her sensitive data on cloud in encrypted form. If user wants to perform any type of computation on cloud data, user has to share credentials with cloud administrator. Which puts data privacy on risk. If user does not share his/her credentials with cloud provider, user has to download all data and only then decryption process and computation can be performed. This research, focuses on ECC based homomorphic encryption scheme is good by considering communication and computational cost. Many ECC based schemes are presented to provide data privacy. Analysis of different approaches has been done by selecting different common parameters. Based on the analysis minimum computation time is 0.25 Second required for ECC based homomorphic encryption (HE).*

Keywords: IoT devices; HE; ECC; cloud data server.

I. INTRODUCTION

Large volume of data generated by IoT devices, due to memory constrain, data cannot be stored in IoT devices, so outsource data to third party storage provider. If any computation required on data, user has to download all data and then computation can be performed. Homomorphic Encryption is a terminology that provides the functionality of performing computation on encrypted data without revealing secrets. HE can be applied for securing outsourced computations, for example, securing distributed computing facilities. Also, administrations from various organizations can compute an exchanged information without revealing confidential data. HE can be utilized to secure frameworks, for example, secure casting ballot systems to crash hash capacities, private set crossing point and private data recovery plans. In industries, HE can be used to secure data. [1].Generally, in an association, the computing resource for cloud computing can only be provided by a cloud service provider. An alternative to buying the computing resources, clients can buy computing facilities from cloud providers, is greatly inexpensive than buying the computing resources [2].

Manuscript received on March 18, 2021.
Revised Manuscript received on March 25, 2021.
Manuscript published on April 30, 2021.
* Correspondence Author

Anita Chaudhari*, Thakur College of Engineering and Technology, Mumbai (M.H), India.
Rajesh Bansode, Thakur College of Engineering and Technology, Mumbai (M.H), India.

Cloud services provides benefits in terms of storage, Cloud technology allows on-demand, ubiquitous source allocation and information access to the cloud users efficiently with less infrastructure costs. service but outsourcing important and crucial data on cloud poses serious threat [3]. Luo, et al. [4] improved the levelled FHS structure by including a mingling of public-key matrices in a message-dependent based, to split message space into "identified "and "unidentified "portions by a suitable rule. This paper presents the analysis of different approaches of ECC based HE and the overview of the approaches. Finding the strength and weakness of each method is to getting future research directions. Recent Techniques and their alternatives are explored for developing ECC based HE scheme.

II. LITERATURE REVIEW

Ganapathy [5] proposed secure privacy-preserving framework using CRT for providing safety on cloud and IoT-based system. In this method, an innovative technique is presented for generation of group key for retrieving the encrypted cloud data. In this research ,it is directed for the plain text only with 1MB bits. So this may lead to various hypothetical analysis which are researched with various other bit calculations. Hou, et al, [6] presented a review on IoT security to secure data generated by sensors. This methodology survey is of three-dimensional approach to explore IoT security, i.e., with the one-stop, multi-stop and end-application dimension.Bocu and Costache, [7] implemented a HE system for maintaining healthcare data. Application that maintains personal health information using HE to preserve data Privacy. Martins and Sousa [8] explores a FHE based Cloud Computing Model. Fixed-point method offers for enhanced performance. Aung et al. [9] presented a Fully HE (FHE) , new bootstrapping algorithm which was developed for SHE system by presenting simplifications of many functions in binary arithmetic that would achieve better results. The effectiveness of bootstrapping takes place in non-binary case. Lu and Zhu, [10] proposed a Privacy-preserving distributed optimization using HE. The scheme achieves perfect accuracy and concurrently protects each member's states and coefficients from other members. Yang et al. [11] explores a public key size HE system creates on the sum of sparse subsets and integers HE system with critical public size based on summation integer of sparse subset progresses effectiveness of the novel scheme, it is shown to be semantically secured.

