Khan et al LGURJCSIT 2019

ISSN: 2521-0122 (Online)
ISSN: 2519-7991 (Print)

LGU Research Jounral for
Computer Sciences & IT

Vol. 3 Issue 4, October - December 2019

An Intelligent and Secure Communication of AIoT enabled Devices empowered with IPK Algorithm

Muhammad Adnan Khan[a], Muhammad Sarfraz[b], Muhammad Asif[b], Muhammad Saleem[b], Muhammad Yousaf[b]

[a] Department of Computer Science, Lahore Garrison University, Lahore, Pakistan.
[b] School of Computer Science, National College of Business Administration & Economics, Lahore, Pakistan.

Abstract:

Artificial intelligence Internet of Things (AIoT) will be a necessary part of our lives in the near future. It will be found as quick cooperation in our surroundings through the related sensor-based system. To be sure, even in an indirect method, it will serve us in a couple of structures as esteem included organizations over the cell stages. With the AIoT structures that make usage of data, actually, the data collection from contraptions can in like manner be a goal of cyberattacks. Device to Device (D-2-D) interchanges in AIoT was planned alongside various shows, for instance, Constrained Access Protocol (CoAP). Its huge stresses in the course of action of AIoT are to ensure the security of mechanisms and D-2-D one place to another. Furthermore, present correspondence shows for AIoT are without reliability features. It is a result of this that countermeasures in perspective on encryption are starting at now getting importance. There is a requirement for a solid cryptosystem for D-2-D in AIoT. In this investigation paper, we present an encryption technique which is indicated as EPEB as a security answer for AIoT. The proposed methodology works with the message which shows special characters, numbers, and bits for data encryption and decryption. In authority, the end key isn't known so we would encryption to able have the option to gadgets data using particular keys and scramble packet per special key.

Keywords: AIoT, D2D Communication, Encryption, Decryption, CoAP, secure communication algorithm.

1. Introduction

AIoT is creating advancement which can irritate the present examples in Information and Communication Technologies (ICT). It has been proposed as a critical bit of related living. As it will be a basic piece of the lives of people there are a couple of challenges. The AIoT has made new characteristics by interfacing various devices to the structure, yet has similarly motivated security threat getting the opportunity to be basic issues as found in the continuous reports of illegal observation camera control and vehicle hacking, etc. IoT is as of now required to apply encryption to sensor contraptions in conditions with various constraints that have not previously been at risk to encryption. Improvements zone for cutting edge things, Information Technology Communication and IPV6 (Internet show) are empowering quick arrangement of action of AIoT wherever on the world. It is assessed that billions of IoT contraptions will be sent in the next 5 years [1]. IoT approach is vast in number and used to given responses for an enormous number for enhanced issues. Regardless of the way that IoT has some portion of potential outcomes in the propelled world, in the midst of its course of action, it encounters a couple of issues with respect to (w.r.t) heterogeneity of devices, device character, contraption organization, a safety device to device correspondence (D-2-D, etc [2]. To empower the reconciliation and administration of heterogeneous IoT gadgets, models, for example, Ubiquitous Sensor Network (USN), Sensor Web Enablement

(SWE), and so forth, are proposed [2]. Here, the security of contraptions, (for instance, discount extortion, data uprightness), D-2-D correspondence, etc, are not tended to altogether.

Cryptography is exhaustively named Symmetric, Asymmetric and Hybrid based [15]. Exactly when cryptography has a spot with the amiss sort, by then it has open and private keys. At present Public Key Cryptography (PKC) [6], [8], [10], [13], [16], [18] accept a key part in a couple of zones, for instance, Banking, Online purchasing, E-mail, etc., Due to this, there is the high peril of getting attacked [9], [19] through estimating the remarkable RSA riddle keys from general society type. A part of the progressing varieties of RSA with respect to their execution examination [3], [5], [11], [12], [14], [17], [19], [20], [22] and memory prerequisites of key [7].A segment of the PKC is appropriate for a multi-key age plot [20], [21], [23], [24] for capable sharing of information among the substances like IoT and Cloud enlisting. Here we have examined the multi-key-based cryptosystems with reuse of keys are according to the accompanying: Enhanced and Secured RSA based Key Generation (ESRKG) [4], Dual RSA [8], Trivial RSA [7], and N-prime RSA. In these varieties, the quality insignificantly depends upon the N-bit moduli and on account of this, the time-memory tradeoff in like manner gets extended. Regardless, the IoT based device has the inconsequential gear basic, for instance, low power and low estimation of around 2K bits. Remembering the true objective to achieve high-security quality, we propose here the IPKS plan for encryption for D-2-D correspondence in IoT.

I. Literature Review

In [25], ABE is associated with assurance security for IoT in perspective on nonspecific Publish-Subscribe structure. By then we battle, IoT contraptions produce only two or three little bit of data and to perform encoding on two or three little parts of data both ABE and AES [42] encryption systems turn out the computational raised for IoT devices.

