ISSN No.: 2455-6130
Volume 1, Issue 7, 2016, pp. 15-28

website: www.ijoetr.com

International Journal of Emerging Trends in Research

Enhanced Hybrid Cipher based Cryptography Scheme for Internet of Things

Silkey Arora[1], Vikas Sandhu[2], Viney Dhawan[3]

[1,2,3]ECE, KITM, Kunjpura Karnal, Haryana, India

Abstract

With the emergence of an internet of things, new techniques which can be regulatory ensure its privacy and protection become necessary. In particular, assaults have actually to be data authenticated, intercepted, access controlled and the privacy of customers. The nature for the IoT asks for a heterogeneous and differentiated framework that is legal acceptably takes into account the globalist, verticality, ubiquity and technicity of the IoT. Geographically restricted legislation that is nationwide maybe not seems appropriate in this context. However, self-regulation as it has been applied until now may possibly not be sufficient to ensure privacy that is effective protection, either. Therefore, a framework of substantive key concepts set by a legislator at the worldwide level, complemented by the private sector with more detailed regulation is apparently the solution that is most beneficial. Through such a framework, general pillars of regulation could be set for everyone, which are then suitable to be supplemented by the individuals concerned in ways that suits their needs that are present. Also, the inclusion of an legislator that is worldwide the process additionally ensures the continued involvement of the public sector, contributing at minimum by monitoring the process. Present work proposed a protocol that uses key matrices concept. In this protocol we make use of key matrices and store same key matrix at all the communicating nodes. Thus when plain text is encrypted to cipher text at the sending side, the sender transmits the cipher text without the key that is to be used to decrypt the message.

Keywords: Internet ; Security; Encryption; Hybrid Cipher

1. Security in IoT

As with the advancement of IoT, the application of IoT/M2M is affecting our daily lives. So it is very important to ensure the security of the IoT/M2M system[1]. As IP addresses are being used in order to develop IoT/M2M systems, the system has become the target of various intruders and attacks. With time these attacks will grow complex and more sophisticated and it is necessary to stop such attacks by incorporating various security measures in the IoT/M2M system. Also there are large number of endpoints in the IoT system, so the intruder can enter through any of the end-point in the system, thus making it more complex to establish security in the system. The potential attack can span from just minor stalking to damage to infrastructure or loss of life.

As seen, the threats to the IoT system may be similar to that of the conventional system but the damage that can be done is significantly different. That is why there are many efforts to analyze the threats and risks.

One of the fundamental elements in securing an IoT infrastructure is around device identity and mechanisms to authenticate it. Many IOT devices may not have the required compute power, memory or storage to support the current authentication protocols. Today's strong encryption and authentication schemes are based on cryptographic suites such as Advanced Encryption System (AES)[2] for confidential data transport, Rivest-Shamir-Adleman (RSA)[3] for digital signatures and key transport and Diffie-Hellman (DH)[4] for key negotiations and management. While the protocols are robust, they require high compute platform and a resource that may not exist in all IoT-attached devices. Authentication and authorization need to be done in an appropriate way in order to make our new IoT world threat free.

The authentication and authorization protocols need human intervention which is not possible in some cases due to limited access to IoT devices. Therefore these devices need initial configuration to be done to protect from tampering, thefts and any other form of attack throughout its life.

In order to overcome these issues new authentication and authorization need to be built using the experience of today’s strong encryption algorithms.

2. Related work

Antonio f Skarmeta, (2014)[5] proposed a paper that provides various challenges that are existing in this field and also provides description of some challenges that need to be overcome in coming years for full acceptance of IoT by the society. The paper also proposes a capability-based access control mechanism which is built on public key cryptography in order to eradicate or overcome these challenges. Its solution is based on token used to access the constrained application protocol (CoAP). It also uses an optimized implementation of Elliptical curve Digital Signature Algorithm (ECDSA) inside the smart entities. *Xu Xingmei, (2013)* [6] proposed a paper that introduces various aspects like basic characteristics, network architecture, key technologies and Security problems of internet of things. The basic characteristics include overall perception, reliable transmission and intelligent processing. The network architecture is divided into layers viz-sensing layer, transport layer and application layer. The Key technologies comprise of radio frequency identification (RFID), Sensor technology and network and embedded system technology. The paper also describes some method to provide security in internet of things.