The future ideas lead to a novel perception of learning the FHE system is built on approximate GCD of integers. Cetin et al. [12] presents on encrypted genomic data to encrypt the records using HE in a way that permits to store data securely in the cloud, which allows capable privacy-preserving techniques for inquiring existence of specific mutations in accurate size datasets. Wang et al. [13] experimented the Cryptanalysis of a Symmetric FHE. Found that almost all the secret keys can be recovered from the randomly-generated 100 instances under different parameter settings. Advancement in crypto analysis for limited multiplications is kept for future work. Farokhi et al. [14] provides secure and separate control using semi-HE.

This paper presents the parameters of the encryption method which provide the assurance the reliability and the presentation of the closed-loop system. As projected the computational period growths with the key size; it is to achieve all the essential responsibilities if the key size is lesser than or equivalent to 256 bits within 0.1 sec sampling time.

Gomez-Barrero, et al. [15] discusses the Multi-Biometric Template Protection Based on HE overall outline for multibiometric template safety based on homomorphic probabilistic encryption, in this only the encrypted information is handled in the encrypted field, no encryptions are essential during confirmation which shows high precision rates. Given the small computational cost of the scheme and the good performance obtained (EER = 0.12%). Kalpana et al. [16] proposed a Shifted Adaption HE (SAHE) for Mobile and Cloud Learning. This method suggests a SAHE, which was observed as the improved choice for all the present investigations going on. The main difficulty is defending user's enquiries, which was lectured by considering a public key encryption method.

III. BASIC TERMINOLOGY

Elliptic Curve Cryptography(ECC)

Elliptic Curve was invented by Koblitz and Miller in 1985.ECC is a public key cryptography approach based on algebraic structure of elliptic curves over finite fields. Elliptic curve cryptography is useful in tiny environment.

= +by + a mod p (1)

x,y,a,b are real number

Elliptic curve defines mainly two fields[21],

1.Fp,where p is large prime numbers.

2. ,Binary fields.

The Elliptic curve is defined as,

Key Generation process:

Generation of Public key and private key, the sender will encrypt message using receivers public key and the receiver will decrypt message using his secret key.E is elliptic curve ,Q is point on curve, n is maximum limit, Select c within the range of n,Public key generation,

G=c*O (2)

Select c=random number selected on in a range 1—(n-1).P point on curve.

G is public key and c is private key.

Encryption process:

Sending some message to sender, represent message on curve.

Randomly select j from 1---(n-1)

C1=j*O (3)

C2=M+j*G (4)

Decryption :

M=C2-c*C1 (5)

C2-c*C1=(M+j*G)-c*(j*O) (6)

=M+j*c*O-c*j*O

=M

Homomorphic Encryption (HE)

Homomorphic Encryption method carried out on encrypted data that is cipher text instead of original text. The main thing in homomorphic encryption is after performing computation on data encrypted data, generated result should match with the computation performed on plain-text data.A function that satisfies fun(a+b) = fun(a)+fun(b) is called a homomorphism. The symbol "+" can stand for any operation,and it need not stand for the same thing on both sides of the equation. Technically + is the group operation, and if the function *fun* maps elements of one group to another, the group operation may be different in the two groups.

IoT devices using HE

Edge of Things (EoT) figures out the framework for secure and smart healthcare surveillance services. FHE preserve data privacy and is stored and processed within an EoT framework [17]. Data is verified using two level verification such as cryptography and intrusion detection techniques. Indeed, a lightweight HE gives efficient secure data aggregation with a game-theory based technique [18]. To avoid data privacy leakage, individual device initially encrypts its data using a HE schemes before submitting them to the fog nodes [19]. HE schemes provides a complete data defense on IoT, collect data from "Things", data transfer via dispersed networks, data process in data Centre and store in data warehouse. To be improved into IoT framework such as planning of the tiniest "Things" and its constrained resources, a more lightweight and high performance of HE systems is important [20,21].However, due to the problems of high computational complexity and low efficiency, HE was not suitable for high dimensional data removal, especially in the field of IoT[22]. Privacy has been separated into two main categories, context and content- oriented privacy as illustrated in Figure 1[23].

