SINERGI Vol. 28, No. 2, June 2024: 405-412
http://publikasi.mercubuana.ac.id/index.php/sinergi
http://doi.org/10.22441/sinergi.2024.2.019

A superior secure key spawn using boosted uniqueness encryption for cloud computing in advanced extensive mobile network

G. Rajesh Chandra[1], K. Jagan Mohan[1], Osamah Ibrahim Khalaf[2], Guru Kesava Dasu Gopisetty[3], Dama Anand[4]*, Sameer Algburi[5], S. Vijaya Lakshmi[1]
[1]Department of Computer Science and Engineering, KKR & KSR Institute of Technology and Sciences, India
[2]Department of Solar, Al-Nahrain Research Center for Renewable Energy, Al-Nahrain University, Iraq
[3]Department of Computer Science and Engineering, KKR & KSR College of Technology and Sciences, India
[4]Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, India
[5]Al-Kitab University, College of Engineering Techniques, Iraq

Abstract
The cloud computing sector, including mobile networks has increased in the present time. Because of advanced features and security related information in cloud. So many methods are available for handling these problems. Cloud security, large number of methods existing for provide security. Among that, so many widespread techniques cast-off to protected data in cloud based on Individuality based encryption. This method specialty is allowing only authorized end users for access legal data and avoid smalevolent attack. Individuality -based encryption method follows up the four stages like Name, Key generation, encryption and decryption. Among these Key generation is most important for generating secure key. It provides unbreakable and non-derivable secure keys to provide strong security. This paper provides a novel approach for providing advanced security called identity-based encryption. This approach uses segment of a bitidentity thread in demandto evade seepage of user's data identity, if any attacker decodes the key also. Statistical reports show that the proposed algorithm takes less time in the process of decryption and encryption compared to other traditional approaches. One more feature of our novel method is skinning the user's uniqueness by using parametric curve fitting. It contains a polynomial interpolation function.

Keywords:
Cloud computing;
Encryption;
Mobile network;
Secure key generation;

Article History:
Received: November 14, 2023
Revised: January 9, 2024
Accepted: February 13, 2024
Published: June 2, 2024

Corresponding Author:
Dama Anand
Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, India
Email:
ananddama92@gmail.com

INTRODUCTION

Cloud computing is a one of the most important domainsfor all fields on requestand suitable network admission to communallot of computational resources, it can be rapidly provided with fewer administration effort. In this context there are four major features that can modify any field in cloud computing [1]. They are self-service on demand, network admission, resources, and speedy springiness. So many issues are available in cloud services like authenticity, Security and Confidentiality [2]. For different applications, authentication plays a crucial role in retaining security using unique access control [3]. Cloud encryption platforms encrypt data when it is transmitted to and from cloud-based applications and storage, as well as to authorized users in different locations.

In addition, these tools encrypt data when it is stored on cloud-based storage devices. These measures prevent unauthorized users from being able to read data as it travels to and from the cloud or read files when they are saved to cloud storage. Storage vendors like Amazon Web Services (AWS), Dropbox, Microsoft Azure and Google Cloud provide data-at-rest cloud

encryption. The software handles encryption key exchanges and the encryption and decryption processes in the background.

Two types of infrastructures most common in security approaches of public and private keys, among these two public keys is castoff to safecommunication amid two different end users. Private key indicates based on public key identity of user's email. So, private key is produced at the time of communiqué. Due to lack of prior knowledge, accuracy of encryption and decryption is very less [1]. Several computationally hard methods are available. One of the most popular methods used to secure data over the cloud is Identity-Based Encryption (IBE). It is an access policy that allows only authorized users to access legible data in order to avoid a malicious attack. IBE comprises of four stages, namely, setup, key generation or extract, encryption, and decryption.

Key generation is one of the important and time-consuming phases in which a security key is generated. It is a computational and decisional hard problem for generating unbreakable and nonderivable secure keys.