Jungyub Lee et al., (2015) [7] have published a paper on securing internet of things network. As we know that using the present internet, data owners can provide integrity and authentication when data is getting generated. But confidentiality is not implemented by the owners as it is implemented by the symmetric keys between ends. But in internet of things confidentiality cannot be implemented suitably using this method as there are many consumers. Also consumers differ in their ability to use only a specific a part of the cipher text as the nodes don’t know about the context. In this paper they have shown work as how confidentiality can be done in IoT. They have proposed a way in which producer encrypts the data along with context. They have improved key policy attribute based encryption and cipher text policy attribute based encryption to allow consumers to decrypt data according to context. *Jong jin Lee e al.,* [8] proposed an authentication scheme based on elliptical curve cryptosystem and opened in the internet of things. In internet of things secure communication should be designed between one node and the other.

In this paper they have focused on an efficient secure key establishment based on ECC. This proposed method can prevent attacks like eavesdropping, man in the middle, replay attacks.

Pierre de Leusse et al., [9] proposed a paper on internet of things. In this paper it has stated as in internet of things large number of items can be addressed through internet and thus various attacks can be done. Therefore, it has led to the conclusion that current internet cannot be used as the platform to IoT. In this paper the authors has also stated various requirements for resources that will make them to be used in IoT environment. Also the authors have proposed an architectural model of self managed security cell. *Giulio Peretti et al.,* [10] proposed a paper entitles "An end to end security framework for internet of things". The paper describes a framework called as BlinkToSCoAP. The name due to the integration of three lightweight technologies of DTLS, CoAP and 6LoWPAN over tinyOS.

Christina Hochleitner et al., [11] proposes a paper in which they have given a method of making the end points trustworthy. One of the important end point of internet of thing environment are mobile phones. These end points help users to interact with their appliances known as "things" in IoT. This paper presents an approach that provides users with the underlying security information on mobile systems and helps them to establish trust in internet of things. *Sasa Radomirovic et al.,* [12] proposed a paperin whichthey provide a security model which allows to ponder about security and privacy of communication protocols in the internet of things. The model they provided is designed on few assumptions and on various observations on various threats that we may face in internet of things.

Hui Suo et al., [13] proposed a paper in security of internet of things. In the past decade internet of things is finding its use in full throttle. The key features of IoT application are security and privacy. With such advancement in technology Internet of things is still facing various enormous challenges in its application. The paper proposed by the author puts emphasis on these key features i.e security. The paper has discussed the status of the key technologies being used in implementation of internet of things. These technologies include encryption mechanism, communication security, protection of sensor data and various cryptographic algorithms.

Quangang Wen, (2012) [14] proposed a paper that describes the security structure of sensor level, network layer and application layer in internet of things. The paper analyses the security feature of the sensor layer and then applies a protocol called as Hybrid Cyber security certificate, a new method for authentication mechanism among various nodes in sensor level. This certificate is based on the principle "one time one cipher" between communicating nodes. This technology or method uses time stamp technology band timeliness is guaranteed between two parties. Hybrid cipher certificate can be applied for communication among various nodes in IoT. The hybrid variable security certificate is an authentication protocol; based on request-reply mechanism.

A. Botta, et al. in "Integration of Cloud Calculating and Internet of Things: a Survey" [15] (2016) In this paper, author focus attention on the integration of Cloud and IoT, that is what we call the Claudio paradigm. Countless works in works have surveyed Cloud and IoT separately and, extra precisely, their main properties, features, underlying technologies, and open issues. Though, to the best of our vision, these works lack a methodical research of the new Claudio paradigm, that involves completely new requests, trials, and research issues. To connection this gap, in this paper we furnish a works survey on the integration of Cloud and IoT. Starting by analyzing the basics of both IoT and Cloud Computing, we debate their complementarily, detailing what is presently steering to their integration. In this paper, we surveyed the works in order to recognize the complementary aspects of Cloud and IoT and the main drivers for incorporating them into a

exceptional environment. As the adoption of the Claudio paradigm enabled countless new requests, we derived the main research trials of attention for every single of them.

L. Marin , et al. in "Optimized ECC Implementation for Safeguard Contact amid Heterogeneous IoT Mechanisms " [16] (2015] We present optimized elliptic arc Cryptography algorithms that address the protection subjects in the heterogeneous IoT networks. We have joined cryptographic algorithms for the NXP/Jennic 5148- and MSP430-based IoT mechanisms and utilized them to crafted novel key arbitration protocol. Ongoing work is concentrated on the optimization of the ECC primitives for the needs of the disparate microprocessors, and a extra elevated authentication mechanism is being designed. Power is additionally locale into the integration of the counseled resolution alongside Belief Expansion Protocol for Authentication of New used Objects and sensors across the Producer, and additionally, an expansion of this work is envisioned for the Bluetooth Low Power mechanisms for the needs of the honestly heterogeneous IoT ecosystem. *D Hemalatha , et al.* in "Development in RFID (Radio Frequency Identification) Knowledge in Internet of Things (IOT) [17] (2015) This paper provides an overview of the Internet of Things (IoT) that is enabled by the latest events in RFID, intelligent sensors, contact technologies and Internet protocols. The present metamorphosis in Internet, mobile and machine-to-machine (M2M) technologies can be perceived as the early period of the IoT. The radio-frequency identification (RFID) knowledge is one of the core technologies of IoT placements in the healthcare environment. We recognized a little of the protection necessities that an RFID authentication scheme ought to satisfy. We discovered that merely three presently counseled ECC-based RFID authentication schemes are able to gratify all the protection requirements.