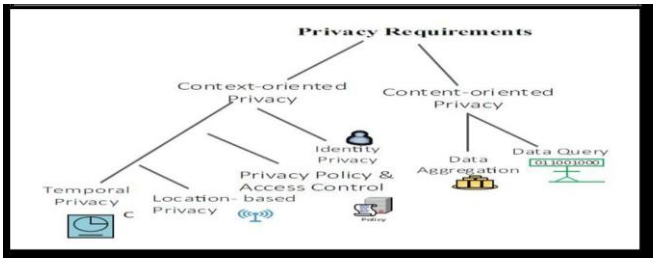


Figure 1. Privacy Requirement of IoT

ECC can be used for the HE, Private information retrieval, Short signatures, Broadcast encryption, Proofs of irretrievability, Knowledge and zero-knowledge proofs, Security threats, Challenges on data sharing, Encryption and Decryption.

MORE

Sender selects 2*2 invertible matrix A in S_n symmetric key Encryption,

Encryption:

For each plaintext input element P_i sender selects random number G_i in S_n

Pi and Gi is kept on order of diagonal of 2*2 matrix.

Matrix Method of

$$(Pi)=Bi=A\begin{pmatrix}Pi,0\\0,Gi\end{pmatrix}A^{-1}=\begin{pmatrix}b11,b12\\b21,b22\end{pmatrix} \quad (7)$$

Decryption:

$$P=(A^{-1}BA)_{11} \quad (8)$$

Eigenvector vector (1,c) of matrix B is= $A\begin{pmatrix}P,0\\0,G\end{pmatrix}A^{-1}$

(1 , c)B=(P , e·P) **Enhanced More:** (9)

Decryption of B matrix

$$P=b11+c.b21(MOD\ N) \quad (10)$$

Let B1 and B2 are encrypted values of P1 and P2,

$$MORE(B1)+MORE(B2)=P1+P2 \quad (11)$$

Equation shows More supports additive Homomorphism.

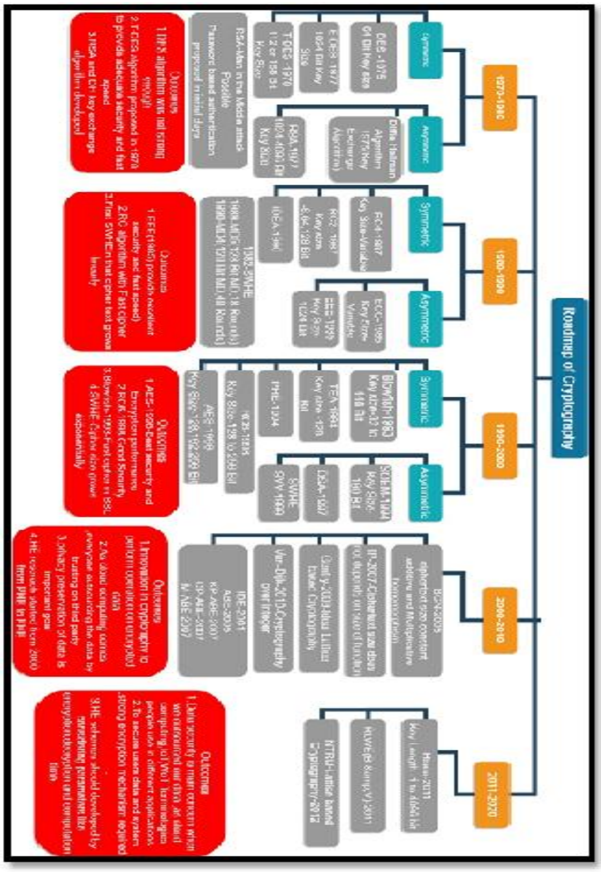
PORE:

Sender selects two polynomial number g1,g2 for symmetric key ,sender computes polynomial

$$bb(g)=(g-g1).(g-g2) \bmod N= g^2+b.g+d \quad (12)$$

Encryption:

Encryption



(Pi)=Fi.g+Hi should satisfy Fi·g1 + Hi = Pi (13)

pair (Fi, Hi) define Enc (Pi).