A critical analysis of the security concerns of the internet of things (IoT) dissects the security issues and challenges and gives a well-characterized security system as the secrecy of the client's protection and security which could result in its more extensive selection by masses[22].

This Enabling information assurance through PKI encryption in IoT m-Health gadgets introduces a framework dependent on Gateways (GW) that total wellbeing sensor information and resolve security issues through advanced testaments and PKI information encryption[23].

In this paper author looks at the improvement of a cloud-based, versatile IoT back-end structure and administrations dependent on top for managing and dealing with vehicular data in various use case circumstances: CAN data gathering, remote device blasting, Eco-driving, atmosphere projection, and guess. The fundamental variation is an Infrastructure-as-a-Service (IaaS) plan with a reference execution passed on an Open Nebula based cloud. The second cycle continues running on a private Platform-as-a-Service (PaaS) cloud-dependent on the Cloud Foundry arrange inside the premises of a vehicle supplier association. The two varieties have been viably evaluated and endorsed with benchmarks[24].

In the paper, the author centers around information ingestion and amassing perspectives, putting in verification issues and plans. The course of action proposed has been made and associated concerning the Sii-Mobility national splendid city adventure on flexibility and transport joined with organizations. Sii-Mobility is grounded on Km4City theory and instruments for keen city-data accumulation and organization creation [25].

Various sequences of action keeping an eye on data aggregation while ensuring the security, for example, security, uprightness, approval, and openness, can be found in the composing [30]-[41]. Makers sketched out a middleware in light of the Pub-Sub plan in [27]. Here security of endorser's bit of leeway and private of disseminated substance are guaranteed by utilizing engaging Predicate Based Encryption (PBE) and CP-ABE. Basically in [26], [28], makers delineated an arrangement for Pub-Sub building using CP-ABE KP/plans. Here every supporter characterizes separating ventures as passage systems in light of this and in KP-ABE, crush performs leak of messages by executing encoded look on mixed qualities. Thusly, it propels message to proposed endorsers.

To ensure message security Publisher scrambles message using CP-ABE and appropriates it. In [29], Tariq delineated security plans using IBE and ABE to engage privacy and approval. Here it

empowers wholesalers to sign and encode events in the meantime by using IBE and in like manner engage productively controlling of mixed events (from merchants to supporters) by means of Searchable Encryption. Advance Subscribers affirm the imprints identified with all of the qualities (of an event) using CP/KP-ABE. Most of these plans delineated is sensible for nonspecific Pub-Sub models. Thusly a point by point considers is required for the credibility of altering these designs for IoT. From now on toward this way, we propose and execute improved designs for secure EPEB, which engages secure AIoT.

It is the upgraded variety of Vigenere figuring. Security examination displays that the proposed upgraded outline is much secure as emerge from customary Vigene re-figure.

II. Proposed Intelligent Privacy Key (IPK) Algorithms for AIoT Devices Communication

In this research, an Intelligent Privacy Key(IPK) encryption algorithm is proposed for data security in AIoT gadgets correspondence in an intelligent way.

A. Highlights of proposed techniques:

Some fundamental features of the proposed system for data protection are given beneath: Proposed method relies upon the symmetric key planning that is essentially speedier than an awry key calculation:

- The proposed strategy relies upon the symmetric key calculation that is essentially speedier than an uneven key calculation.
- Key create strategy is exceptionally unpredictable
- what's more, strong. (inappropriate bullet)
- The unique cryptographic key for each customer.
- It takes after a poly-alphabetic substitution procedure that replaces plain substance character with various figure characters.
- Repeat examination and cryptanalysis are incredibly problematic that makes our techniques much secure.

B. Proposed Method in IoT Framework:

In the underlying advance, the IoT gadget will exchange the data at the IoT server. At the point when data will send that point in the second step, the key is acquired b/w IoT first gadgets and different gadgets. In the third step, the send data will be encrypted with the help of the encryption key. In the fourth step, the encoded data will be placed in IoT gadgets. At whatever point any IoT gadget will get to the required data, the IoT gadget will affirm the other gadget and give the required data in the decrypted form.

There are 9 major steps of proposed algorithms. 1-5 steps for sender device end and 5-9 steps for receiver device end.

- Encrypt the message with an encryption key
- Encrypt training bits with encryption key
- Addition of encrypted message with encrypted training bits
- Final encrypted message sends to receiver device using IoT platform
- At receiver end separate encrypted message and encrypted training bits
- Secure Communication of IoT based Devices using EPEB Algorithm.
- Key generate from encrypted training bits
- Decrypt encrypted message using key (those obtain from above step)
- Finally, receive an original message at the receiver end

device.

In given method key will be created b/w IoT 1st device which send the information & other IoT device. It like a symmetric key, so the key remains the same at both the sender and receiver side.

A. Encryption for Message at Sender Device:

Once the key is selected then encrypt message and training bits with this key and adding an encrypted message with encrypted training bits and final encrypted message transferred to receiver device with want to communicate with sender device using IoT platform. The system of encryption by proposes approach can be effortlessly comprehended with help of piece outline figure 1.