S. Sicari, et al. in "Security, privacy and belief in Internet of Things: The road in front [18] (2015) the satisfaction of protection and privacy necessities plays a frank role. Such necessities contain data confidentiality and authentication, admission manipulation inside the IoT web, privacy and belief amid users and things, and the implementation of protection and privacy policies. Instituted protection countermeasures cannot be undeviatingly requested to IoT technologies due to the disparate standards and contact stacks involved. This paper will be helpful in counseling the research road in front, in order to permit a large placement of IoT arrangements in real world. *A Agarwal, et al.* in "The Internet of Things—A survey of cases and trends [19] (2015) The Internet of Things is a paradigm whereas everyday objects can be outfitted alongside recognizing, detecting, networking and processing skills that will permit them to converse alongside one more and alongside supplementary mechanisms and services above the Internet to finish a little objective. The IoT builds on continuing technologies such as RFID and Wireless Sensor Webs alongside alongside standards and protocols to prop machine-to-machine contact such as those envisioned for the semantic web. One question that stays is whether or not the IoT is to be a tolerating knowledge, whether it will flounder to materialize, or whether it is a pacing stone to one more paradigm. Merely period will in the end answer that question. Though, by carrying continuing technologies jointly in a novel method, the IoT has the possible to reshape our world.

H. Shafagh, et al., in "Toward Calculating above Encrypted Data in IoT Arrangements [20] (2015] Methods established on encrypted data computing materialize to be enthusing approaches. Though, they hold new trials alongside respect to functionality and computing resources that have to early be resolved beforehand they can be consolidated into IoT systems. In this article, we debate encrypted data computing ways, their use-cases, and the trials yet to be addressed, exceptionally alongside stare to the IoT. The power of comprehending hypothetical cryptographic ways below real-world conditions sheds light on undiscovered flaws and creates opportunities for

enhancements in cryptosystems. It stays an vital open research setback to design and clarify safeguard and useful encrypted data processing schemes for the IoT domain.

JM Bohli,et al. in "Selective Decryption of Outsourced IoT Data [21] (2015) We counsel believed of a Protection Broker established on symmetric encryption schemes. It proposals a key association scheme to flexibly craft short decryption keys for period intervals or specific scopes of measurement values. We more display how the scheme can be generalized or a combination of the schemes can be applied. We requested a prototype in Java and analyzed its performance. In this paper we gave a novel protection scheme projected to enable data proprietors to offload IoT data storage into Cloud Service Providers cryptographically minimizing data exposure. The scheme is exceedingly configurable to encounter the data proprietors needs and supports time-, range- and context-based protection of data.

J. Granjal, et al. in "Security for the Internet of Things: A Survey of Continuing Protocols and Open Research Subjects [22] (2015) The Internet of Things (IoT) introduces a vision of a upcoming Internet whereas users, computing arrangements, and everyday objects owning detecting and actuating skills cooperate alongside unprecedented ease and frugal benefits. As alongside the present Internet design, IP-based contact protocols will frolic a key act in enabling the omnipresent connectivity of mechanisms in the context of IoT applications. In conclusion, we trust this survey could furnish an vital contribution to the research area, by documenting the present rank of this vital and extremely vibrant span of research, helping readers interested in growing new resolutions to address protection in the context of contact protocols for the IoT.