Sender selects a large-number mod N random Si , for Fi and solves the linear equation

Si ·g1 + Hi = Pi for Hi ; thus Hi = Pi - Si ·g1 (14)

Ciphertext(Pi)=pair(Fi,Hi)

Sender can solve the following equation by generating random Number,

Fi ·g1 + Hi = Pi , and (15)

Fi ·g2 + Hi = Si (16)

Fi = (Pi - Si)/ (g1 – g2), and Hi = Pi - Fi ·g1 = (Si ·g1 – Pi ·g2)/(g1 – g2). (17)

Additive Homomorphism:

Addition:

PORE(P1) + PORE(P2) = (F1+F2 , H1+H2) (18)

Multiplicative Homomorphism:

Multiplication:

PORE(P1) · PORE(P2) = ((F1 + H1) · (F2 + H2) – F1 · F2 · (1 + b) – H1 · H2 , (H1 · H2 – F1 · F2 · d)) (19)crypted variable denoted by a pair (F,H), decryption can by done by computing

F ·g1 + H . (20)

Keygen (,Pick up two primes p(γ), q(γ),

M=p.q (21)

G=$F_{M,n} (22)

Return M,G

Encryption :

$E(G,M,(p1,p2,---pn)$

F← $DiagonalMatrix(p1,p2,---,pn)$ (23)

Return G^{-1} .F .G

Decryption:-

D(G,M,C)

F← G.F.G^{-1} (24)

Return(F1,1,------Fn,n)

PORE and MORE algorithm required extra storage and provides less chances of attack.

Elliptic Curve Naccache-Stern (EC-NS) Encryption:

EC-OU uses discreate logarithm techniques ,so that will be easy to compute in curve,

$S_p(\bar{c}_p\ ,\bar{d}_p)$ (25)

Public Key generation:

m=h.i,c,σ,A,T_n(0,c) (26)

Secret Key Generation:

(h,i) or ε =lcm(h+1,i+1) (27)

Retrieval Number:100.1/ijeat.D23330410421
DOI:10.35940/ijeat.D2333.0410421
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Encryption: Plaintext p $\in T_{\sigma}$

n$\in NT_{m}$

ciphertext (C)=(p+$\sigma.n)$.A (28)

Decryption:

Compute $k = (^{\varepsilon}/_{\sigma})$.C=p.$A^{\iota}$ (29)

This technique attains smaller expansion and provides great efficiency

Elliptic Curve Okamoto-Uchiyama (EC-OU) Encryption:

Public key is generated, c=$a^{2}.b$,A,G,D_{c},Select private key q,

encryption performed on plain text p<2^{l-1}

b$\in_{B}.2^{2l}$

ciphertext c=p.A+b.G (30)

Decryption performed on following data, plaintext generated using,

P= $\frac{\varphi_q\ ((q+2).c)}{\varphi_q((q+2).A}$ (mod q) (31)

This algorithm provides security that is equivalent to the factorization of n. If chosen ciphertext attack applied, by considering factorization problem security will be on risk.