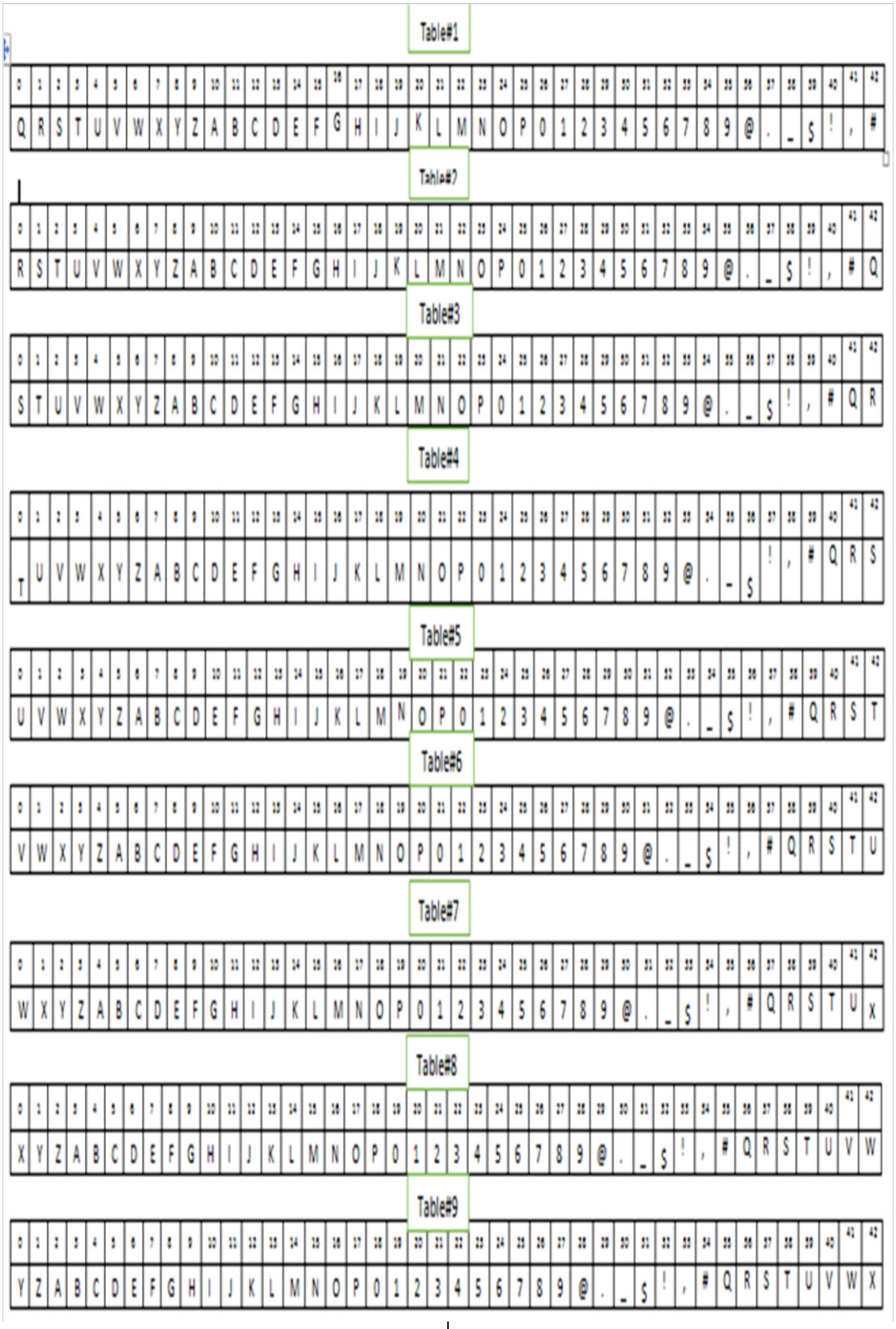

Table 1-9. Numeric, Alpha and special character values

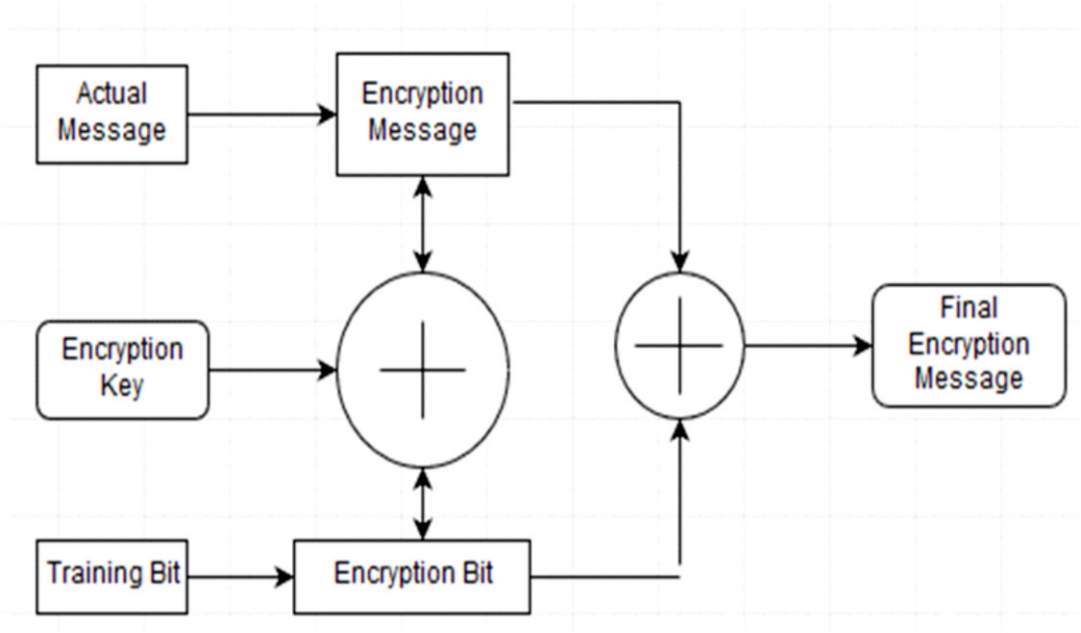

Figure 1. Encryption Message Method

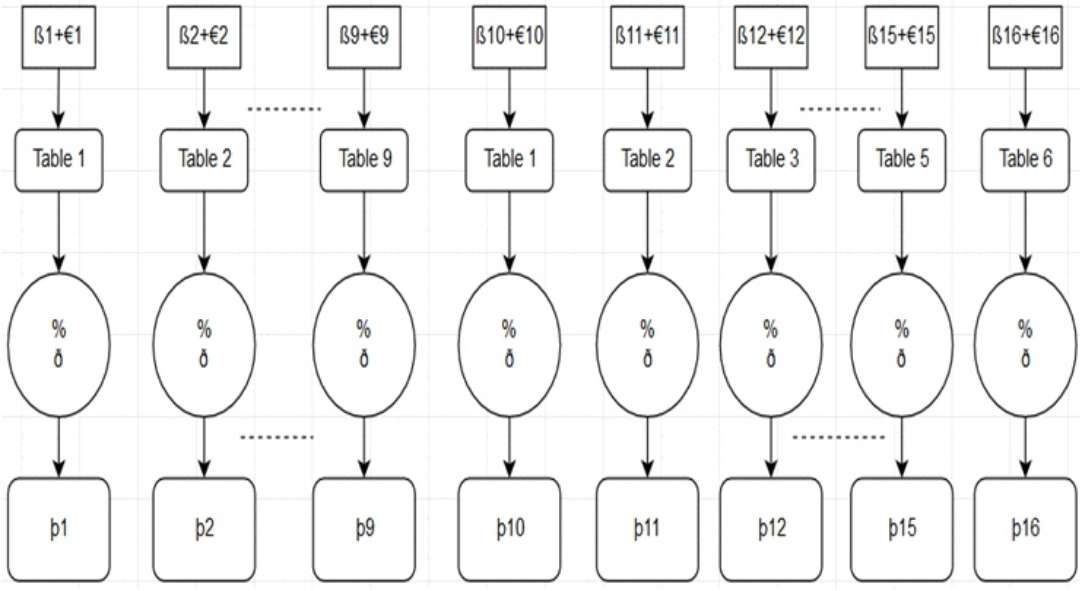

Figure 2. Message Encryption for Proposed IPK Algorithm

The formula for D2D encryption for final message is:
ßf= þi+ Ði
ßf= Final encrypted Message text character in the proposed method.
þi= Encrypted message in the proposed method.
Ði= Encrypted training bits character in the proposed method.

1. Original Message Encryption with Key: (Wrong heading number?)

In our proposed method first letter set of message phrase & key is encoded by using table no. 1 and second letter set message phrase & key encoded by utilizing table no. 2 and vice versa. This is repeated again and again up to table no 9. At that point 10th letters in order of message phrase & key encoded by table no 1 vice versa. Encryption formula for message is:

Where,

þi =ßi + €i
þi= Encrypted message in proposed method.