This paper proposes an enhanced identity-based encryption approach where a secure key is generated using part of an identity bit string in order to avoid leakage of users' identity even if an adversary or attacker decodes the key or encrypted data. Experiment results show that the prosed algorithm takes less time in the encryption and decryption as compared to the competitive approach named efficient selective-ID secure identity-based encryption approach. One of the most important features of the proposed approach is that it hides the user's identity by using the Lagrange coefficient, which consists of a polynomial interpolation function.

The security of the system depends on the hardness of computing the bilinear Diffie-Hellman problem. So many protocols provide security against attackers. Among that Authenticated Key Exchange protocol [4]. In this protocol activate two end users, they have username and shared key with resilient to offline attacks. AsymmetricPassword-Authenticated key exchange is the most important protocol. It delivers setting the server passcode depiction and security is obligated when the server is cooperated.

Past few decades, cloud security is the newest ranges of research and anonymous methods have been projected [5, 6, 7, 8, 9]. A framework 2F provides authentication clients, link cloud system for encryption keys for provide tight security to avoid attackers at any cost [10], it consists of seed swap for account arrangement in tunnel security of transport layer. An authentication server with encryption key and an influential decryption action, and asynchronous creation about one authentication via TOTP approach via internal memory for cloud computing [11].

Figure 1 shows a Mobile Cloud Architecture that talks about the architecture of the mobile. Figure 2 demonstrates the two users and key generator and Figure 3 talks about the entire framework of security concepts.

The development of bilinear map, IBE approach categorized into random model [12] without bilinear map [13]. Han et al. [14] presented identity-based plaintext-checkable encryption for mobile electronics trade. [15] Ma projected an identity-based encryption security apparatus named IBE with subcontracted equivalence test in the cloud setting. Qin et al. [16] focused based on an IBE system for cloud computing settings, they also use the equivalence examination and overwhelms restriction [15].