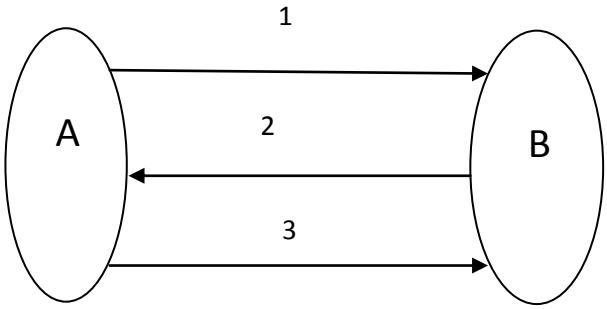
H. Shafagh, et al. in " Poster: Towards Encrypted Query Processing for the Internet of Things [23] (2015] The potential of inferring privacy disregarding data from IoT data necessitates adequate protection measures considering data storage and communication. To address these privacy and protection concerns, we familiarize our arrangement that stores IoT data securely in the Cloud database as yet permitting query processing above the encrypted data. We will display the usefully and presentation of our arrangement across an enhanced prototype implementation and methodical evaluation pondering both micro benchmarking and arrangement performance. *W. Shi,et al.* in" On the protection of a certificate less online/offline signcryption for Internet of Things [24] (2015] this paper, we will display their scheme is vulnerable to the confidential key compromised setback, i.e., an antagonist might become a user's confidential key across an interrupted message. The research display that *Luo et al.*'s scheme is not suitable for the IOT. Recently, *Luo et al.* counseled an effectual COOSC scheme for the Internet of Things. They asserted that their scheme is provably safeguard in the random oracle mode. Though, afterward studying of their scheme and analyzing its protection, we clarify that their scheme is vulnerable to the confidential key compromised problem.

A. Patil, et al. in "Hybrid Handy and Robust Encryption Design for Protection in IoT [25] (2015) In this paper, we have counseled a robust hybrid construction by mixture of RECTANGLE, LED and SPECK. With the aid of a hybrid design, we have enhanced the key arranging aspect of LED and connected key aggressions that were disregarded in the LED cipher. In this paper, we additionally aimed at bestowing robust design by cutting impression span to as less as possible. In this paper, we aimed at reinforcing the LED cipher by encompassing SPECK key arranging that was disregarded across the design of LED cipher. This could expose LED to the connected key attacks. SPECK key arranging flawlessly meets the necessity of LED cipher, by producing flawlessly 13 keys of 64 bits each. Moreover, in this paper, we have deigned compact hybrid arrangement for LED cipher that aftermath in less impression span as contrasted to LED cipher

design. To the best of our vision, this is the most compact and smallest implementation of LED cipher so far.

HJ Kim, et al. in "Toward an Inverse-free Handy Encryption Scheme for IoT [26] (2014) In this paper, we familiarize a well-known handy encryption scheme, PRINCE, and a method to increase the memo space of PRINCE by familiarizing XLS (eXtension by Latin Square). We debate the cryptographic necessities of our inverse-free handy encryption scheme and counsel how to spread a PRINCE-like encryption scheme for the safeguard IoT system. Our counseled scheme ought to be adjusted to challenge the connected key attack, and finished protection facts of the scheme opposing all the recognized aggressions encompassing side-channel aggressions ought to be done. The disparate kinds of the multipart mutation and the constituents of PRINCE ought to be learned to design a faster and cost-efficient encryption scheme

J Pescatore, et al. in Safeguarding the "Internet of Things" Survey [27] (2014) But what precisely is the Internet of Things? And what will it mean to cyber security? There are supplementary words in use that usually mean the alike thing. The Nationwide Protection Telecommunications Advisory Council (NSTAC) has commenced a working cluster to gaze at the nationwide protection implications of the "Industrial Internet,"1 and the Nationwide Institute of Standards and Knowledge (NIST) has utilized the word "Cyber-Physical Systems."2 Countless vendors have additionally utilized the word the "Internet of Everything." Though, Internet of Things (IoT) is the most extensively utilized term. Dynamic cipher [15] security certificate is a protocol that works on reply-request mechanism. In this protocol a key matrix is generated and same key matrix is stored at all communicating parties. The advance thing in using this protocol is that the sender does not need to send decryption key instead it sends the co-ordinate of the key matrix where this key is stored. As same key matrix is stored at all the nodes, the recipient will use the co-ordinate sent by the sender and will get the key from its key matrix using this co-ordinate. The authentication process of this protocol is shown between two parties A and B as client and server respectively.



The process is as follows:

1. *A B: Pos_x1_y1, E(Kab1: ID_A, cmd, Ta1)*
2. *B A: Pos_X2_Y2, E(Kab2: ID_B, Com_x_y, Ta1, Tb1)*
3. *A B: E(Kab3: Text, ID_A, Ta2, Tb1)*

Where ID_A, ID_B means ID number of node A and node , Cmd means connection request, Pos_X_Y means coordinates of the key matrix, TA and TB means timestamp of node A and node B, E(Kab:m) means using password Kab to code message m, Text means message constant.