ßi= Original message text character in the proposed method.
€i= Key phrase character in the proposed method (for shorter length key repeat).
ð = alphabet length in the proposed method.
We can additionally simplify the proposed formula as:

þ1 = ß1 + €1 (% ð) {from table 1, in which Q=0, R=1, S=2……. #=42}
þ2 = ß2 + €2 (% ð) {from table 2, in which R=0, S=1, T=2……. Q=42}
þ3 = ß3 + €3 (% ð) {from table 3, in which S=0, T=1, U=2……. R=42}
.
.
.
þ8 = ß8 + €8 (% ð) {from table 8, in which X=0, Y=1, Z=2……. W=42}
þ9 = ß9 + €9 (% ð) {from table 9, in which Y=0, Z=1, A=2……. X=42}
þ10 = ß10 + €10 (% ð) {from table 1, in which Q=0, R=1, S=2……. #=42}
þ11 = ß11 + €11 (% ð) {from table 2, in which R=0, S=1, T=2……. Q=42}
þ13 = ß13 + €13 (% ð) {from table 3, in which S=0, T=1, U=2 … … . R=42}
þ 14 = ß 14 + €14 (% ð) {from table 4, in which T=0, U=1, V=2……. S=42}
Examples:
Let us we consider this, our Message text is "H.NO#10, LHR, PK" & key phrase is "MOR@GMAIL.COM" as shown in table 10.