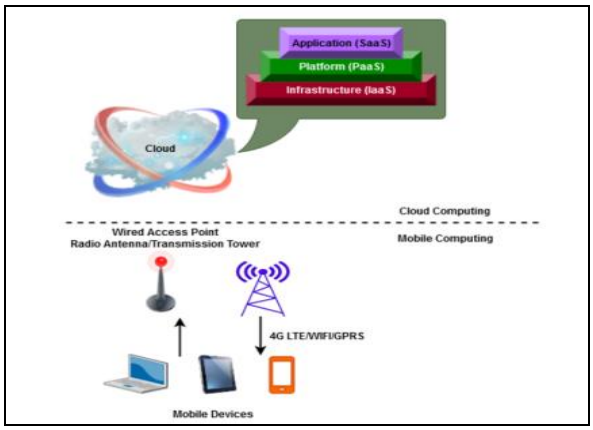


Figure 1. Mobile Cloud Architecture

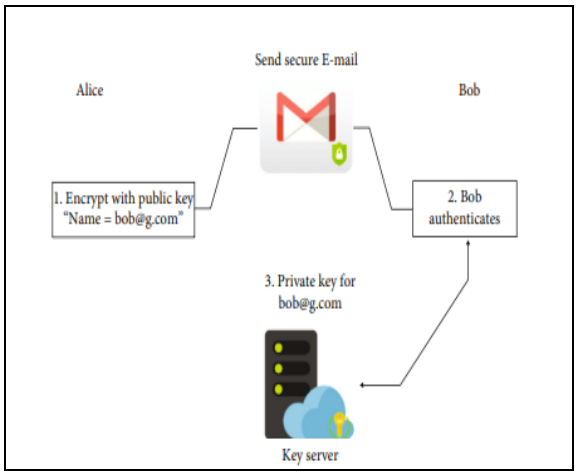


Figure 2. Users and key generator

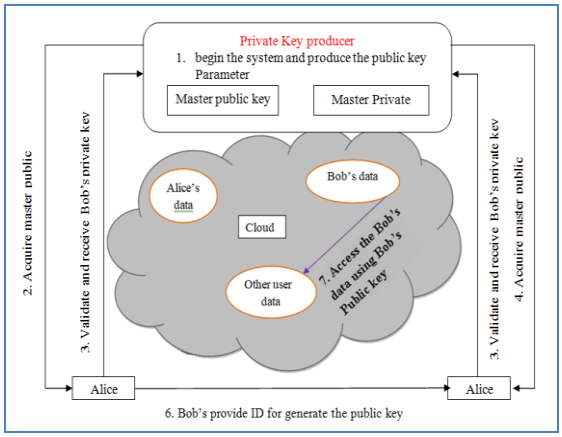


Figure 3. Framework of security concepts

This paper provides security concepts in section two. Section three provides the proposed framework. Section four provides individuality-based encryption algorithm. Section five

MATERIAL AND METHODS

Security Concepts

The major security concept shows that simulator environment response for encryption using identity-based encryption. It faces so many challenges and quires during this process. The task of decryption is plain text using identity initialization.

The following hierarchy for four different levels:

a. Setting: generate the reproduction setting as follows:
b. Simulant runs the setting of security. In this process option-1 is, d=1 because single layer protected, in multi-levelIBE, is orderedIBE f> 1.
c. After make public constraints with master key.

Algorithm

1. Parameters like bits and curves decided by Private Key generator.
2. From Private Key generator, Bobreceived the master public key.
3. Bob validates himself by distributing his uniqueness to Private Keyproducerandobtains private key for encryption.
4. From Private Key generator, Alicegets the master public key.
5. Alice validates him by distributing his uniqueness to Private Key producer and obtains private key for encryption.
6. Bob leads his uniqueness to Alice for producing the public key connected to Bob's uniqueness. Bob authentic the data, what data Alice will use for decryption using this key.
7. From database, Bob's data and getting by Alice and decrypts it for retrieving.

Data Encryption is a method of preserving data confidentiality by transforming it into ciphertext, which can only be decoded using a unique decryption key produced at the time of the encryption or prior to it. Data encryption converts data into a different form (code) that can only be accessed by people who have a secret key (formally known as a decryption key) or password. Data that has not been encrypted is referred to as plaintext, and data that has been encrypted is referred to as ciphertext. Encryption is one of the most widely used and successful data protection technologies in today's corporate world. Encryption is a critical tool for maintaining data integrity, and its importance cannot be overstated. Almost everything on the internet has been encrypted at some point.

Proposed Framework

Our novel framework, identity-based encryption plays a key role in this work. This method permitted to admission the data using its uniqueness for authentication. This type of implementation is initially done in deputation (proxy) servers for revokes the unofficial users and their storage.

General process registers their uniqueness for using the legal provision. In cloud computing safety is the most important factor for computation. Security providers implement novel schemes for providing hard security. If provides more security, then the next factor is upload and download of data from cloud. Figure 3 shows the security environment between two parties using private and public keys. Particularly in novel approach concentrate on decryption, key generation, and encryption time is computed.

In few cases unauthorized users use identity from authorized users then Lagrange polynomial used for computationally hard to third party to crack original identity [24]. In Figure 3, Bob directs his uniqueness to Alice in middle of net; an attacker can't get the uniqueness because they allocation these characteristics by means of protected socket linking [21, 22, 23, 24]. Among so many methods, Hash-based key produce approaches are more computationalexpensive, so we prefer pairing-based key produce approaches can be used [17, 18, 19, 20].

Proposed Individuality Based Encryption Algorithm

In proposed algorithm H represents the group with order q. This group derived from bilinear map H1. It defined as:

e: H× H1➔H2 (1)

The cluster size finding by safety parameter and every parameter represents the four strings of length m4.