As seen from the above description, three steps exists, In the first step client node A send the encrypted information ID_a, a connection request Cmd, and a timestamp Ta1, and at the same

time client A starts a timer and id it does not receive acknowledgment in allotted time then cancels the session.
If some information is received by server B, it will verify the ID_a from node A. if A validates it then B sends an encrypted information to A. the encrypted information consists of encrypted information ID_b, co-ordinates of key matrix Com_x_y, Timestamp Ta1, Timestamp Tb1 and at the same tie B starts a timer. If it does not receive any feedback from client A, it will cancel the session.
When some information is received at A, it will verify the encrypted information Ta1. If B is validity the A gets a communication password Kab according to co-ordinates of the key matrix. Then A generates a new time stamp ta2, combines with ta1 and sending message constant. Whole of this will be sent to B and up to this point a communicational channel is set between two parties.

3. Proposed work

The hybrid RSA and AES based algorithm uses random waypoint mobility model, In random-based mobility models, the mobile nodes move randomly and freely lacking restrictions. To be extra specific, the destination, speed and association are all selected randomly and independently of supplementary nodes. This kind of ideal has been utilized in countless simulation studies.
The Random Waypoint Ideal the Random Waypoint Ideal was early counseled by Johnson and Maltz. Soon, it came to be'benchmark' mobility ideal to assess the mobile routing protocols, because of its simplicity and expansive availability. To produce the node draw of the Random Waypoint ideal the set examination instrument from the CMU Sovereign cluster could be used. This instrument is encompassed in the extensively utilized web simulator ns-2.

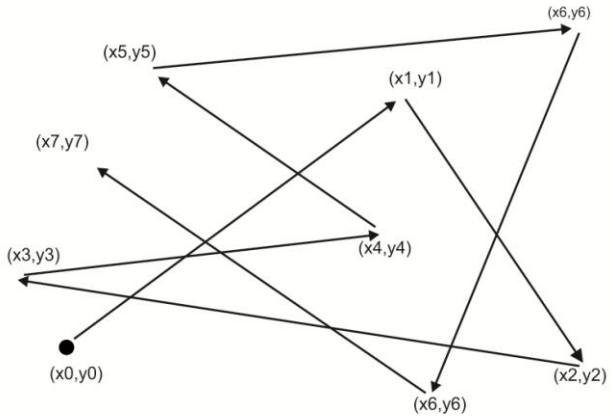


Figure 1. IoT node movement in the Random Waypoint Model

The implementation of this mobility ideal is as follows: as the simulation starts, every single mobile node randomly selects one locale in the simulation earth as the destination. It next travels towards this destination alongside steady velocity selected uniformly and randomly from [*0, Vmax*], whereas the parameter Vmax is the maximum allowable velocity for every single mobile node. The velocity and association of a node are selected independently of supplementary nodes. On grasping the destination, the node stops for a period described by the 'pause time' parameter Tpause. If *Tpause =0*, this leads to constant mobility. Later this period, it once more chooses one more random destination in the simulation earth and moves towards it. The finished procedure is

recapped once more and once more till the simulation ends. As an example, the movement draw of a node is shown in Fig above.

In the Random Waypoint ideal, *Vmax* and *Tpause* are the two key parameters that ascertain the mobility deeds of nodes. If the *Vmax* is tiny and the pause period *Tpause* is long, the topology of Ad Hoc web becomes moderately stable. On the supplementary hand, if the node moves fast (i.e., is large) and the pause period Tpause is tiny, the topology is anticipated to be exceedingly vibrant *Vmax*. Fluctuating these two parameters, exceptionally the *Vmax* parameter, the Random Waypoint ideal can produce assorted mobility scenarios alongside disparate levels of nodal speed. Therefore, it seems vital to quantify the nodal speed.

Public Key Encryption: Encryption Scheme used to Encrypt Messages using Public Key of the node and Decryption usingthe Private keys.

Private Key Encryption: Encryption Scheme used to Encrypt Private key of the Node using the Location of each node before Sending any data.

Step 1: Receiver **R** Requests data from the node **S**, only receiver knows the exact location of itself.

Step 2: On receiving request from the **R** node the sender initiate public key Exchange using RSA algorithm and stores keys P_k as Private key of the node R and P_u as the public key to encrypt the data.

Step 3: Node S then Request the Location L_{Rxy} of the node R.

Step 4: After receiving request from the node S the R sends its location L_{Rxy} to the node S.