Original message	H	.	N	0	#	1	0	,	L	H	R	,	P	K
Key	M	O	R	@	G	M	A	I	L	.	C	O	M	M

Table 10. Message and Key Phrase

Þ1 = ß 1 + €1 (ð %) = H + M (ð%) = 17 + 22 = 39 = $ {TABLE-1}
þ2 = ß 2 + €2 (ð %) = + O (ð%) = 36 + 23 = 59 (43%) = 16 = H {TABLE-2}
þ3 = ß 3 + €3 (ð %) = N + R (ð%) = 21 + 42 = 63 (43%) = 20 = M{TABLE-3}
.
.
.
þ8 = ß8 + €8 (ð %) = + I (% ð) = 34+ 11 = 44 (%) = 2 = Z {TABLE-8}
þ9 = ß9 + €9 (% ð) = L+ L (% ð) = 13 + 13 = 26 = 8 {TABLE-9}
þ10 = ß10 + €10 (% ð) = H+. (% ð) = 17 + 37 = 54 (43%) = 11 = B {TABLE-1}
þ11= ß11 + €11 (% ð) = R + C (% ð) = 0 + 11 = 11 = C {TABLE-2}
þ12= ß12 + €12 (% ð) = , + O (% ð) = 39 + 22 = 61 (43%) = 18 = K {TABLE-3}
þ13= ß13 + €13 (% ð) = P + M (% ð) = 22 + 19 = 41 = R {TABLE-4}
þ14= ß14 + €14 (% ð) = K + M (% ð) = 16 + 18 = 34= _ {TABLE-5}

Original Message	H	.	N	0	#	1	0	,	L	H	R	,	P	K
Key	M	O	R	@	G	M	A	I	L	.	C	O	M	M
Encrypted	$	H	M	E	B	R	4	Z	8	B	C	K	R	_

Table 11. Encrypted Message

2.Training Bits Encryption with Key:

The formula for training bits encryption is Ð i = µ i + € i
Ði= Encrypted training bits character in the proposed method.
µi= Training bits character in the proposed method.
€i= Key phrase character in the proposed method (In the event that key length is shorter than the length of plain text then the key will be repeated).
ð = alphabet length in the proposed method.
Ð1 = µ1 + €1 (% ð) = N + M (% ð) = 23 + 22 = 45(43%) =2= S {TABLE-1}
Ð2 = µ2 + €2 (% ð) = E + O (% ð) = 13 + 23 = 36 = {TABLE-2}
.
.
.
Ð8 = µ8 + €8 (% ð) = + I (% ð) = 30 + 11 = 41 = V { T A B L E - 8 }
Ð9 = µ9 + €9 (% ð) = N + L (% ð) = 15 + 13 = 28 = @ { T A B L E - 9 }
Ð10 = µ10 + €10 (% ð) = E +. (% ð) = 14 + 37 = 5 1 (4 3 %) = 8 = Y { T A B L E - 1 }
Ð11 = µ11 + €11 (% ð) = T + C (% ð) = 2 + 11 = 1 3 = E { T A B L E - 2 }
Ð12 = µ12 + €12 (% ð) = + O (% ð) = 35 + 22 = 5 7 (4 3 %) = 1 4 = G { T A B L E - 3 }
Ð13= µ13 + €13 (% ð) = P + M (% ð) = 22 + 19 = 4 1 = R { T A B L E - 4 }
Ð14 = µ14 + €14 (% ð) = K + M (% ð) = 16 + 18 = 3 4 = _ { T A B L E - 5 }

Finally, your encrypted bits will be in shown in table 12:

Training bit	N	E	X	L	I	N	X	.	N	E	T	.	P	K
Key	M	O	R	@	G	M	A	I	L	.	C	O	M	M
Encrypted bit	S	.	W	C	4	!	C	V	@	Y	E	G	R	_

Table 12. Encrypted bits

3. Final encrypted message

Now we add encrypted message and training bits by utilizing table 1-9 accordingly represented in table 13:

Encrypted message	$	H	M	E	B	R	4	Z	8	B	C	K	R	_
Encrypted training bit	S	.	W	R	4	!	C	V	@	Y	E	G	Q	_
Final Encrypted message	,	B	P	2	1	6	@	A	J	J	P	9	,	4

Figure 3. Decryption Message Method

In the proposed method at the receiver end, we received the message in the encrypted form like this “, BP216@AJJP9,4”. Now we separate encrypted training bits and messages using table 1-9 as shown in table 14.