ID = (id1, id2, id3…. idn) (2)

Proposed Algorithm
Step 1: Start
Step 2: Bilinear mapping between variables with collision free hash function.
Step 3: Generate System parameters and random selection with length n.
Step 4: Finally, setup the public parameters with master key.
Step 4: Generate the bit string identity for end user
Step 5: It divides into two dissimilar parts.
Step 6: A random value added for security to proposed method.
Step 7: Identity generated by choosing a random value(that is Private Key)

$$d_u = (h_2^{\tau}(v' \prod_{j \epsilon U} v_j), h^r \quad (3)$$

V = {v1, v2,…, vm} and U ={u1,u2,….un} such that
Step 8: Now use Parametric curve fitting method to generate polynomial function to perform polynomial interpolation for hide few values for recovered existing data.

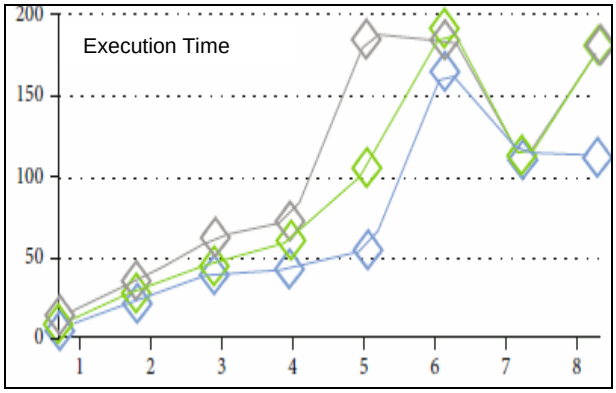
s=∫t2t1√(dxdt)2+(dydt)2dt (4)

Step 9: The random set generated for each user identity and generated parametric curve fitting for each identity for each identity value.
Step 11: System will use m terms of identity value due to hacker can't guess the original identity of authorized user.
Step 12: Now if all the values of user identity and system identity are same, so error rate is zero.
Step 13: So hacker will not be able to guess anything from the key.
Step 14: Finally do the encryption and decryption as stated in (6)-(11).

In preprocessing stage execution time of bilinear mapping with the help of Java pairing based cryptography library and pairing based library. The PBC value at o.4.7 and 0.3.14. JPBC provides a wrapper around PBC by means of a tiny and well-organized layer that enables communication between the two libraries.

Analytical server of cryptography, on deals with what will have to do be. In this type of research, the variables involved are carefully and scientifically controlled and manipulated. Analytical research is also known as experimental research and is a very sophisticated technique. This kind of research is based on four important characteristics namely, control, manipulation, observation and replication.

Figure 4 shows the bilinear mapping pairing at the time preprocessing. It shows the difference between before preprocessing and after preprocessing.



Pairing based library

Figure 4. Bilinear mapping execution time of using Pairing encryption and java pairing version (preprocessing stage)