Step 5: S then Encrypts the private key of the by using L_{Rxy}as Private key using AES algorithm

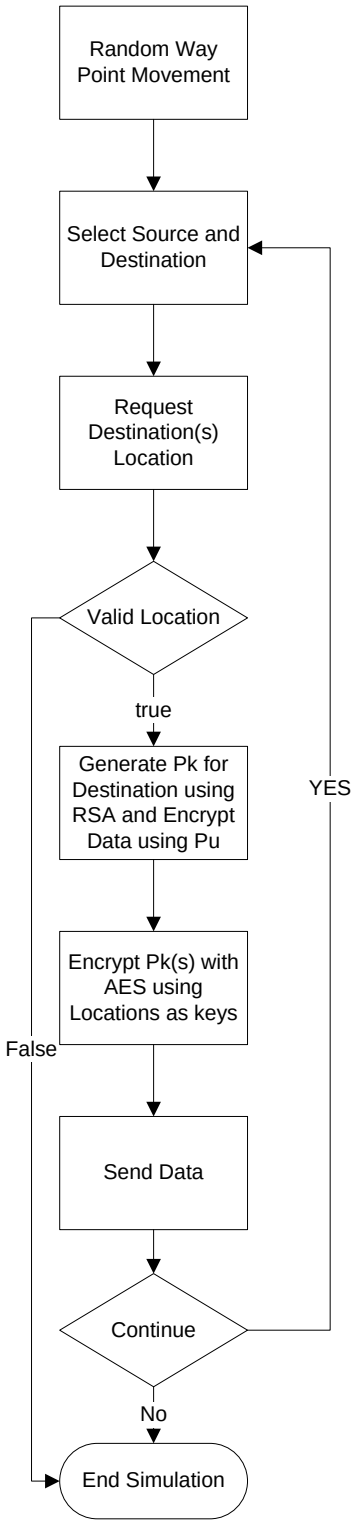
Step 6: for multiple recipients the Same process in repeated and a matrix is formed in following manner and forwarded to recipients

Encrypted Data (RSA)	L_{Rxy}private key of the receiver 1 (AES)
	L_{Rxy}private key of the receiver 2 (AES)
	….
	L_{Rxy}private key of the receiver N (AES)

.

Step 7: After receiving the packet the recipient decrypts the private key using its location and then decrypts the data sent by the sender.

The nodes need to send data between each other. But if the nodes will send the data in plain text, any attacker or intruder can get that data and misuse it or even alter it. So in order to restrict an intruder to carry out any sort of attack on the data, the data is sent in a form that is not easily understandable by any third party person. We used AES algorithm to encrypt the private key of the authenticated user by estimating its exact location.



4. Simulation parameters

Following table describes the simulation parameters for IoT mobility in MATLAB, each node properties is defined in MATLAB Structure.

Parameter	Value
Node POSITION_X_INTERVAL	10-30
Node POSITION_Y_INTERVAL	10-30
Node SPEED_INTERVAL	0.2-2.2
Node PAUSE_INTERVAL	0-1
Node WALK_INTERVAL	2.00-6.00
Node DIRECTION_INTERVAL	-180-180
SIMULATION_TIME	500
Number of Nodes	20
Public Key Encryption	RSA
Private Key Encryption	AES

Node POSITION_X_INTERVAL: X position of the Node at any given moment, updates due to Random Way Point Model

Node POSITION_Y_INTERVAL: Y position of the Node at any given moment, updates due to Random Way Point Model

Node SPEED_INTERVAL: Speed Range of Each Node factor of 0.2 to 2.2x speed with respect to stationary nodes.

Node PAUSE_INTERVAL: For how long a node will stay stationary

Node WALK_INTERVAL: For how long a node will stay moving

Node DIRECTION_INTERVAL: In which direction the node will be moving.

SIMULATION_TIME: Overall Simulation Time of the Node.

Number of Nodes: Total number of nodes present in the Simulation (default: 20)