Encrypted Training Bit	S	.	W	R	4	!	C	V	@	Y	E	G	Q	_
Encrypted message	$	H	M	E	B	R	4	Z	8	B	C	K	R	_

Table 14. Encrypted bits and message

1st find encryption key from encrypted training bits, when the proposed system finds the optimum key then decrypts the given a message. The formula for D2D decryption for final encrypted message

ßi =þi -€i

ßi= Final encrypted Message text character in the proposed method.
þi= Encrypted message in the proposed method.
€I= Encryption key character in the proposed method.

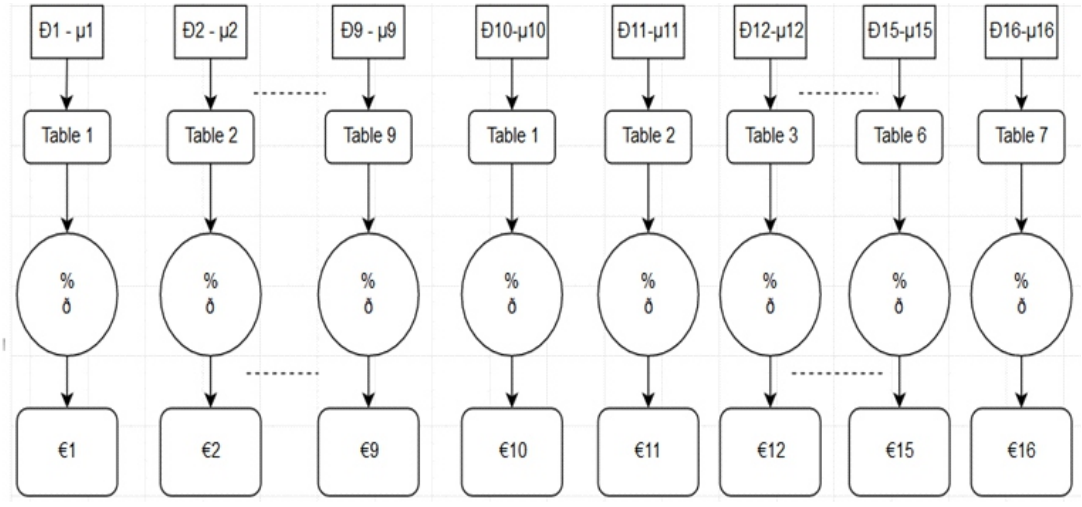

Figure 4. Key decryption from training bits for proposed IPK algorithm

For the following above example:
€1 = Ð1 - µ1 (% ð) = S - N (% ð) = 2 - 23 = -21(43%) = 22= M {TABLE-1}
€2= Ð2 – µ2 (% ð) =- E (% ð) = 36 – 13 = 23 = O {TABLE-2}
.
.
€8 = Ð8 – µ8 (% ð) = V - (% ð) = 41 - 30 = 11 = I {TABLE-8}
€9 = Ð9 – µ9 (% ð) = @ - N (% ð) = 28 - 15 = 13 = L {TABLE-9}
.
€9 = Ð9 – µ9 (% ð) = @ - N (% ð) = 28 - 15 = 13 = L {TABLE-9}
€10 = Ð10 – µ10 (% ð) = Y - E (% ð) = 8 - 14 = -6(43%) = 37= {TABLE-1}
€11 = Ð11 – µ11 (% ð) = E - T (% ð) = 13 - 2 = 11 = C {TABLE-2}
€12 = Ð12 – µ12 (% ð) = G - (% ð) = 14 - 35 = -21(43%) = 22= O {TABLE-3}
€13 = Ð13 – µ13 (% ð) = Q - P (% ð) = 41 - 22 = 19 = M {TABLE-4}
€14 = Ð14 – µ14 (% ð) = _ - K (% ð) = 34 - 16 = 18 = M {TABLE-5}

At last, the proposed method generated decrypted key from training bits will be shown in table 15.

Encrypted Training bit	S	.	W	R	4	!	C	V	@	Y	E	G	Q	_
Key	N	E	X	L	I	N	X	.	N	E	T	.	P	K
Encrypted bit	M	O	R	@	G	M	A	I	L	.	C	O	M	M

Table 15. Encryption key generation.

Now proposed method use this key for decrypting the encrypted message.

2. Decryption of Encrypted Message using Obtaining Key:

Figure 5 shown the decryption procedure given below:

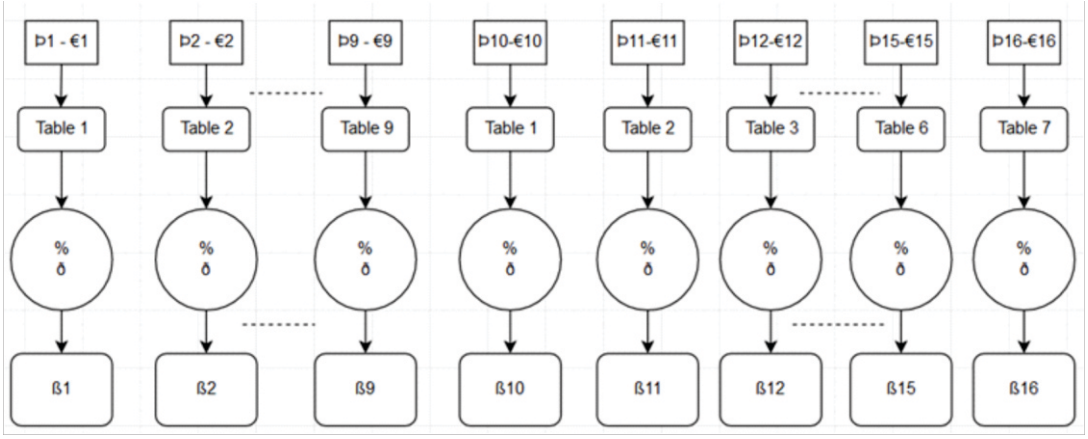

Figure 5. Message decryption using the key for proposed IPK algorithm

The formula of original message decryption is:

For the following above example:
ß1 = Þ1 - €1 (% ð) = $ - M (% ð) = 39 - 22 = 17 = H {TABLE-1}
ß2 = Þ2 – €2 (% ð) = H - O (% ð) = 16 – 23 = -7 (43%) = 36 =. {TABLE-2}
.
.
.
.
ß8 = Þ8 – €8 (% ð) = Z - I (% ð) = 2 -11 = -9 (43%) = 34 = {TABLE-8}
ß9 = Þ9 – €9 (% ð) = 8 - L (% ð) = 26 - 13 = 13 = L {TABLE-9}
ß10 = Þ10 – €10 (% ð) = B - (% ð) = 11 - 37 = -26 (43%) = 17 = H {TABLE-1}
ß11 = Þ11 – €11 (% ð) = C – C = (% ð) = 11 – 11 = 0 = R {TABLE-2}
ß12 = Þ12 – €12 (% ð) = K - O (% ð) = 18 – 22 = -4 (43%) = 39 = , {TABLE-3}
ß13 = Þ13 – €13 (% ð) = R - M (% ð) = 41 – 19 = 22 = P {TABLE-4}
ß14 = Þ14 – €14 (% ð) = _ - M (% ð) = 34 – 18 = 16 = K {TABLE-5}

Encrypted message	$	H	M	E	R	R	4	Z	8	B	C	K	R	_
Decrypted Key	M	O	R	@	G	M	A	I	L	.	C	O	M	M
Original Message text	H	.	N	O	#	1	0	,	L	H	R	,	P	K

Table 16. Decrypted message

Finally, we get the original message from the proposed method at the receiver end device.

Conclusion:

Strong Algorithms mechanism play a very strong role in different application domain like IoT, IoMT, AIoT, etc. In this article, proposed a new encryption method name IPK for secure communication for IoT devices. The proposed methodology worked with the message which shows special characters, numbers, and bits for data encryption and decryption. In authority, the end key isn't known so we would encryption to able have the option to gadgets data using particular keys and scramble packet per special key.

References

[1] B. S. Adiga, P. Balamuralidhar, M. A. Rajan, R. Shastry, and V. L. Shivraj, "An Identity Based Encryption Using Elliptic Curve Cryptography for Secure M2MCommunication," in Proceedings of the first international Conference on Security of Internet of things, ser. SecurIT '12. ACM, 2012, pp. 68–74

[2] D. D´ıaz Pardo de Vera, ´A. Sig¨uenzaIzquierdo, J. BernatVercher, and L. A. Hernandez Gomez, "AUbiquitous sensor network platform for integrating smart devices into the semantic sensor web," vol. 14, no. 6.Multidisciplinary Digital Publishing Institute, 2014, pp. 10725–10752.

[3] ChandrasegarThirumalai, Senthilkumar M, SilambarasanR, Carlos Becker Westphall, "Analyzing the strength of Pell's RSA," IJPT, Vol. 8 Issue 4, Dec. 2016 pp.21869-21874.

[4] Thangavel, M., P. Varalakshmi, MukundMurrali, K. Nithya, "An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)," in Journal of Information Security and application, Vol. 20, 2015, pp. 3-10.

[5] ChandrasegarThirumalai, Senthilkumar M, Vaishnavi B, "Physicians Medicament using Linear Public Key Crypto System," in International Conference on Electrical, Electronics, and Optimization Techniques IEEEICEEOT, March 2016.

[6] Bellini, Emanuele, and Nadir Murru. 2015. "An Efficient and Secure RSA--like Cryptosystem Exploiting R'edei Rational Functions over Conics." : 1–18.

[7] ChandrasegarThirumalai, "Review on the memory-efficient RSA variants," International Journal of Pharmacy andTechnology, Vol. 8 Issue 4, Dec. 2016, pp.4907-4916.

[8] Hung-min sun, Mu-en wu, Wei-chi ting, and M. JasonHinek "Dual RSA and its security analysis," IEEE transactions on information theory, vol. 53, no. 8, August 2007.

[9] T Chandra Segar, R Vijayaragavan, "Pell's RSA key generation and its security analysis," in Computing, Communications, and Networking Technologies (ICCCNT) 2013, pp. 1-5.