Elliptic Curve Paillier (EC-P) Encryption

It provides advantages over Elliptic Curve Okamoto-Uchiyama

Generate public key m=a.b,H,$T_{m^{2}}$ generate private key

$\gamma = lcm(a+2, b+2)$ (32)

In Encryption process, plaintext p $\in Z_{p}$

b$\in_{B} Z_{m}$

c=(p+m.b) (33)

In decryption process, p= $\frac{\varphi_m(\gamma.c)}{\varphi_m(\gamma.H)}$ (mod m) (34)

This scheme is better that other scheme as it decreases the expansion value from 3 to 2

Elliptic Curve Elgamal(EC-EG) Encryption:

Supports additive homomorphic property Its security is based upon the .EC-EG security based on Elliptic Curve Discrete Log Problem .
Public key generation A,q,H,D=x.H where H,D $\in G_{q}$
Secret key x$\in G_{q}$
Encryption plaintext P=maping(p)
b
Ciphertext c=(B,V) (35)
Where B=k.H ,V=P+k.D
Decryption performed on ciphertext,
P=-x.B+V=-xk.H+P+xk.H, (36)
p=reversemaping(P)

Addition two ciphertexts requires two point addition one for each generated ciphertext in given case B,V .Mapping function is used to map values into points on curve. It is compulsory that same plaintext always map wit same point on curve.

BGN-ECC ALGORITHM

Input for the following algorithm will be from different sensors data.

Key Generation Phase:

Select security parameter (γ),
Generate Public Private key pair, calculate (b1,b2,C) using security parameter γ
C=set of elliptic curve points ,to form cyclic group
ord(C)= q=b1,b2 (37)
where b1,b2 are large prime numbers.
Length of these should be equal ,len(b1)=len(b2)
Randomly select two variables, S,N
Where ord(S)=ord(N)=q
Calculate point T=b2 * N $\therefore ord$(T)=b1
Select parameter R <b1 as a maximum plaintext boundary
Generate public key P_k =(q,C,S,T,R),
Secret key S_k=b1

Encryption: (P_k,Plaintext denoted as M):

Plaintext space should belong to Sensors M $\in \{0,1,2, \ldots \ldots .., R\}$
Select random number X$\in \{0,1,2, \ldots \ldots$...,q-1)

Ciphertext generation C= M*S+X*T (38)
Return C
Addition on ciphertext of data collected from sensors,
Two ciphertext C_1,C_2
Where C_1=M_1*S + X_1*T (39)
C_2=M_2*S+X_2*T (40)
Randomly select $X^{\prime} \in \{0,1,2, \ldots \ldots$...,q-1)
Computation of additive ciphertext,
$C^{\prime}$=C_1+C_2+ $X^{\prime}$ * T (41)
=(M_1+M_2)*S+(X_1+X_2+$X^{\prime}$)*T (42)
Return $C^{\prime}$

Decryption: Decrypt ciphertext C using secret key
Calculate M=$log_{\overline{S}}$(b1*C)
=$log_{\overline{S}}\ (b_1 * (M * S + X * T))$
=$log_{\overline{S}}(b_1 * M * S)$ (43)
Where $\overline{S}$ =b_1*S (44)
M is plaintext received after decryption to valid user.
In given methodology, implemented ECC based homomorphic encryption algorithm. Exploring additive homomorphic encryption in IoT based application.

IV. ANALYSIS

To address the limitations of previous records and a comparative analysis has been done on IoT devices and computation model using HE among ECC on the cloud. The researchers had implemented different secure mechanism using partial homomorphic property, fully homomorphic property.

Based on the different parameters like computation time, communication cost, encryption time, decryption time are considered for experimentation. Main goal behind research is minimising computation overhead and algorithm should support in IoT environment without compromising security.

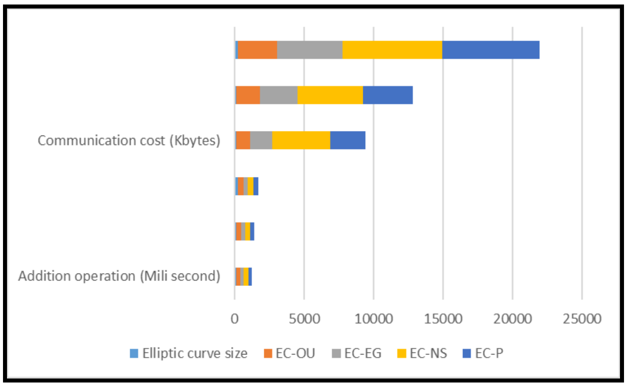


Figure 2. Comparison of Different ECC scheme

Figure 2 shows that Elliptic Curve Okamoto-Uchiyama takes more time for encryption, decryption and computation process as compared to other three algorithms. Elliptic Curve Paillier takes less time for performing addition and multiplication homomorphism on encrypted data. From analysis, we can comment that EC-P takes less time for performing computation as compared to others.