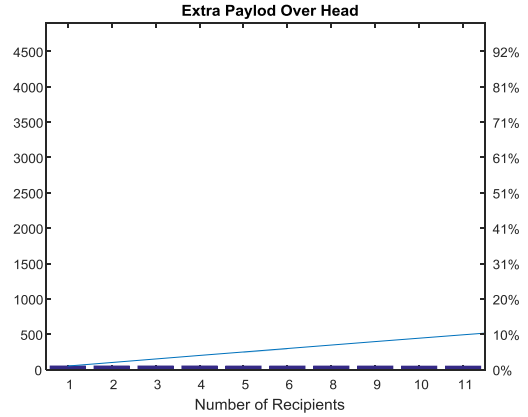
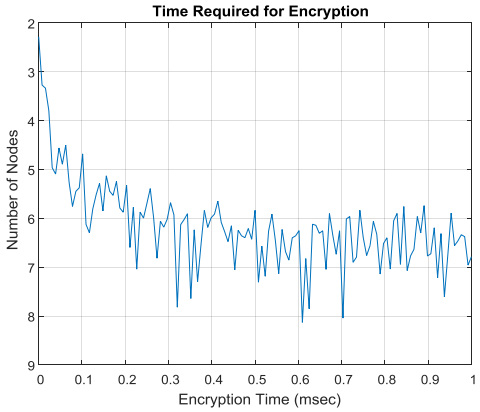
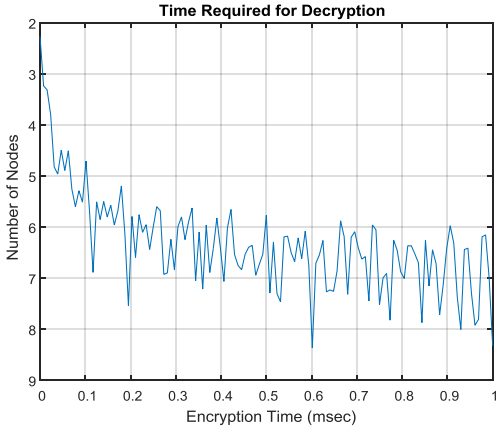


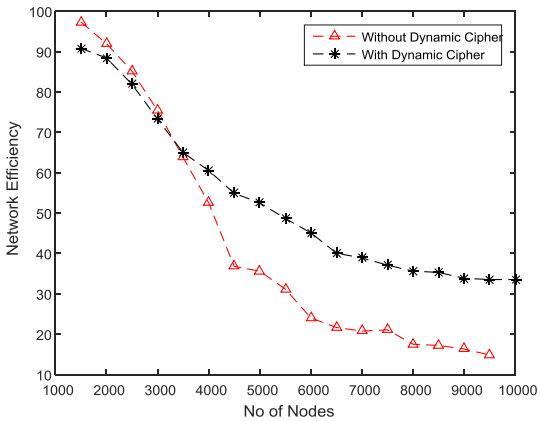
Figure 2: Number of Recipients and network overhead (payload)

As for each location a new private key is generated and attached to the packet, we require that there must not be a significant overhead as the Number of recipient grow**.**



The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. This speed surmounts the symmetric encryption problem of managing secret keys. As on the other hand, this unique feature of public key encryption makes it mathematically less prone to attacks. However, asymmetric encryption techniques are slower than symmetric techniques, because they require more computational processing power. As it can be seen from above fig the encryption time does not increases too much when number of nodes increase as seen in above figure. So does the decryption process as seen below.





The proposed routing protocols performs better when no security scheme is applied when node density and node mobility are made high.The simulation is conducted with 1000 to 10000 nodes for comparing performance of protocol separately with and without encryption. Figure aboveshows nodes efficiency of the proposed protocol when number of nodes is raised upto 10000. Even at this much load the protocol works significantly better than no cipher scheme.

5. Conclusion

The presented simulation results showed that proposed method has a better performance than other common encryption algorithms used. Since it becomes very difficult to estimate the exact location of the node and has not any known security weak points so far, which makes it an excellent candidate to be considered as a standard encryption algorithm for communication between IoT nodes? Using hybrid encryption has although added extra processing time, but overall it was relatively negligible especially for certain application that requires more secure encryption to a relatively large data blocks. Many principles and protocols, given by assorted authors, have been counseled in this report that will aid in safeguarding an Internet of Things (IoT) network. Introduction of the vibrant variable cipher protection certificate protocol is given. This protocol uses key matrices concept. In this protocol we make use of key matrices and store alike key matrix at all the conversing nodes. Therefore after plain text is encrypted to cipher text at the dispatching side, the sender transmits the cipher text lacking the key that is to be utilized to decrypt the message. In spite, the sender sends the co-ordinate of the key matrix whereas the key is stored. Additionally the work to be led has been uttered in that we are employing this protocol to admission several mechanisms simultaneously. We ca finish from the above data that the vibrant variable cipher protection certificate is a extremely good protocol to be requested in internet of thing. In server nodes, area key cryptography needs of influential nodes and/or cryptographic chips. In client nodes whose requests merely demand to link external servers from period to period, this way can be a viable solution. Pre-shared key ways can be functional for server nodes in tiny real-world applications. Though, continuing mathematical-based Key Association Schemes such as RSA scheme, furnish larger properties if the request can afford the supplementary overhead.

References

[1] Kopetz, H. (2011). *Real-time systems: design principles for distributed embedded applications*. Springer Science & Business Media.