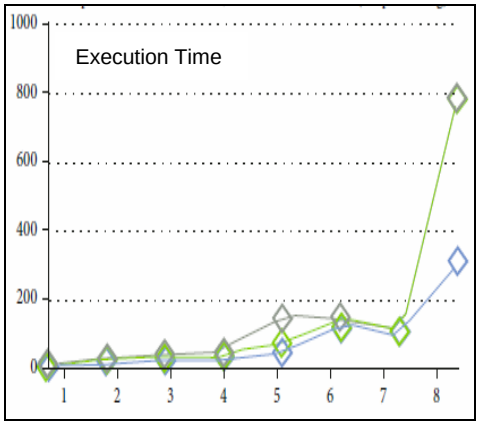


Figure 5. Pairing based library

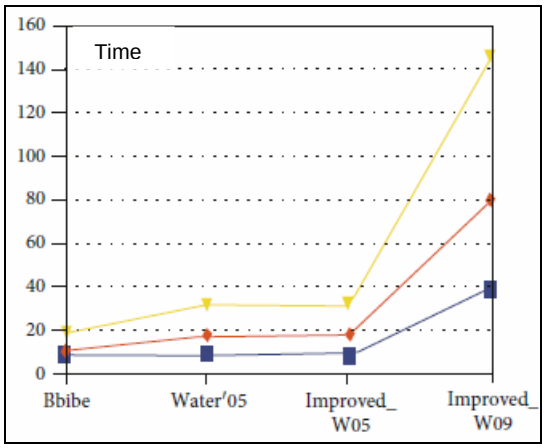


Figure 6. Individuality based Encryption

Lagrange coefficient is

$$\Delta_{j,u}\Sigma_{j=0,l\epsilon U}^{m}(\Pi_{0<j<m,i\neq j}\frac{y-y_i}{y_j-y_i})y_k \quad (5)$$

Where y= vjand x= up:

Lagrange coefficient determines the function's cost, evenparameters are not spaced. The above equation is used to calculate the value of independent variable x that agrees to a given function cost.

For every user identified one time from random set uiit is generated by Lagrange coefficient with same value. There is possibility to use m-terms of identity value; it is constant for standard identity of certified user. So, it is impossible to guessextracted ID generated by key. Due to such type of user identity error is zero.

Initial Encryption: Let “b” consider as random value. For few individualities, (5) describes the encryption performance.

$$B = (g(h1,h2)N,h,(v^{\prod_{j=U} u_j} \quad (6)$$

Secondary Decryption. Let B= ðB1, B2, B3Þ be a suitable ciphertext for notethat M is under user individualityv. So ciphertext, B can be decoded using fu= ðf1, f2Þ has given in (7)– (11):

$$C = \left(g(h_1,h2)N, e^c, \left(v'\prod_{j=u} ui\right)\right) \quad (7)$$

$$= (g(h1,h_2)^c M)\frac{e\left(g^r,(u'\prod_{i=V} v_i)^c\right)}{e(g_2^{\alpha},(u'\prod_{i=V} v_i)^r,g^c)} \quad (8)$$

$$= \left(g(h_1,h_2)^c N\right)\frac{e\left(g,(u'\prod_{i=V} v_i)^{rc}\right)}{e(g_1,g_2)^c e((u'\prod_{i=V} v_i)^{rc},g)} \quad (9)$$

$$= \left(g(h_1,h_2)^c N\right)\frac{e\left(g,(u'\prod_{i=V} v_i)^{rc}\right)}{e(g_1,g_2)^c e(g(u'\prod_{i=V} v_i)^{rc})} \quad (10)$$

$$= N \quad (11)$$

Figure 5 tells about bilinear mapping execution time using Pairing encryption and java pairing version

Figure 6 tells about Timing graph of Individuality based encryption schemes for setup phase

Table 1: Decryption phase comparison of proposed and Water’s method.

Figure 6: key generation stage time graph for

Figure 7: Decryption stage Timing graph for proposed task

Figure 8: Encryption stage timing grph for the proposed task

RESULTS AND DISCUSSION

Performing identity-based encryption by JPBC is more efficient withdissimilarkinds A, A1, F (159,201,224), G, D, and H (149) combinations for develop bilinear charting. Among these, kind of A is cast-off as perfect curve for cryptography andit customs super singular curve X2 = Y3 + X. Figure 6, Figure 7, Figure 8 show the bilinear mapping of JPBC and PBC before preprocessing and after preprocessing and shows time variation also. Table 1 shows the bits essential by curvature category and the pre offerings implanting degree of each curve.

Figure 6 demonstrates the processing time necessary by proposed individuality-based encryption, better W09, and enhancedW05, Water 05, and BBibe for SS512 curvature in the generation of crucial stage. Among these methods, BBibe take less computational time for key generation and provide tight security.