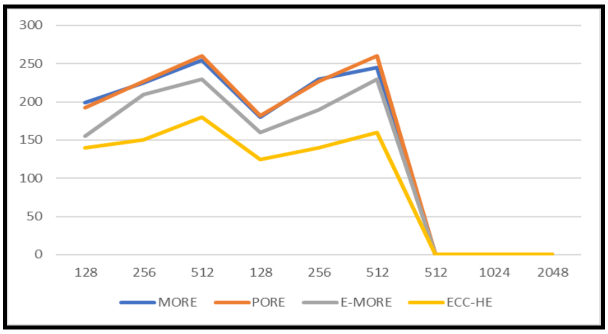


Figure 3. Comparative Analysis of Elliptic curve cryptography based on Encryption time, decryption time and Computation time

From Figure 3. Matrix Operation for Randomization and Encryption (MORE) takes more time as compared to other 3 algorithm. FH-ECC mechanism, encryption time can be improved with the linear increase in the key size (bits). From the investigation, it was detected that the FH-ECC method needs a smaller amount encryption time, decryption time and computation time compared to other methods. After analysis our comment is elliptical curve cryptography is useful in resource constrained devices and as compared to other schemes takes less computation time.

V. CONCLUSION

In this review, the researcher has presented the security and privacy difficulties in IoT devices and schemes. Authentication in IoT systems and architectures is reviewed. However, HE suffers the performance of computations. Fully HE is a solution on encrypted data, to secure cloud confidentiality, however, fully HE runs slow and the faster fully HE systems are needed. This cryptographic security algorithm has a default steps like key generation, encryption, decryption, and investigation. The latter part of work surveyed the security questions and answers in four layers. The scheme surveyed is simple and secure because the ECC is used to implement the encrypted files on a remote cloud system. Built on the exact case, completely IoT devices could be susceptible to certain kinds of attacks. Also, surveyed a security investigation and presented the security of diverse protocol under various attacks. After analysis of different ECC based encryption algorithm-P and ECC-HE gives excellent result. This research may encourage researchers in emerging new privacy preservation schemes with performance effectiveness in the context of IoT using HE with ECC.