[2] Feldhofer, M., Dominikus, S., & Wolkerstorfer, J. (2004, August). Strong authentication for RFID systems using the AES algorithm. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 357-370). Springer Berlin Heidelberg.

[3] Smith, D. R., & Palmer, J. T. (1979). Universal fixed messages and the Rivest-Shamir-Adleman cryptosystem. *Mathematika*, *26*(01), 44-52.

[4] Jara, A. J., Lopez, P., Fernandez, D., Castillo, J. F., Zamora, M. A., & Skarmeta, A. F. (2014). Mobile digcovery: discovering and interacting with the world through the internet of things. *Personal and ubiquitous computing*,*18*(2), 323-338.

[5] Xingmei, X., Jing, Z., & He, W. (2013, October). Research on the basic characteristics, the key technologies, the network architecture and security problems of the internet of things. In *Computer Science and Network Technology (ICCSNT), 2013 3rd International Conference on* (pp. 825-828). IEEE.

[6] Lee, J., Oh, S., & Jang, J. W. (2015). A Work in Progress: Context based encryption scheme for Internet of Things. *Procedia Computer Science*, *56*, 271-275.

[7] Lee, J. J., Hong, Y. S., & Lee, K. Y. (2015, January). An Authentication Scheme Based on Elliptic Curve Cryptosystem and OpenID in the Internet of Things. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 192). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[8] Peretti, G., Lakkundi, V., & Zorzi, M. (2015, January). BlinkToSCoAP: An end-to-end security framework for the Internet of Things. In *2015 7th International Conference on Communication Systems and Networks (COMSNETS)* (pp. 1-6). IEEE.

[9] Hochleitner, C., Graf, C., Unger, D., & Tscheligi, M. (2012, June). Making devices trustworthy: security and trust feedback in the internet of things. In*Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), Newcastle, UK*.

[10] Van Deursen, T., & Radomirovic, S. (2008). Attacks on RFID Protocols.*IACR Cryptology ePrint Archive*, *2008*, 310.

[11] Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on* (Vol. 3, pp. 648-651). IEEE.

[12] Wen, Q., Dong, X., & Zhang, R. (2012, October). Application of dynamic variable cipher security certificate in internet of things. In *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems* (Vol. 3, pp. 1062-1066). IEEE.

[13] Wang, Y., Wong, K. W., Liao, X., & Xiang, T. (2009). A block cipher with dynamic S-boxes based on tent map. *Communications in Nonlinear Science and Numerical Simulation*, *14*(7), 3089-3099.

[14] He, D., Chen, Y., & Chen, J. (2012). Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol. *Nonlinear Dynamics*,*69*(3), 1149-1157.

[15] Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future Generation Computer Systems*, *56*, 684-700.

[16] Marin, L., Pawlowski, M. P., & Jara, A. (2015). Optimized ECC implementation for secure communication between heterogeneous IoT devices. *Sensors*, *15*(9), 21478-21499.

[17] HEMALATHA, D., & AFREEN, B. E. (2015). Development in RFID (Radio Frequency Identification) Technology in Internet of Things (IOT).*Development*, *4*(11).

[18] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*,*76*, 146-164.

[19] Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261-274.

[20] Shafagh, H. (2015). Toward computing over encrypted data in IoT systems.*XRDS: Crossroads, The ACM Magazine for Students*, *22*(2), 48-52.

[21] Bohli, J. M., Kurpatov, R., & Schmidt, M. (2015, December). Selective decryption of outsourced IoT data. In *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on* (pp. 739-744). IEEE.

[22] Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294-1312.

[23] Shafagh, H., Hithnawi, A., Dröscher, A., Duquennoy, S., & Hu, W. (2015, September). Poster: Towards Encrypted Query Processing for the Internet of Things. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking* (pp. 251-253). ACM.

[24] Shi, W., Kumar, N., Gong, P., Chilamkurti, N., & Chang, H. (2015). On the security of a certificateless online/offline signcryption for Internet of Things.*Peer-to-Peer Networking and Applications*, *8*(5), 881-885.

[25] Patil, A., Bansod, G., & Pisharoty, N. (2015). Hybrid Lightweight and Robust Encryption Design for Security in IoT. *International Journal of Security and Its Applications*, *9*(12), 85-98.

[26] Kim, H., & Kim, K. (2014, December). Toward an Inverse-free Lightweight Encryption Scheme for IoT. In *2014 Conference on Information Security & Cryptography*.

[27] Pescatore, J., & Shpantzer, G. (2014). Securing the internet of things survey. *SANS Institute, January*.