Table 1. The bits essential by curvature category

Decryption	Water’s Individuality based encryption	Projected Method
Computation of Bilinear map	2	2
Cluster operation	1	1
Transposal	1	1

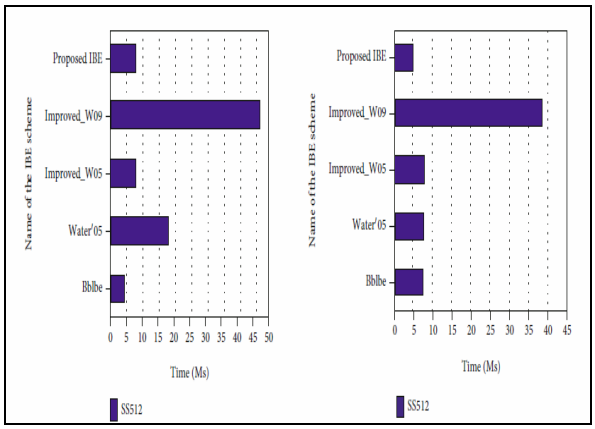


Figure 6. The processing time necessary

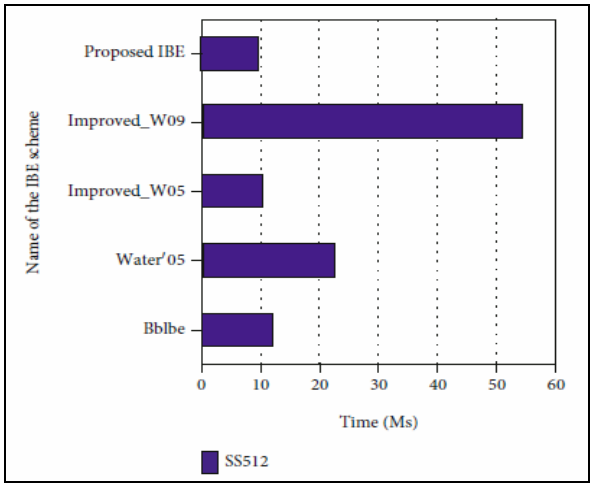


Figure 7. The processing time engaged

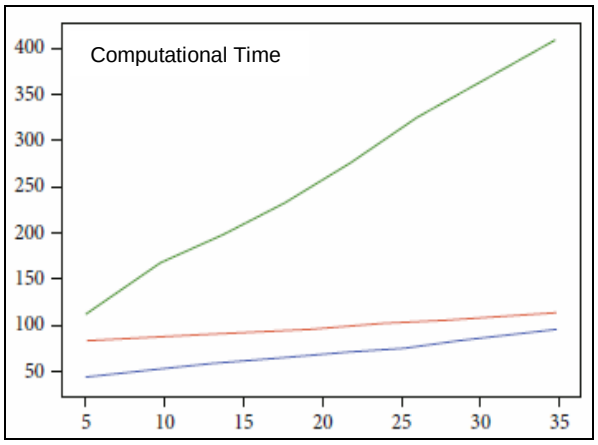


Figure 8. The decryption stages

Figure 7 describe the processing time engaged by dissimilar approach during the encryption stage. The projected novel technique is added effective and takings fewer calculation time in encryption stage, while executing the encryption using SS512 curve.

Figure 8 shows decryption stage, it proves proposed method is efficient and takes less computational time. Figure 9 describes the entire phase's encryption, decryption, security and computational time of proposed method for different messages. Results of this article got high accuracy comparing to existing results of previous work done [26] with high accuracy we can say our work is good. In these results we got better accuracy results comparing to previous works [8].

CONCLUSION

Cloud security, large number of methods existing for provide security. Among that, so many widespread techniques cast-off to protected data in cloud based on Individuality based encryption. This method specialty is allowing only authorized end users to access legal data and avoidsmalevolent attack. Individuality -based encryption method follows up the four stages like Name, Key generation, encryption, and decryption. Among these Key generation is most important for generating secure key. It providesunbreakable and non-derivable secure keys for provide strong security. This paper provides a novel approach for providing advanced security called identity-based encryption. This approach uses segment of a bit identity thread in demand to evade seepage of user's data identity, if any attacker decodes the key also. Statistical reports show that the proposed algorithm takes less time in the process of decryption and encryption compared to other traditional approaches. One more feature of our novel method is skinning the user's uniqueness by using parametric curve fitting.