REFERENCES

1. S. Trab, E. Bajic, A. Zouinkhi, M.N.Abdelkrim, H. Chekir, and R.H. Ltaief. "Product allocation planning with safety compatibility constraints in IoT-based warehouse." Procedia Computer Science, 73, 290-297, 2015.
2. R. Hayward, and C.C. Chiang, "Parallelizing fully homomorphic encryption for a cloud environment". Journal of applied research and technology, 13(2), 245-252, 2015.
3. S. Tahir, S. Ruj, A. Sajjad, and M. Rajarajan, "Fuzzy keywords enabled ranked searchable encryption scheme for a public Cloud environment." Computer Communications, 133, 102-114, 2019.
4. F.Luo, F. Wang, K. Wang, and K. Chen, "A more efficient leveled strongly-unforgeable fully homomorphic signature scheme." Information Sciences, 480, 70-89, 2019.
5. S. Ganapathy, "A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications." Computer Networks, 151, 181-190, 2019.
6. J. Hou, L. Qu, and W. Shi, "A survey on internet of things security from data perspectives." Computer Networks, 148, 295-306, 2019.
7. R. Bocu and C. Costache, "A homomorphic encryption-based system for securely managing personal health metrics data." IBM Journal of Research and Development, 62(1), 1-1, 2018.
8. P. Martins, and L. Sousa, L. "A methodical FHE-based cloud computing model." Future Generation Computer Systems, 95, 639-648, 2019.
9. K.M.M. Aung, H.T. Lee, B.H.M. Tan and H. Wang, "Fully homomorphic encryption over the integers for non-binary plaintexts without the sparse subset sum problem". Theoretical Computer Science, 2018.
10. Y. Lu, and M. Zhu, "Privacy preserving distributed optimization using homomorphic encryption." Automatica, 96, 314-325, 2018.
11. J. Yang, M. Fan and G. Wang, "A public key size homomorphic encryption scheme based on the sum of sparse subsets and integers." Cognitive Systems Research, 52, 543-549, 2018.
12. G. S. Çetin, H. Chen, K. Laine, K. Lauter, P. Rindal, and Y. Xia, "Private queries on encrypted genomic data." BMC medical genomics, 10(2), 45, 2017.
13. B. Wang, Y. Zhan, and Z. Zhang, "Cryptanalysis of a symmetric fully homomorphic encryption scheme" IEEE Transactions on Information Forensics and Security, 13(6), 1460-1467, 2018.
14. F. Farokhi, I. Shames, and N. Batterham, "Secure and private control using semi-homomorphic encryption." Control Engineering Practice, 67, 13-20, 2017.
15. M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on Homomorphic Encryption." Pattern Recognition, 67, 149-163, 2017.
16. G. Kalpana, P.V. Kumar, S. Aljawarneh, and R. V. Krishnaiah, "Shifted adaption homomorphism encryption for mobile and cloud learning." Computers & Electrical Engineering, 65, 178-195, 2018.
17. S. Mendhurwar, and R. Mishra, "Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges." Enterprise Information Systems, 1-20, 2019.

18. A. Alabdulatif, I. Khalil, X. Yi, and M. Guizani, “Secure Edge of Things for Smart Healthcare Surveillance Framework.” IEEE Access, 2018.
19. O.R.M. Boudia, H. Sedjelmaci, and S.M. Senouci, “Two-Levels Verification for Secure Data Aggregation in Resource-Constrained Environments.” In 2018 IEEE International Conference on Communications (ICC) (pp. 1-6). 2018, IEEE.
20. J. Ni, X. Lin, and X.S. Shen, “Toward Edge-Assisted Internet of Things: From Security and Efficiency Perspectives.” IEEE Network, 33(2), 50-57, 2019.
21. S.F. Tan, A. Samsudin, and S. Alias, “Internet of Things: Security Challenges and Its Future Direction.” In 10th International Conference on Robotics, Vision, Signal Processing and Power Applications (pp. 483-488). 2019, Springer, Singapore.
22. S Tonyali, K. Akkaya, N. Saputro, A.S. Uluagac, amd M. Nojoumian, “Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems.” Future Generation Computer Systems, 78, 547-557, 2018.
23. R. Miguel, and K.M.M. Aung, “Hedup: Secure deduplication with homomorphic encryption.” In 2015 IEEE International Conference on Networking, Architecture and Storage (NAS) (pp. 215-223). 2015, IEEE.

AUTHORS PROFILE

Anita Chaudhari, is an Assistant Professor in Department of Information Technology, St. John College of Engineering and Management, Mumbai. She received Bachelors degree from pune university in 2009 and Masters degree from Mumbai university in 2013.Currently pursuing Ph.D from Mumbai University. Her current research focuses on network security, Internet of Things.

Dr. Rajesh Bansode, is an Professor and Head of Department of Information Technology, Thakur College of Engineering and Technology, Mumbai. He received B.Tech in Electronics and Communication from J.N.T.U Hydrabad in 1999.He received his M.Tech from DAVV Indore.in 2001. He received his Ph.D in Information Technology from SGBAU Amaravati in 2016.His research interest include Network Security, Wireless Communication in MIMO OFDM, Light Weight Cryptography.