[10] Rivest RL, Shamir A, Adleman LA.1978, "Method for obtaining digital signatures and public-key cryptosystems". CommunACM.

[11] ChandrasegarThirumalai, "Physicians Drug encoding system using an Efficient and Secured Linear Public KeyCryptosystem (ESLPKC)," International Journal of pharmacy and technology, Vol. 8 Issue 3, Sep. 2016 pp. 16296-16303.

[12] Mayank Jhalani, Piyush Singh, Gaurav Shrivastava, "Enhancement over the variant of public-key cryptography algorithm," in International journal of emerging technology and advanced engineering, Vol. 2, Issue 12, Dec. 2012.

[13] Chandramowliswaran, N., S. Srinivasan, and P. Muralikrishna. "Authenticated key distribution using a given set of primes for secret sharing," Systems Science & Control Engineering 2015, Vol.3, Issue 1, pp. 106-112.

[14] Chandramowliswaran N, Srinivasan's, and ChandraSegar.T, "A Note on Linear based Set Associative CacheAddress System" International J. of Computer Science and Engg. (IJCSE) & India, Engineering Journals & 0975-3397, Vol. 4 No. 08 / pp. 1383-1386 / Aug. 2012.

[15] Forouzan BA.2007, “Cryptography and network security”. Special Indian Edition. Tata McGraw-Hill, p. 2011.

[16] ChandrasegarThirumalai, Senthilkumar M, “Secured E-Mail System using Base 128 Encoding Scheme,” International Journal of pharmacy and technology, Vol. 8 Issue 4, Dec. 2016 pp. 21797-21806.

[17] Ravi Shankar Dhakar, Amit Kumar Gupta, Prashant Sharma, 2012,” Modified RSA Encryption Algorithm(MREA)” advanceAdvancedComputing&Communication Technologies (ACCT).

[18] Chandramowliswaran N, Srinivasan.S and ChandraSegar.T, “A Novel Scheme for Secured Associative Mapping” The International J. of Computer Science and applications (TIJCSA) & India, TIJCSA Publishers & 2278-1080, Vol. 1, No 5 / pp. 1-7 / July 2012.

[19] He, Debian, et al. "Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures." IEEE Transactions on Information Forensics and Security 11.9 (2016): 2052-2064.

[20] ChandrasegarThirumalai, SathishShanmugam, “Multi-key distribution scheme using Diophantine form for secure IoT communications,” IEEE IPACT 2017.

[21] Butun, Ismail, et al. "Cloud-centric multi-level authentication as a service for secure public safety device networks." IEEE Communications Magazine 54.4 (2016): 47-53.

[22] ChandrasegarThirumalai, Viswanathan P, “Diophantine based Asymmetric Cryptomata for cloud Confidentiality and Blind Signatureapplications,” JISA, Elsevier, 2017.

[23] Vasco, María Isabel González, Florian Hess, and Rainer Steinwandt. "Combined schemes for signature and encryption: The public-key and the identity-based setting." Information and Computation 247 (2016): 110.

[24] Shim, Kyung-Ah. "A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks." IEEE Communications Surveys & Tutorials 18.1 (2016): 577-601.

[25] X. Wang, J.Zhang, E.Schooler, and M. Ion, “Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT,” in Communications(ICC), 2014 IEEE International Conference on, June 2014, pp. 725–730.

[26] M. Ion, “Security of Publish/Subscribe Systems,” Ph.D. dissertation, University of Trento, Italy, May 2013.

[27] P. Pal, G. Lauer, J. Khoury, N. Hoff, and J. Loyall, “P3S: A Privacy-Preserving Publish-subscribe Middleware,” in Proceedings of the 13th International Middleware Conference, ser. Middleware '12, pp. 476– 495.

[28] M. Ion, G.Russello, and B.Crispo, “Supporting Publication and Subscription Confidentiality in Pub/Sub Networks,” in Security and Privacy in CommunicationNetworks, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 50, 2010, pp. 272–289.

[29] M. A. Tariq, “Non-functional Requirements in Publish/SubscribeSystems,” Ph.D.dissertation, Secure Communication of IoT-based Devices using EPEB Algorithm.

[30] Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis of the security concerns of the internet of things (IoT). International Journal of Computer Applications, 111(7).

[31] Doukas, C., Maglogiannis, I., Koufi, V., Malamateniou, F., & Vassilacopoulos, G. (2012, November). Enabling data protection through PKI encryption in IoT m-Health devices. In 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE) (pp. 25-29). IEEE.

[32] Marosi, A. C., Lovas, R., Kisari, Á., & Simonyi, E. (2018, January). A novel IoT platform for the era of connected cars. In 2018 IEEE International Conference on Future IoT Technologies (Future IoT) (pp. 1-11). IEEE.

[33] Bellini, P., Nesi, P., Paolucci, M., & Zaza, I. (2018, March). Smart City architecture for data ingestion and analytics: Processes and solutions. In 2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService) (pp. 137-144). IEEE.