REFERENCES

[1] K. Lee and J. Park, "Identity-based revocation from subset dereference methods under simple assumptions," *IEEE Access*, vol. 7, pp. 60333–60347, 2019, doi: 10.1109/ACCESS.2019.2915373

[2] K. Latha and T. Sheela, "Block based data security and data distribution on multi cloud environment," *Journal of Ambient Intelligence and Humanized Computing*, 2019.

[3] T. Joseph, S. A. Kalaiselvan, S. U. Aswathy, R. Radhakrishnan, and A. R. Shamna, "A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 6, pp. 6141–6149, 2021, doi: 10.1007/s12652-020-02184-8

[4] S. Jarecki, H. Krawczyk, and J. Xu, "OPAQUE: an asymmetric PAKE protocol secure against pre-computation attacks," in Advances in Cryptology – EUROCRYPT 2018, *Lecture Notes in Computer Science*, vol. 10822 pp. 456–486, Springer International Publishing, Cham, 2018, doi: 10.1007/978-3-319-78372-7_15

[5] D. Boneh and M. Franklin, "Identity-based encryption from the Weil Pairing," *SIAM Journal of Computing*, vol. 32, no. 3, pp. 586–615, 2003, doi: 10.1007/3-540-44647-8_13

[6] R. Langrehr and J. Pan, "Hierarchical identity-based encryption with tight multi-challenge security," in *IACR International Conference on Public-Key Cryptography*, pp. 153–183, Cham, 2020, doi: 10.1007/978-3-030-45374-9_6

[7] M. Xuecheng and D. Lin, "Generic Constructions of Revocable Identity-Based Encryption," in Information Security and Cryptology. Inscrypt 2019. *Lecture Notes in Computer Science*, Z. Liu and M. Yung, Eds., vol. 12020, Springer, Cham, 2020, doi: 10.1007/978-3-030-42921-8_22

[8] B. Waters, "Efficient identity-based encryption without random oracles," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, *Lecture Notes in Computer Science*, vol. 3027, pp. 114-127, Berlin, Heidelberg, 2005, doi: 10.1007/978-3-540-24676-3_14

[9] A. S. Rajawat, P. Bedi, S. B. Goyal et. al., "Securing 5G-IoT Device Connectivity and

Coverage Using Boltzmann Machine Keys Generation," *Mathematical Problems in Engineering*, vol. 2021, Article ID 2330049, pp. 1-10, 2021, doi: 10.1155/2021/2330049

[10] M. L. T. Uymatiao and W. E. S. Yu, "Time-based OTP authentication via secure tunnel (TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystore," *2014 4th IEEE International Conference on Information Science and Technology*, Shenzhen, China, 2014, pp. 225-229, doi: 10.1109/ICIST.2014.6920371.

[11] M. Obaidat, J. Brown, S. Obeidat, M. Rawashdeh, "A hybrid dynamic encryption scheme for multi-factor verification: a novel paradigm for remote authentication," *Sensors*, vol. 20, no. 15, ID: 4212, 2020, doi: 10.3390/s20154212

[12] B. Waters, "Efficient identity-based encryption without random oracles," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 114-127, Berlin, Heidelberg, 2005, doi: 10.1007/978-3-540-24676-3_14

[13] M. Zheng, H. Zhou and G. Cui, "An Improved Identity-Based Encryption Scheme Without Bilinear Map," *2009 International Conference on Multimedia Information Networking and Security*, Wuhan, China, 2009, pp. 374-377, doi: 10.1109/MINES.2009.171.

[14] J. Han, Y. Yang, X. Huang, H. Yuen, J. Lie, and J. Cao, "Accountable mobile E-commerce scheme via identity-based plaintext-checkable encryption," *Information Sciences*, vol. 345, pp. 143-155, 2016, doi: 10.1016/j.ins.2016.01.045

[15] S. Ma, "Identity-based encryption with outsourced equality test in cloud computing," *Information Sciences*, vol. 328, pp. 389-402, 2016, doi: 10.1016/j.ins.2015.08.053

[16] L. Qin, Z. Cao and X. Dong, "Multi-Receiver Identity-Based Encryption in Multiple PKG Environment," *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, New Orleans, LA, USA, 2008, pp. 1-5, doi: 10.1109/GLOCOM.2008.ECP.360.

[17] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," Proc. CRYPTO, *Lecture Notes in Computer Science*, J. Kilian, Ed., vol. 2139, pp. 213–229, 2001, doi: 10.1007/3-540-44647-8_13

[18] P. Ponpurmpoon and P. Hiranvanichakorn," A Pairing-free Identity-based Cryptosystem Using Elliptic Curve Cryptography," *International Journal of Network Security*, vol. 24, no. 4, pp. 695-706, 2022, doi: 10.6633/IJNS.202207 24(4).12

[19] D. Boneh and X. Boyen, "Efficient selective-ID secure identity based encryption without random oracles," in *International conference on the theory and applications of cryptographic techniques*, pp. 223–238, Berlin, Heidelberg, 2004, doi: 10.1007/978-3-540-24676-3_14

[20] S. Joshi, S. Stalin, P. K. Shukla et al., "Unified Authentication and Access Control for Future Mobile Communication- Based Lightweight IoT Systems Using Block chain," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 8621230, pp. 12, 2021, doi: 10.1155/2021/8621230

[21] H. Wang, Z. Zheng and L. Wu, "Hierarchial Identity-Based Encryption Scheme from Multilinear Maps," *2014 Tenth International Conference on Computational Intelligence and Security*, Kunming, China, 2014, pp. 455-458, doi: 10.1109/CIS.2014.112.

[22] C. Cocks, "An identity-based encryption scheme based on quadratic residues," in Cryptography and Coding. Cryptography and Coding 2001. *Lecture Notes in Computer Science*, B. Honary, Ed., vol. 2260, Springer, Berlin, Heidelberg, 2001, doi: 10.1007/3-540-45325-3_32

[23] S. Chatterjee and P. Sarkar, "On (Hierarchical) Identity Based Encryption Protocols with Short Public Parameters (With an Exposition of Waters' Artificial Abort Technique), *International Journal of Applied Cryptography*, 2011, doi: 10.1504/IJACT.2013.053434

[24] Y. Ren, S. Wang, X. Zhang and Z. Qian, "Fully Secure Anonymous Identity-Based Encryption under Simple Assumptions," *2010 International Conference on Multimedia Information Networking and Security*, Nanjing, China, 2010, pp. 428-432, doi: 10.1109/MINES.2010.96.

[25] R. Gupta, K. K. Almuzaini, R. K. Pateriya, K. Shah, P. K. Shukla, and R. Akwafo, "An Improved Secure Key Generation Using Enhanced Identity-Based Encryption for Cloud Computing in Large-Scale 5G," *Wireless Communication and Mobile Computing Journal*, vol. 4, no. pp. 1-14, 2022, doi: 10.1155 /2022 /7291250.

[26] D. Anand, O. I. Khalaf, F. Hajjej, W. K. Wong, S. H. Pan, G. R. Chandra, "Optimized Swarm Enabled Deep Learning Technique for Bone Tumor Detection using Histopathological Image," *SINERGI*, vol. 27, no. 3, pp. 451-466, 2023, doi: 10.22441/sinergi.2023.3.016

[27] N. Lilansa, M. N. Rizal, P. Anggraeni, N. J. Ramadhan, "Implementation consensus algorithm and leader-follower of multi-robot system formation," *SINERGI*, vol. 27, no. 1, pp. 46-56, 2023, doi: 10.22441/sinergi. 2023.1.006